

(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
2025 年 1 月 2 日 (02.01.2025)



(10) 国际公布号
WO 2025/001496 A1

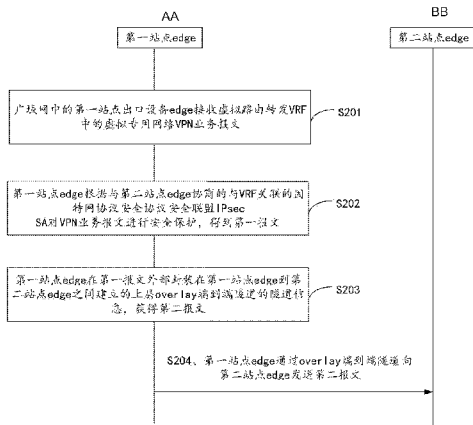
- (51) 国际专利分类号:
H04L 12/46 (2006.01)
- (21) 国际申请号: PCT/CN2024/091039
- (22) 国际申请日: 2024 年 4 月 30 日 (30.04.2024)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202310803215.6 2023年6月30日 (30.06.2023) CN
- (71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (72) 发明人: 骅志康 (PIAN, Zhikang); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129

(CN)。郭天萍 (GUO, Tianping); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。庞东磊 (PANG, Donglei); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。董甲甲 (DONG, Jiajia); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。盛成 (SHENG, Cheng); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。胡棣 (HU, Di); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。金海燕 (JIN, Haiyan); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。田涛 (TIAN, Tao); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 广州三环专利商标代理有限公司 (SCIHEAD IP LAW FIRM); 中国广东省广州市

(54) Title: METHOD FOR SECURELY TRANSMITTING PACKET, AND RELATED DEVICE

(54) 发明名称: 安全传输报文的方法及相关装置



- S201 A first station egress device edge in a wide area network receives a virtual private network (VPN) service packet in virtual routing and forwarding (VRF)
- S202 The first station edge carries out security protection on the VPN service packet on the basis of an Internet Protocol security security association (IPsec SA) about which the first station edge negotiates with a second station edge and which is associated with the VRF, so as to obtain a first packet
- S203 The first station edge encapsulates, outside the first packet, tunnel information of an overlay end-to-end tunnel established between the first station edge and the second station edge, so as to obtain a second packet
- S204 The first station edge transmits the second packet to the second station edge by means of the overlay end-to-end tunnel
- AA First station edge
BB Second station edge

(57) Abstract: The present application provides a method for securely transmitting a packet, a method for negotiating an IPsec SA, and a related device, applied to a wide area network. In an across-multi-tunnel scenario, the IPsec SA for end-to-end security protection is negotiated between a first station edge and a second station edge on the basis of VRF granularity by extending a BGP routing. The first station edge carries out security protection on a VPN service packet on the basis of the IPsec SA, and then transmits the packet by means of an overlay end-to-end tunnel between the first station edge and the second station edge, and the second station edge processes the packet on the basis of the IPsec SA to obtain the VPN service packet. In the present application, it is only needed to carry out security protection once at the first station edge, and an intermediate node does not need to carry out encryption and decryption, thereby ensuring the secure transmission of the packet, improving the transmission efficiency and reducing the transmission delay.

(57) 摘要: 本申请提供了安全传输报文的方法、协商IPsec SA的方法及相关装置, 应用于广域网。在跨越多段隧道场景下, 通过扩展BGP路由, 基于VRF粒度, 在第一站点edge与第二站点edge之间协商用于端到端安全保护的IPsec SA。第一站点edge基于IPsec SA对VPN业务报文进行安全保护后, 将通过第一站点edge与第二站点edge之间的overlay端到端隧道发送所述报文, 第二站点edge基于IPsec SA对报文进行处理, 获得VPN业务报文。本申请中只需在第一站点edge进行一次安全保护, 中间节点无需加解密处理, 既保证报文的安全传输, 又提高传输效率、降低传输延迟。

越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (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, CV, 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, MG, MK, MN, MU, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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))。

安全传输报文的方法及相关装置

本申请要求于 2023 年 06 月 30 日提交中国专利局、申请号为 202310803215.6、申请名称为“安全传输报文的方法及相关装置”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

本申请涉及广域网报文传输领域，尤其涉及安全传输报文的方法和协商 IPsec SA 的方法及相关装置。

背景技术

在底层（underlay）网络的基础上，通过在多个网络节点之间建立隧道，可以构建上层（overlay）网络。overlay 网络实现了业务与底层网络的解耦，使得业务报文能够实现端到端的快速交付。

但由于隧道是基于运营商网络建立的，该网络无法保障业务报文的安全性，因此，隧道自身需要具备一定安全能力，以保证业务报文的安全性。当前普遍采用的方法是，在控制面上建立隧道时，在隧道的入节点与出节点之间通过边界网关协议（border gateway protocol, BGP）基于传输网络端口（transport network port, TNP）粒度进行密钥协商，其中，密钥是与隧道的入节点的端口和出节点的端口绑定的。在隧道建立完成后，当业务报文在隧道中传输时，入节点根据与出节点协商的密钥对业务报文进行加密，使得业务报文在隧道中传输时处于加密状态，当业务报文到达隧道的出节点时，出节点再根据协商的密钥对业务报文进行解密，从而保证业务报文传输的安全性。

上述基于网络节点的 TNP 粒度来对报文进行加解密传输报文的方法，对于每一段隧道都需要入节点与出节点之间协商密钥信息，当业务报文在该段隧道中传输时，在该段隧道的入节点按照协商的方式进行加密，在出节点按照协商的方式进行解密。当业务流需要跨越多段隧道时，各段隧道之间的密钥是不同的，需要在每段隧道的入节点上进行加密，出节点上进行解密，在下一段隧道的入节点上再加密，出节点上再解密...加解密操作繁琐，且消耗设备大量的计算资源，增加了业务报文的转发延迟。

发明内容

本申请提供了安全传输报文的方法、协商 IPsec SA 的方法及相关装置，采用本申请所述的方法，可以提高报文传输效率，降低传输延迟。

第一方面，本申请提供了一种安全传输报文的方法，从数据转发面的发送侧来描述，所述方法包括：广域网中的第一站点出口设备 edge 接收虚拟路由转发 VRF 中的虚拟专用网络 VPN 业务报文；

所述第一站点 edge 根据与第二站点 edge 协商的与所述 VRF 关联的因特网协议安全协议安全联盟 IPsecSA 对所述 VPN 业务报文进行安全保护，以得到第一报文；

所述第一站点 edge 在所述第一报文外层封装在所述第一站点 edge 到所述第二站点 edge 之间建立的上层 overlay 端到端隧道的隧道信息，以获得第二报文，其中，所述 overlay 端到端隧道对应的底层 underlay 隧道包括多段隧道，所述隧道信息包括第一入网点 POP 的第一信息，所述第一站点 edge 为所述 overlay 端到端隧道的入端点，所述第二站点 edge 为所述 overlay 端到端隧道的出端点，所述 overlay 端到端隧道经过所述第一 POP；

所述第一站点 edge 通过所述 overlay 端到端隧道，向所述第二站点 edge 发送所述第二报文。

本申请方案中，在第一站点 edge 与第二站点 edge 之间跨越多段隧道的场景下，第一站点 edge 与第二站点 edge 预先协商好了与 VRF 关联的 IPsecSA，在第一站点 edge 接收到 VRF 中的 VPN 业务报文后，根据与第二站点 edge 协商好的与 VRF 关联的 IPsecSA 对 VPN 业务报文进行安全保护，得到第一报文；再在第一报文的外层封装上第一站点 edge 至第二站点 edge 之间建立的上层 overlay 端到端隧道的隧道信息，获得第二报文；然后，第一站点 edge 将第二报文通过上层 overlay 端到端隧道传输至第二站点 edge，其中，overlay 端到端隧道经过的各个 POP 无需对第二报文进行解密或者加密，只需按照隧道信息进行转发即可。

在第一站点 edge 与第二站点 edge 之间跨越多段隧道的场景下，本申请提供了一种安全传输报文的方法，该方法只需在两个站点 edge 之间建立的上层 overlay 端到端隧道的入端点进行安全保护，在传输过程中无需各个 POP 对报文进行加密或解密，节省了算力资源，降低了传输延迟，提高了报文传输效率。

基于第一方面，在可能的实现方式中，所述对所述 VPN 业务报文进行安全保护包括：对所述 VPN 业务报文进行封装安全载荷 ESP 协议加密；和/或，对所述 VPN 业务报文封装认证头 Authentication Header。

基于第一方面，在可能的实现方式中，所述隧道信息还包括第二 POP 的第二信息，所述 overlay 端到端隧道经过所述第一 POP 和所述第二 POP，所述第一站点 edge 通过所述第一 POP 接入所述广域网，所述第二站点 edge 通过所述第二 POP 接入所述广域网。

基于第一方面，在可能的实现方式中，所述 overlay 端到端隧道为互联网协议第六版本 IPv6 的段路由 SRv6 隧道，所述第二报文包括 IPv6 头和分段路由头 SRH，所述 IPv6 头的目的地址指向所述第一 POP，所述 SRH 包括所述第一信息和所述第二信息。

overlay 端到端隧道可以为 SRv6 隧道，第一站点 edge 在第一报文的外层封装上 SRv6 隧道的隧道信息，SRv6 隧道的隧道信息包括 IPv6 头和分段路由头 SRH，隧道上的各个 POP 可以根据 IPv6 头和分段路由头 SRH 对第二报文进行转发。

基于第一方面，在可能的实现方式中，所述第一信息为所述第一 POP 的第一端点段标识 END.SID，所述第一端点段标识 END.SID 关联的操作包括：根据所述 END.SID 的下一跳 SID 匹配从所述第一 POP 到所述第二 POP 之间的上层 overlay SRv6 Policy。

基于第一方面，在可能的实现方式中，所述 overlay 端到端隧道为分段路由多协议标签交换流量工程策略 SR-MPLS TE Policy，所述第二报文包括 MPLS 标签栈，所述 MPLS 标签栈包括所述第一信息和所述第二信息。

基于第一方面，在可能的实现方式中，所述第一信息为所述第一 POP 的第一节点 SID，所述第一节点 SID 关联的操作包括：根据所述标签栈中所述第一节点 SID 的下一跳 SID 匹配从所述第一 POP 到所述第二 POP 之间的上层 overlay SR MPLS 隧道。

基于第一方面，在可能的实现方式中，所述 overlay 端到端隧道为基于通用网络虚拟化封装 GENEVE 协议封装的隧道，所述第二报文采用 SRv6 in GENEVE 封装。

基于第一方面，在可能的实现方式中，所述 overlay 端到端隧道为基于通用路由封装 GRE 协议封装的隧道，所述第二报文采用 SRv6 over GRE 封装。

基于第一方面，在可能的实现方式中，在所述第一站点 edge 接收所述业务报文之前，所述方法还包括：

所述第一站点 edge 接收所述第二站点 edge 通告的边界网关协议 BGP 路由，所述 BGP 路由包括路由类型 RT、所述 IPsec SA、所述第二站点 edge 的标识、以及导出路由目标 Export RT，其中，所述路由类型 RT 指示所述 BGP 路由通告的所述 IPsec SA 用于对与所述 Export RT 匹配的所述虚拟路由转发 VRF 中的所述 VPN 业务报文进行端到端安全保护；根据所述路由类型 RT 和所述 Export RT，所述第一站点 edge 将所述 IPsec SA 与所述 VRF 关联。

BGP 路由中新增了一种路由类型，BGP 路由中携带了 IPsec SA 和 Export RT，新增的路由类型 RT 指示 BGP 路由通告的 IPsec SA 用于对与 Export RT 匹配的 VRF 中的 VPN 业务报文进行端到端安全保护。通过 BGP 路由通告，使得第一站点 edge 与第二站点 edge 之间协商好了与 VRF 关联的 IPsec SA，该 IPsec SA 用于对 VRF 中的 VPN 业务报文进行安全保护，尤其在第一站点 edge 与第二站点 edge 之间跨越多段隧道的情况下，为 VPN 业务报文的安全、快速传输奠定了基础。实施本申请实施例，实现了 VPN 业务报文的安全、快速传输，降低了传输延时，提高了传输效率。

基于第一方面，在可能的实现方式中，所述 BGP 路由为 BGP 软件定义的广域网 SD-WAN 路由，该 BGP SD-WAN 路由的子地址族为 SD-WAN 子地址族，或者，所述 BGP 路由为 BGP 以太网虚拟专用网络 EVPN 路由，该 BGP EVPN 路由的子地址族为 EVPN 子地址族。

基于第一方面，在可能的实现方式中，所述第二站点 edge 的标识包括所述第二站点 edge 所属的站点标识 site ID 和/或所述第二站点 edge 的节点标识 Node ID。在一种实现方式中，第二站点 edge 的标识可以是第二站点标识 site ID 和节点标识 Node ID，通过第二站点标识 site ID 和节点标识 Node ID 可以确定第二站点 edge，第一站点 edge 与第二站点 edge 之间基于协商的 IPsec SA 对业务报文进行安全保护和传输。在又一种实现方式中，第二站点 edge 的标识可以是节点标识 Node ID，节点 Node ID 在广域网中是全局唯一的，根据 Node ID 可以确定第二站点 edge。在又一种实现方式中，第二站点 edge 的标识可以是第二站点标识 site ID，这种情况下，第一站点中的任意一个 edge 接收到第二站点中的任意一个 edge 通告的 BGP 路由，其中 BGP 路由中携带的包括第二站点的标识和 IPsec SA，则表示第一站点与第二站点协商的密钥为 IPsec SA，第一站点中的任意一个 edge 与第二站点中的任意一个 edge 之间均可以通过协商的 IPsec SA 对业务报文进行安全保护和传输。

基于第一方面，在可能的实现方式中，所述 BGP 路由包括网络层可达信息 NLRI，所述 NLRI 包括所述路由类型 RT 和所述第二站点 edge 的标识。

基于第一方面，在可能的实现方式中，所述 BGP 路由包括隧道封装属性类型长度值 Tunnel Encapsulation Attribute TLV，所述 Tunnel Encapsulation Attribute TLV 包括所述 IPsec SA。

基于第一方面，在可能的实现方式中，所述 BGP 路由包括扩展团体属性，所述扩展团体属性用于携带所述 Export RT。

基于第一方面，在可能的实现方式中，所述第一站点 edge 和所述第二站点 edge 为软件定义的广域网 SD-WAN 中站点 edge。

第二方面，本申请提供了一种安全传输报文的方法，从数据转发面的接收侧来描述，所述方法包括：

广域网中的第二站点出口设备 edge 接收第一站点 edge 通过在所述第一站点 edge 和所述第二站点 edge 之间建立的上层 overlay 端到端隧道发送的第二报文，所述第二报文中包括第一报文以及在所述第一报文外层封装的所述 overlay 端到端隧道的隧道信息，所述 overlay 端到端隧道对应的底层 underlay 隧道包括多段隧道，所述隧道信息包括第一入网点 POP 的第一信息，所述第一站点 edge 为所述 overlay 端到端隧道的入端点，所述第二站点 edge 为所述 overlay 端到端隧道的出端点，所述 overlay 端到端隧道经过所述第一 POP，所述第一报文为通过所述第二站点 edge 与所述第一站点 edge 协商的因特网协议安全协议安全联盟 IPsec SA 对虚拟专用网络 VPN 业务报文进行安全保护所得到的报文；

所述第二站点 edge 对所述第二报文进行解封装，获得第一报文；

所述第二站点 edge 根据所述 IPsec SA 对所述第一报文进行处理，以获得所述 VPN 业务报文。

第二站点 edge 接收到第二报文后，第二报文中包括第一报文和封装在第一报文外层的隧道信息，第二站点 edge 对第二报文进行解封装，获得第一报文，然后根据与第一站点 edge 协商好的 IPsec SA 对第一报文进行处理，获得 VPN 业务报文。第二报文在整个传输过程中，无需 overlay 端到端隧道上的各个 POP 进行加密或解密，只需在第二站点 edge 处进行一次处理即可，提高了传输效率，降低传输延时。

基于第二方面，在可能的实现方式中，所述对所述第一报文进行处理包括：根据所述 IPsec SA，对所述第一报文进行封装安全载荷 ESP 协议解密；和/或，根据所述 IPsec SA 和所述第一报文的认证头 Authentication Header 中携带的认证数据对所述第一报文进行认证。

基于第二方面，在可能的实现方式中，所述隧道信息还包括第二 POP 的第二信息，所述 overlay 端到端隧道经过所述第一 POP 和所述第二 POP，所述第一站点 edge 通过所述第一 POP 接入所述广域网，所述第二站点 edge 通过所述第二 POP 接入所述广域网。

基于第二方面，在可能的实现方式中，所述 overlay 端到端隧道为互联网协议第六版本 IPv6 的段路由 SRv6 隧道，所述第二报文包括 IPv6 头和分段路由头 SRH，所述 IPv6 头的目的地址指向所述第一 POP，所述 SRH 头包括所述第一信息和所述第二信息。

基于第二方面，在可能的实现方式中，所述第一信息为第一 POP 的第一端点段标识 END.SID，所述第一端点段标识 END.SID 关联的操作包括：根据所述 END.SID 的下一跳 SID 匹配从所述第一 POP 到所述第二 POP 之间的上层 overlay SRv6 Policy。

基于第二方面，在可能的实现方式中，所述 overlay 端到端隧道为分段路由多协议标签交换流量工程策略 SR-MPLS TE Policy，所述第二报文包括 MPLS 标签栈，所述 MPLS 标签栈包括所述第一信息和所述第二信息。

基于第二方面，在可能的实现方式中，所述第一信息为所述第一 POP 的第一节点 SID，所述第一节点 SID 关联的操作包括：

根据所述标签栈中所述第一节点 SID 的下一跳 SID 匹配从所述第一 POP 到所述第二 POP 之间的上层 overlay SR MPLS 隧道。

基于第二方面，在可能的实现方式中，所述 overlay 端到端隧道为基于通用网络虚拟化封装 GENEVE 协议封装的隧道，所述第二报文采用 SRv6 in GENEVE 封装。

基于第二方面，在可能的实现方式中，所述 overlay 端到端隧道为基于通用路由封装 GRE 协议封装的隧道，所述第二报文采用 SRv6 over GRE 封装。

基于第二方面，在可能的实现方式中，在所述广域网中的第二站点出口设备 edge 接收第一站点 edge 通过上层 overlay 端到端隧道发送的第二报文之前，所述方法还包括：所述第二站点出口设备 edge 生成边界网关协议 BGP 路由，其中，所述 BGP 路由包括路由类型 RT、所述 IPsec SA、所述第二站点 edge 的标识、以及导出路由目标 Export RT，其中，所述路由类型 RT 指示所述 BGP 路由通告的所述 IPsec SA 用于对与所述 Export RT 匹配的虚拟路由转发 VRF 中的所述 VPN 业务报文进行端到端安全保护；所述第二站点 edge 向所述第一站点 edge 通告所述 BGP 路由。

基于第二方面，在可能的实现方式中，所述 BGP 路由为 BGP 软件定义的广域网 SD-WAN 路由，该 BGP SD-WAN 路由的子地址族为 SD-WAN 子地址族，或者，所述 BGP 路由为 BGP 以太网虚拟专用网络 EVPN 路由，该 BGP EVPN 路由的子地址族为 EVPN 子地址族。

基于第二方面，在可能的实现方式中，所述第二站点 edge 的标识包括所述第二站点 edge 所属的站点标识 site ID 和/或所述第二站点 edge 的节点标识 Node ID。

基于第二方面，在可能的实现方式中，所述 BGP 路由包括网络层可达信息 NLRI，所述 NLRI 包括所述路由类型 RT 和所述第二站点 edge 的标识。

基于第二方面，在可能的实现方式中，所述 BGP 路由包括隧道封装属性类型长度值 Tunnel Encapsulation Attribute TLV，所述 Tunnel Encapsulation Attribute TLV 包括所述 IPsec SA。

基于第二方面，在可能的实现方式中，所述 BGP 路由包括扩展团体属性，所述扩展团体属性用于携带所述 Export RT。

基于第二方面，在可能的实现方式中，所述第一站点 edge 和所述第二站点 edge 为软件定义的广域网 SD-WAN 中站点 edge。

第三方面，本申请提供了一种协商因特网协议安全协议安全联盟 IPsec SA 的方法，从控制面的接收侧来描述，所述方法包括：

广域网中的第一站点出口设备 edge 接收第二站点 edge 通告的边界网关协议 BGP 路由，所述 BGP 路由包括路由类型 RT、所述 IPsec SA、所述第二站点 edge 的标识、以及导出路由目标 ExportRT，其中，所述路由类型 RT 指示所述 BGP 路由通告的所述 IPsec SA 用于对与所述 Export RT 匹配的虚拟路由转发 VRF 中的业务报文进行端到端安全保护；

根据所述路由类型 RT 和所述 Export RT，所述第一站点 edge 将所述 IPsec SA 与所述 VRF 关联。

本申请方案在 BGP 路由中新增了一种路由类型 RT，BGP 路由中携带了 IPsec SA 和导出路由目标 ExportRT，新增的路由类型 RT 用于指示 BGP 路由通告的 IPsec SA 用于对于 ExportRT 匹配的 VRF 中的业务报文进行端到端的安全保护。通过将 BGP 路由在广域网中进行通告，实现了两个站点 edge 之间基于 VRF 粒度的端到端的 IPsec SA 协商，以便后续采用协商好的 IPsec SA 进行 VPN 业务报文的传输，为 VPN 业务报文的传输奠定了基础。

基于第三方面，在可能的实现方式中，所述 BGP 路由为 BGP 软件定义的广域网 SD-WAN 路由，该 BGP SD-WAN 路由的子地址族为 SD-WAN 子地址族，或者，所述 BGP 路由为 BGP 以太网虚拟专用网络 EVPN 路由，该 BGP EVPN 路由的子地址族为 EVPN 子地址族。

基于第三方面，在可能的实现方式中，所述第二站点 edge 的标识包括所述第二站点 edge 所属的站点标识 site ID 和/或所述第二站点 edge 的节点标识 Node ID。

可以理解，第二站点 edge 的标识可以是第二站点标识 site ID 和节点标识 Node ID，通过第二站点标识 site ID 和节点标识 Node ID 可以确定第二站点 edge，第一站点 edge 与第二站点 edge 之间协商约定 IPsec SA。在又一种实现方式中，第二站点 edge 的标识可以是节点标识 Node ID，节点 Node ID 在广域网中是全局唯一的，根据 Node ID 可以确定第二站点 edge，第一站点 edge 与第二站点 edge 之间协商约定 IPsec SA。在又一种实现方式中，第二站点 edge 的标识可以是第二站点标识 site ID，这种情况下，第一站点中的任意一个 edge 接收到第二站点中的任意一个 edge 通告的 BGP 路由，其中 BGP 路由中携带的包括第二站点的标识和 IPsec SA，则表示第一站点与第二站点协商的密钥为 IPsec SA，后续第一站点中的任意一个 edge 与第二站点中的任意一个 edge 之间均可以通过协商的密钥 IPsec SA 对业务报文进行安全保护和传输。

基于第三方面，在可能的实现方式中，所述 BGP 路由包括网络层可达信息 NLRI，所述 NLRI 包括所述路由类型 RT 和所述第二站点 edge 的标识。

基于第三方面，在可能的实现方式中，所述 BGP 路由包括隧道封装属性类型长度值 Tunnel Encapsulation Attribute TLV，所述 Tunnel Encapsulation Attribute TLV 包括所述 IPsec SA。

基于第三方面，在可能的实现方式中，所述 BGP 路由包括扩展团体属性，所述扩展团体属性用于携带所述 Export RT。

基于第三方面，在可能的实现方式中，所述第一站点 edge 和所述第二站点 edge 为软件定义的广域网 SD-WAN 中站点 edge。

第四方面，本申请提供了一种协商因特网协议安全协议安全联盟 IPsec SA 的方法，从控制面的发送侧来描述，所述方法包括：

广域网中的第二站点出口设备 edge 生成边界网关协议 BGP 路由，其中，所述 BGP 路由包括路由类型

RT、所述 IPsec SA、所述第二站点 edge 的标识、以及导出路由目标 ExportRT，其中，所述路由类型 RT 指示所述 BGP 路由通告的所述 IPsec SA 用于对与所述 Export RT 匹配的虚拟路由转发 VRF 中的业务报文进行端到端安全保护；

所述第二站点 edge 向第一站点 edge 通告所述 BGP 路由。

本申请方案在 BGP 路由中新增了一种路由类型 RT，BGP 路由中携带了 IPsec SA 和导出路由目标 ExportRT，新增的路由类型 RT 用于指示 BGP 路由通告的 IPsec SA 用于对于 ExportRT 匹配的 VRF 中的业务报文进行端到端的安全保护。通过将 BGP 路由在广域网中进行通告，实现了两个站点 edge 之间基于 VRF 粒度的端到端的 IPsec SA 协商，以便后续采用协商好的 IPsec SA 进行 VPN 业务报文的传输，为 VPN 业务报文的传输奠定了基础。

基于第四方面，在可能的实现方式中，所述 BGP 路由为 BGP 软件定义的广域网 SD-WAN 路由，该 BGP SD-WAN 路由的子地址族为 SD-WAN 子地址族，或者，所述 BGP 路由为 BGP 以太网虚拟专用网络 EVPN 路由，该 BGP EVPN 路由的子地址族为 EVPN 子地址族。

基于第四方面，在可能的实现方式中，所述第二站点 edge 的标识包括所述第二站点 edge 所属的站点标识 site ID 和/或所述第二站点 edge 的节点标识 Node ID。第二站点 edge 的标识可以是第二站点标识 site ID 和节点标识 Node ID，通过第二站点标识 site ID 和节点标识 Node ID 可以确定第二站点 edge，第一站点 edge 与第二站点 edge 之间协商约定 IPsec SA。在又一种实现方式中，第二站点 edge 的标识可以是节点标识 Node ID，节点 Node ID 在广域网中是全局唯一的，根据 Node ID 可以确定第二站点 edge，第一站点 edge 与第二站点 edge 之间协商约定 IPsec SA。在又一种实现方式中，第二站点 edge 的标识可以是第二站点标识 site ID，这种情况下，第一站点中的任意一个 edge 接收到第二站点中的任意一个 edge 通告的 BGP 路由，其中 BGP 路由中携带的包括第二站点的标识和 IPsec SA，则表示第一站点与第二站点协商的密钥为 IPsec SA，后续第一站点中的任意一个 edge 与第二站点中的任意一个 edge 之间均可以通过协商的密钥 IPsec SA 对业务报文进行安全保护和传输。

基于第四方面，在可能的实现方式中，所述 BGP 路由包括网络层可达信息 NLRI，所述 NLRI 包括所述路由类型 RT 和所述第二站点 edge 的标识。

基于第四方面，在可能的实现方式中，所述 BGP 路由包括隧道封装属性类型长度值 Tunnel Encapsulation Attribute TLV，所述 Tunnel Encapsulation Attribute TLV 包括所述 IPsec SA。

基于第四方面，在可能的实现方式中，所述 BGP 路由包括扩展团体属性，所述扩展团体属性用于携带所述 Export RT。

基于第四方面，在可能的实现方式中，所述第一站点 edge 和所述第二站点 edge 为软件定义的广域网 SD-WAN 中站点 edge。

第五方面，本申请提供了一种安全传输报文的装置，所述装置应用于广域网中的第一站点出口设备 edge，所述装置包括：

接收模块，用于接收虚拟路由转发 VRF 中的虚拟专用网络 VPN 业务报文；

处理模块，用于根据与第二站点 edge 协商的与所述 VRF 关联的因特网协议安全协议安全联盟 IPsecSA 对所述 VPN 业务报文进行安全保护，以得到第一报文；

所述处理模块，用于在所述第一报文外层封装在所述第一站点 edge 到所述第二站点 edge 之间建立的上层 overlay 端到端隧道的隧道信息，以获得第二报文，其中，所述 overlay 端到端隧道对应的底层 underlay 隧道包括多段隧道，所述隧道信息包括第一入网点 POP 的第一信息，所述第一站点 edge 为所述 overlay 端到端隧道的入端点，所述第二站点 edge 为所述 overlay 端到端隧道的出端点，所述 overlay 端到端隧道经过所述第一 POP；

发送模块，用于通过所述 overlay 端到端隧道，向所述第二站点 edge 发送所述第二报文。

基于第五方面，在可能的实现方式中，所述处理模块用于：对所述 VPN 业务报文进行封装安全载荷 ESP 协议加密；和/或，对所述 VPN 业务报文封装认证头 Authentication Header。

基于第五方面，在可能的实现方式中，所述隧道信息还包括第二 POP 的第二信息，所述 overlay 端到端隧道经过所述第一 POP 和所述第二 POP，所述第一站点 edge 通过所述第一 POP 接入所述广域网，所述第二站点 edge 通过所述第二 POP 接入所述广域网。

基于第五方面，在可能的实现方式中，所述 overlay 端到端隧道为互联网协议第六版本 IPv6 的段路由 SRv6 隧道，所述第二报文包括 IPv6 头和分段路由头 SRH，所述 IPv6 头的目的地址指向所述第一 POP，所述 SRH 包括所述第一信息和所述第二信息。

基于第五方面，在可能的实现方式中，所述第一信息为所述第一 POP 的第一端点段标识 END.SID，所述第一端点段标识 END.SID 关联的操作包括：根据所述 END.SID 的下一跳 SID 匹配从所述第一 POP 到所述第二 POP 之间的上层 overlay SRv6 Policy。

基于第五方面，在可能的实现方式中，所述 overlay 端到端隧道为分段路由多协议标签交换流量工程策略 SR-MPLS TE Policy，所述第二报文包括 MPLS 标签栈，所述 MPLS 标签栈包括所述第一信息和所述第二信息。

基于第五方面，在可能的实现方式中，所述第一信息为所述第一 POP 的第一节点 SID，所述第一节点 SID 关联的操作包括：根据所述标签栈中所述第一节点 SID 的下一跳 SID 匹配从所述第一 POP 到所述第二 POP 之间的上层 overlay SR MPLS 隧道。

基于第五方面，在可能的实现方式中，所述 overlay 端到端隧道为基于通用网络虚拟化封装 GENEVE 协议封装的隧道，所述第二报文采用 SRv6 in GENEVE 封装。

基于第五方面，在可能的实现方式中，所述 overlay 端到端隧道为基于通用路由封装 GRE 协议封装的隧道，所述第二报文采用 SRv6 over GRE 封装。

基于第五方面，在可能的实现方式中，所述接收模块还用于，接收所述第二站点 edge 通告的边界网关协议 BGP 路由，所述 BGP 路由包括路由类型 RT、所述 IPsec SA、所述第二站点 edge 的标识、以及导出路由目标 ExportRT，其中，所述路由类型 RT 指示所述 BGP 路由通告的所述 IPsec SA 用于对与所述 Export RT 匹配的所述虚拟路由转发 VRF 中的所述 VPN 业务报文进行端到端安全保护；所述处理模块还用于，根据所述路由类型 RT 和所述 Export RT，将所述 IPsec SA 与所述 VRF 关联。

基于第五方面，在可能的实现方式中，所述 BGP 路由为 BGP 软件定义的广域网 SD-WAN 路由，该 BGP SD-WAN 路由的子地址族为 SD-WAN 子地址族，或者，所述 BGP 路由为 BGP 以太网虚拟专用网络 EVPN 路由，该 BGP EVPN 路由的子地址族为 EVPN 子地址族。

基于第五方面，在可能的实现方式中，所述第二站点 edge 的标识包括所述第二站点 edge 所属的站点标识 site ID 和/或所述第二站点 edge 的节点标识 Node ID。

基于第五方面，在可能的实现方式中，所述 BGP 路由包括网络层可达信息 NLRI，所述 NLRI 包括所述路由类型 RT 和所述第二站点 edge 的标识。

基于第五方面，在可能的实现方式中，所述 BGP 路由包括隧道封装属性类型长度值 Tunnel Encapsulation Attribute TLV，所述 Tunnel Encapsulation Attribute TLV 包括所述 IPsec SA。

基于第五方面，在可能的实现方式中，所述 BGP 路由包括扩展团体属性，所述扩展团体属性用于携带所述 Export RT。

基于第五方面，在可能的实现方式中，所述第一站点 edge 和所述第二站点 edge 为软件定义的广域网 SD-WAN 中站点 edge。

第五方面中的各个功能模块用于实现上述第一方面以及第一方面的任意一种可能的实现方式所述的方法。

第六方面，本申请提供了一种安全传输报文的装置，所述装置应用于广域网中的第二站点 edge，其特征在于，所述装置包括：

接收模块，用于接收第一站点 edge 通过在所述第一站点 edge 和所述第二站点 edge 之间建立的上层 overlay 端到端隧道发送的第二报文，所述第二报文中包括第一报文以及在所述第一报文外层封装的所述 overlay 端到端隧道的隧道信息，所述 overlay 端到端隧道对应的底层 underlay 隧道包括多段隧道，所述隧道信息包括第一入网点 POP 的第一信息，所述第一站点 edge 为所述 overlay 端到端隧道的入端点，所述第二站点 edge 为所述 overlay 端到端隧道的出端点，所述 overlay 端到端隧道经过所述第一 POP，所述第一报文为通过所述第二站点 edge 与所述第一站点 edge 协商的因特网协议安全协议安全联盟 IPsec SA 对虚拟专用网络 VPN 业务报文进行安全保护所得到的报文；

处理模块，用于对所述第二报文进行解封装，获得第一报文；

所述处理模块还用于，根据所述 IPsec SA 对所述第一报文进行处理，以获得所述 VPN 业务报文。

基于第六方面，在可能的实现方式中，所述处理模块用于：根据所述 IPsec SA，对所述第一报文进行封装安全载荷 ESP 协议解密；和/或，根据所述 IPsec SA 和所述第一报文的认证头 Authentication Header 中携带的认证数据对所述第一报文进行认证。

基于第六方面，在可能的实现方式中，所述隧道信息还包括第二 POP 的第二信息，所述 overlay 端到端隧道经过所述第一 POP 和所述第二 POP，所述第一站点 edge 通过所述第一 POP 接入所述广域网，所述

第二站点 edge 通过所述第二 POP 接入所述广域网。

基于第六方面，在可能的实现方式中，所述 overlay 端到端隧道为互联网协议第六版本 IPv6 的段路由 SRv6 隧道，所述第二报文包括 IPv6 头和分段路由头 SRH，所述 IPv6 头的目的地址指向所述第一 POP，所述 SRH 头包括所述第一信息和所述第二信息。

基于第六方面，在可能的实现方式中，所述第一信息为第一 POP 的第一端点段标识 END.SID，所述第一端点段标识 END.SID 关联的操作包括：根据所述 END.SID 的下一跳 SID 匹配从所述第一 POP 到所述第二 POP 之间的上层 overly SRv6 Policy。

基于第六方面，在可能的实现方式中，所述 overlay 端到端隧道为分段路由多协议标签交换流量工程策略 SR-MPLS TE Policy，所述第二报文包括 MPLS 标签栈，所述 MPLS 标签栈包括所述第一信息和所述第二信息。

基于第六方面，在可能的实现方式中，所述第一信息为所述第一 POP 的第一节点 SID，所述第一节点 SID 关联的操作包括：根据所述标签栈中所述第一节点 SID 的下一跳 SID 匹配从所述第一 POP 到所述第二 POP 之间的上层 overly SR MPLS 隧道。

基于第六方面，在可能的实现方式中，所述 overlay 端到端隧道为基于通用网络虚拟化封装 GENEVE 协议封装的隧道，所述第二报文采用 SRv6 in GENEVE 封装。

基于第六方面，在可能的实现方式中，所述 overlay 端到端隧道为基于通用路由封装 GRE 协议封装的隧道，所述第二报文采用 SRv6 over GRE 封装。

基于第六方面，在可能的实现方式中，

所述处理模块还用于，生成边界网关协议 BGP 路由，其中，所述 BGP 路由包括路由类型 RT、所述 IPsec SA、所述第二站点 edge 的标识、以及导出路由目标 ExportRT，其中，所述路由类型 RT 指示所述 BGP 路由通告的所述 IPsec SA 用于对与所述 Export RT 匹配的虚拟路由转发 VRF 中的所述 VPN 业务报文进行端到端安全保护；

发送模块，用于向所述第一站点 edge 通告所述 BGP 路由。

基于第六方面，在可能的实现方式中，所述 BGP 路由为 BGP 软件定义的广域网 SD-WAN 路由，该 BGP SD-WAN 路由的子地址族为 SD-WAN 子地址族，或者，所述 BGP 路由为 BGP 以太网虚拟专用网络 EVPN 路由，该 BGP EVPN 路由的子地址族为 EVPN 子地址族。

基于第六方面，在可能的实现方式中，所述第二站点 edge 的标识包括所述第二站点 edge 所属的站点标识 site ID 和/或所述第二站点 edge 的节点标识 Node ID。

基于第六方面，在可能的实现方式中，所述 BGP 路由包括网络层可达信息 NLRI，所述 NLRI 包括所述路由类型 RT 和所述第二站点 edge 的标识。

基于第六方面，在可能的实现方式中，所述 BGP 路由包括隧道封装属性类型长度值 Tunnel Encapsulation Attribute TLV，所述 Tunnel Encapsulation Attribute TLV 包括所述 IPsec SA。

基于第六方面，在可能的实现方式中，所述 BGP 路由包括扩展团体属性，所述扩展团体属性用于携带所述 Export RT。

基于第六方面，在可能的实现方式中，所述第一站点 edge 和所述第二站点 edge 为软件定义的广域网 SD-WAN 中站点 edge。

第六方面中的各个功能模块用于实现上述第二方面以及第二方面的任意一种可能的实现方式所述的方法。

第七方面，本申请提供了一种协商因特网协议安全协议安全联盟 IPsec SA 的装置，所述装置应用于广域网中的第一站点 edge，所述装置包括：

接收模块，用于接收第二站点 edge 通告的边界网关协议 BGP 路由，所述 BGP 路由包括路由类型 RT、所述 IPsec SA、所述第二站点 edge 的标识、以及导出路由目标 ExportRT，其中，所述路由类型 RT 指示所述 BGP 路由通告的所述 IPsec SA 用于对与所述 Export RT 匹配的虚拟路由转发 VRF 中的业务报文进行端到端安全保护；

处理模块，用于根据所述路由类型 RT 和所述 Export RT，将所述 IPsec SA 与所述 VRF 关联。

基于第七方面，在可能的实现方式中，所述 BGP 路由为 BGP 软件定义的广域网 SD-WAN 路由，该 BGP SD-WAN 路由的子地址族为 SD-WAN 子地址族，或者，所述 BGP 路由为 BGP 以太网虚拟专用网络 EVPN 路由，该 BGP EVPN 路由的子地址族为 EVPN 子地址族。

基于第七方面，在可能的实现方式中，所述第二站点 edge 的标识包括所述第二站点 edge 所属的站点

标识 site ID 和/或所述第二站点 edge 的节点标识 Node ID。

基于第七方面，在可能的实现方式中，所述 BGP 路由包括网络层可达信息 NLRI，所述 NLRI 包括所述路由类型 RT 和所述第二站点 edge 的标识。

基于第七方面，在可能的实现方式中，所述 BGP 路由包括隧道封装属性类型长度值 Tunnel Encapsulation Attribute TLV，所述 Tunnel Encapsulation Attribute TLV 包括所述 IPsec SA。

基于第七方面，在可能的实现方式中，所述 BGP 路由包括扩展团体属性，所述扩展团体属性用于携带所述 Export RT。

基于第七方面，在可能的实现方式中，所述第一站点 edge 和所述第二站点 edge 为软件定义的广域网 SD-WAN 中站点 edge。

第七方面中的各个功能模块用于实现上述第三方面以及第三方面的任意一种可能的实现方式所述的方法。

第八方面，本申请提供了一种协商因特网协议安全协议安全联盟 IPsec SA 的装置，所述装置应用于广域网中的第二站点 edge，所述装置包括：

处理模块，用于生成边界网关协议 BGP 路由，其中，所述 BGP 路由包括路由类型 RT、所述 IPsec SA、所述第二站点 edge 的标识、以及导出路由目标 ExportRT，其中，所述路由类型 RT 指示所述 BGP 路由通告的所述 IPsec SA 用于对与所述 Export RT 匹配的虚拟路由转发 VRF 中的业务报文进行端到端安全保护；

发送模块，用于向第一站点 edge 通告所述 BGP 路由。

基于第八方面，在可能的实现方式中，所述 BGP 路由为 BGP 软件定义的广域网 SD-WAN 路由，该 BGP SD-WAN 路由的子地址族为 SD-WAN 子地址族，或者，所述 BGP 路由为 BGP 以太网虚拟专用网络 EVPN 路由，该 BGP EVPN 路由的子地址族为 EVPN 子地址族。

基于第八方面，在可能的实现方式中，所述第二站点 edge 的标识包括所述第二站点 edge 所属的站点标识 site ID 和所述第二站点 edge 的节点标识 Node ID。

基于第八方面，在可能的实现方式中，所述 BGP 路由包括网络层可达信息 NLRI，所述 NLRI 包括所述路由类型 RT 和/或所述第二站点 edge 的标识。

基于第八方面，在可能的实现方式中，所述 BGP 路由包括隧道封装属性类型长度值 Tunnel Encapsulation Attribute TLV，所述 Tunnel Encapsulation Attribute TLV 包括所述 IPsec SA。

基于第八方面，在可能的实现方式中，所述 BGP 路由包括扩展团体属性，所述扩展团体属性用于携带所述 Export RT。

基于第八方面，在可能的实现方式中，所述第一站点 edge 和所述第二站点 edge 为软件定义的广域网 SD-WAN 中站点 edge。

第八方面中的各个功能模块用于实现上述第四方面以及第四方面的任意一种可能的实现方式所述的方法。

第九方面，本申请提供了一种网络设备，包括存储器和处理器，所述存储器用于存储指令，所述处理器用于执行所述存储器中存储的所述指令，以实现上述第一方面以及第一方面的任意一种可能的实现方式所述的方法，或者，以实现上述第二方面以及第二方面的任意一种可能的实现方式所述的方法，或者，以实现上述第三方面以及第三方面的任意一种可能的实现方式所述的方法，或者，以实现上述第四方面以及第四方面的任意一种可能的实现方式所述的方法。

第十方面，本申请提供了一种系统，包括第一站点出口设备 edge 和第二站点 edge，所述第一站点 edge 用于执行上述第一方面以及第一方面的任意一种可能的实现方式所述的方法，所述第二站点 edge 用于执行上述第二方面以及第二方面的任意一种可能的实现方式所述的方法；或者，所述第一站点 edge 用于执行上述第三方面以及第三方面的任意一种可能的实现方式所述的方法，所述第二站点 edge 用于执行上述第四方面以及第四方面的任意一种可能的实现方式所述的方法。

第十一方面，本申请提供了一种计算机存储介质，其特征在于，包括程序指令，当所述程序指令在处理器上执行时，使得所述处理器实现上述第一方面以及第一方面的任意一种可能的实现方式所述的方法，或者，使得所述处理器实现上述第二方面以及第二方面的任意一种可能的实现方式所述的方法，或者，使得所述处理器实现上述第三方面以及第三方面的任意一种可能的实现方式所述的方法，或者，使得所述处理器实现上述第四方面以及第四方面的任意一种可能的实现方式所述的方法。

第十二方面，本申请提供了一种包括程序指令的计算机程序产品，当所述程序指令在处理器上执行时，使得所述处理器实现上述第一方面以及第一方面的任意一种可能的实现方式所述的方法，或者，使得所述

处理器实现上述第二方面以及第二方面的任意一种可能的实现方式所述的方法，或者，使得所述处理器实现上述第三方面以及第三方面的任意一种可能的实现方式所述的方法，或者，使得所述处理器实现上述第四方面以及第四方面的任意一种可能的实现方式所述的方法。

附图说明

- 图1为本申请提供的一种场景示意图；
图2为本申请提供的一种协商IPsec SA的方法的流程示意图；
图3为本申请提供的一种BGP SD-WAN路由报文的部分结构示意图；
图4为本申请提供的一种BGP EVPN路由报文的部分结构示意图；
图5为本申请提供的一种安全传输报文的方法的流程示意图；
图6A为本申请提供的一种VPN业务报文的结构示意图；
图6B为本申请提供的第一报文的结构示意图；
图6C为本申请提供的第二报文的结构示意图；
图7为本申请提供的一种第二报文的结构示意图；
图8为本申请提供的又一种第二报文的结构示意图；
图9为本申请提供的一种安全传输报文的方法的流程示意图；
图10为本申请提供的一种安全传输报文的装置的结构示意图；
图11为本申请提供的又一种安全传输报文的装置的结构示意图；
图12为本申请提供的一种网络设备的结构示意图。

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。

参见图1，图1为本申请提供的一种场景示意图。在图1所示的软件定义的广域网（software-defined wide-area network, SD-WAN）中，在underlay网络中入网点（point of presence, POP）之间建立SD-WAN隧道，客户终端设备（customer premises equipment, CPE）1与边缘入网点（edge point of presence, EPOP）1之间建立有隧道1，EPOP1与骨干入网点（backbone point of presence, BPOP）1之间建立有隧道2，BPOP1与BPOP2之间建立有隧道3，BPOP2与EPOP2之间建立有隧道4，EPOP2与CPE2之间建立有隧道5，其中，CPE1位于站点1，CPE2位于站点2。每一段隧道的入节点与出节点均基于TNP粒度进行了密钥协商。

在一种应用场景中，根据实际业务需求，业务流（业务报文）需要从CPE1至CPE2，即，业务报文需要跨越多个隧道从CPE1传输至CPE2。首先，CPE1节点按照隧道1上CPE1与EPOP1协商好的密钥对业务报文进行加密，当业务报文传输至EPOP1节点时，EPOP1节点再按照协商好的密钥对报文进行解密；当业务报文到达隧道2时，EPOP1节点按照隧道2上EPOP1与BPOP1协商好的密钥对业务报文进行加密，当业务报文传输至BPOP1节点时，BPOP1节点再按照协商好的密钥对业务报文进行解密；...直至报文传输至隧道5，EPOP2节点按照隧道5上EPOP2与CPE2协商好的密钥对业务报文进行加密，当业务报文传输至CPE2节点时，CPE2节点再按照协商好的密钥对业务报文进行解密，解析报文，获得数据。

对于这种需要跨越多段隧道进行传输的应用场景，需要经过多次加解密，操作繁琐，且消耗了网络设备的计算资源，增加了业务报文的转发延迟。

本申请提供了一种协商因特网协议安全协议（internet protocol security，简称IPsec）安全联盟（security association, SA）的方法，所述方法应用于广域网。IPsec SA是一种安全协议，用于在IP网络上提供数据的机密性、完整性和身份验证。IPsec SA是在两个网络设备之间建立的一组安全参数，用于保护IP数据包的传输。它包括加密算法、身份验证协议、密钥长度、密钥管理和其他安全参数。在IPsec SA建立之前，两个设备必须协商安全参数，以确保它们使用相同的安全参数。一旦建立了IPsec SA，数据包将使用这些安全参数进行加密和身份验证，以确保数据的机密性和完整性。

参见图2所示，图2为本申请提供的一种协商IPsec SA的方法的流程示意图，所述方法包括但不限于以下内容的描述。

S101、广域网中的第二站点出口设备edge生成BGP路由，BGP路由包括路由类型RT、IPsec SA、第二站点edge的标识、以及导出路由目标ExportRT。

BGP 路由中包括路由区分符 (Route Distinguisher, RD) 和导出路由目标 (Export Route Target, 简称 Export RT)。路由区分符 RD 用于标识第二站点 edge 的虚拟路由转发 (virtual routing forwarding, VRF), 导出路由目标 Export RT 用于进行第二站点 edge 的 VRF 匹配。

BGP 路由中还包括第二站点 edge 的标识。在一种实现方式中, 第二站点 edge 的标识包括第二站点 edge 所属的站点标识 site ID 和第二站点 edge 的节点标识 Node ID, 即, 可以通过站点标识和节点标识来确定 edge。在又一种实现方式中, 广域网中的节点标识具有全局唯一性, 这种情况下, 第二站点 edge 的标识可以只包括节点标识, 即, 通过节点标识可以唯一确定 edge。在又一种实现方式中, 第二站点 edge 的标识可以是第二站点标识 site ID, 这种情况下, 第一站点中的任意一个 edge 接收到第二站点中的任意一个 edge 通告的 BGP 路由, 其中 BGP 路由中携带的包括第二站点的标识和 IPsec SA, 则表示第一站点与第二站点之间协商的密钥为 IPsec SA, 后续第一站点中的任意一个 edge 与第二站点中的任意一个 edge 之间均可以通过协商的密钥 IPsec SA 对业务报文进行安全保护和传输。

BGP 路由中还包括路由类型 (Route Type, RT) 和 IPsec SA, 路由类型 RT 指示 BGP 路由通告的 IPsec SA 用于对与导出路由目标 Export RT 匹配的虚拟路由转发 VRF 中的业务报文进行端到端安全保护。比如, 若与导出路由目标 Export RT 匹配的 VRF 是第一站点 edge 的 VRF, 则路由类型 RT 指示 BGP 路由通告的 IPsec SA 用于对第二站点 edge 与第一站点 edge 之间的业务报文进行端到端的安全保护。

可选的, BGP 路由可以为 BGP SD-WAN 路由, 该 BGP 路由的子地址族为 SD-WAN 子地址族, BGP 路由也可以为 BGP 以太网虚拟专用网络 (ethernet virtual private network, EVPN) 路由, 该 BGP 路由的子地址族为 EVPN 子地址族。BGP 路由还可以是其他路由, 其子地址族可以为其他子地址族, 本申请不做限定。

BGP 路由中包括网络层可达信息 (network layer reachability information, NLRI), 其中, 路由类型 RT、路由区分符 RD 和第二站点 edge 的标识均位于 NLRI 中。例如, 参见图 3, 图 3 为本申请提供的一种 BGP SD-WAN 路由的部分结构示意图, 图 3 中, Route Type 表示路由类型 RT, 其长度可以为 2 个字节, 在 SD-WAN 子地址族中, 可以定义路由类型为 2, Route Distinguisher 表示路由区分符 RD, 其长度可以为 8 个字节, 使用 SD-WAN-Color 来表示站点标识, 长度可以为 4 个字节, 使用 SD-WAN-Node-ID 来表示节点标识, 长度可以为 4 个字节或 16 个字节。又例如, 参见图 4, 图 4 为本申请提供的一种 BGP EVPN 路由的部分结构示意图, 图 4 中, 各个字段与图 3 示意图中的各个字段含义均相同, 所不同的是, 在 EVPN 子地址族中, 定义路由类型 RT 为 10。需要说明的是, 这里定义路由类型 RT 为 2 仅仅是 SD-WAN 子地址族中的一个示例, 在 SD-WAN 地址族中还可以使用其他数值来表示新增的路由类型, 定义路由类型 RT 为 10 仅仅是 EVPN 子地址族的一种举例, 在 EVPN 地址族中还可以使用其他数值来表示新增的路由类型, 本申请不做具体限定。

BGP 路由中还包括类型长度值 (type-length-value, 简称 TLV), 具体的, BGP 路由中包括隧道封装属性 (Tunnel Encapsulation Attribute, TEA) TLV, 其中, TEA TLV 中包括 IPsec SA, 即 IPsec SA 携带在了 BGP 路由的 TEA TLV 字段中, 具体的, IPsec SA 携带在了 TEA TLV 的子 TLV 中。BGP 路由中还包括扩展团体属性 TLV, 扩展团体属性 TLV 中包括导出路由目标 Export RT, 即 Export RT 携带在了 BGP 路由的扩展团体属性 TLV 字段中。需要说明的是, 这里 IPsec SA 和 Export RT 的位置是一种举例, IPsec SA 和 Export RT 还可以携带在 BGP 路由的其他 TLV 字段中, 本申请不做具体限定。

例如, 在图 1 所示的广域网场景示意图中, 第二站点 edge 可以是 CPE1 或者 CPE2。

S102、第二站点 edge 向第一站点 edge 通告 BGP 路由。

第二站点 edge 在广域网中通告 BGP 路由。例如, 在图 1 所示的广域网中, 假设第二站点 edge 为 CPE1, CPE1 生成 BGP 路由后, 可以通过区域路由反射器 (route reflector, RR) 将 BGP 路由反射至 EPOP1, EPOP1 通过管理服务提供商 (managed service provider, MSP) RR 将 BGP 路由反射至 BPOP1、BPOP2 和 EPOP2, EPOP2 再通过区域 RR 将 BGP 路由反射至 CPE2, 从而实现 BGP 路由的通告。

广域网中的第一站点 edge 接收到第二站点 edge 通告的 BGP 路由。例如, 图 1 中, 若第二站点 edge 为 CPE1, 则第一站点 edge 可以为 CPE2; 若第二站点 edge 为 CPE2, 则第一站点 edge 可以为 CPE1。

S103、根据路由类型 RT 和 Export RT, 第一站点 edge 将 IPsec SA 与 VRF 关联。

第一站点 edge 接收到第二站点 edge 通告的 BGP 路由, 根据 BGP 路由中的路由类型 RT 和导出路由目标 Export RT, 将 IPsec SA 与 VRF 关联。具体的, Export RT 用于进行第二站点 edge 的 VRF 匹配, 路由类型 RT 指示 BGP 路由通告的 IPsec SA 是用于对与 Export RT 匹配的 VRF 中的业务报文进行端到端的安全保护, 因此, 第一站点 edge 接收到 BGP 路由后, 先确定自身站点的 VRF 与 Export RT 是否匹配, 在匹配

的情况下，第一站点 edge 将 IPsec SA 与第一站点 edge 的 VRF 关联，因为 IPsec SA 与第二站点 edge 也是关联的，因此可以理解为，第一站点 edge 的 VRF、第二站点 edge 的 VRF 均是与 IPsec SA 关联的，在不匹配的情况下，第一站点 edge 与 IPsec SA 不进行关联。

在一种实现方式中，可以设置匹配策略如下。广域网中的各个 edge 中可以设置有导入路由目标和导出路由目标 Export RT，其中，导入路由目标是存储在 edge 本地的，导出路由目标是携带在 BGP 路由中的。第二站点 edge 发送的 BGP 路由中携带的是导出路由目标，第一站点 edge 接收到第二站点发送的 BGP 路由后，将 BGP 路由中的导出路由目标与第一站点 edge 本地存储的导入路由目标做比较，若两者一致，则第一站点 edge 的 VRF 与 BGP 路由中的 Export RT 相匹配，则第一站点 edge 将 BGP 路由中的 IPsec SA 与第一站点 edge 的 VRF 进行关联。若两者不一致，则第一站点 edge 的 VRF 与 BGP 路由中的 Export RT 不匹配，IPsec SA 与第一站点 edge 的 VRF 不进行关联。例如，第二站点 edge 发送的 BGP 路由中携带的 Export RT 为 100，第一站点 edge 本地的导入路由目标为 100，第一站点 edge 接收到 BGP 路由后，将 Export RT 与本地的导入路由目标作比较，经比较，两者一致，则第一站点 edge 将 BGP 路由中携带的 IPsec SA 与第一站点 edge 的 VRF 进行关联。关于匹配策略这里仅仅是其中一种可能的实现方式，匹配策略还可以是其他实现方式，本申请不做限定。

本申请所述方法可以应用于广域网，比如可以应用于软件定义的广域网 SD-WAN，第一站点 edge 和第二站点 edge 可以为 SD-WAN 中的站点 edge。本申请所述方法还可以应用于其他广域网，本申请不做限定。

实际应用中，第一站点 edge 和第二站点 edge 可以根据实际业务需求和业务流来确定，第一站点 edge 的导入路由目标和导出路由目标、以及第二站点 edge 的导入路由目标和导出路由目标均可以按照实际业务需求来设置。

可以理解，经过 BGP 路由的通告，第一站点 edge 的 VRF、第二站点 edge 的 VRF 均与 IPsec SA 进行了关联，即，第一站点 edge 与第二站点 edge 之间协商好了传输业务报文所使用的 IPsec SA，则后续第一站点 edge 与第二站点 edge 之间传输业务报文时，可以基于协商好的 IPsec SA 来对业务报文进行安全保护，通过虚拟路由转发 VRF 来传输 VPN 业务报文，从而实现第一站点 edge 与第二站点 edge 之间端到端的隧道传输，只需一次安全保护和一次解封装处理即可，降低传输延时。

可以看到，本申请提供了一种协商 IPsec SA 的方法，在 BGP 路由中新增一种路由类型，并在 BGP 路由中携带 IPsec SA 和导出路由目标，新增的路由类型用于指示 BGP 路由通告的 IPsec SA 用于对与导出目标路由匹配的 VRF 中的业务报文进行端到端的安全保护，新增的路由类型实现了基于 VRF 粒度的 IPsec SA 协商。通过 BGP 路由的通告，使得第一站点 edge 与第二站点 edge 之间协商好了一种 IPsec SA 方法，以便后续第一站点 edge 与第二站点 edge 之间传输业务报文时，可以基于协商好的 IPsec SA 方法对业务报文进行安全保护，并通过虚拟路由转发 VRF 的方式传输 VPN 业务报文。

在上述提供的协商 IPsec SA 方法的基础上，本申请还提供了一种安全传输报文的方法。参见图 5，图 5 为本申请提供的一种安全传输报文的方法的流程示意图，所述方法应用于广域网，所述方法包括但不限于以下内容的描述。

S201、广域网中的第一站点出口设备 edge 接收虚拟路由转发 VRF 中的虚拟专用网络 VPN 业务报文。

广域网中的第一站点出口设备 edge 接收到 VRF 中的 VPN 业务报文，其中，VPN 业务报文可以由控制器下发至第一站点 edge 的，也可以是由广域网中的其他网络设备发送至第一站点 edge 的。

在图 1 所示的场景示意图中，第一站点 edge 可以是 CPE1 或者 CPE2。

S202、第一站点 edge 根据与第二站点 edge 协商的与 VRF 关联的因特网协议安全协议安全联盟 IPsecSA 对 VPN 业务报文进行安全保护，得到第一报文。

通过 BGP 路由通告，第一站点 edge 与第二站点 edge 之间协商好了 IPsecSA，且第一站点 edge 的 VRF、第二站点 edge 的 VRF 均与 IPsecSA 进行了关联，IPsecSA 用于对第一站点 edge 的 VRF 与第二站点 edge 的 VRF 之间的业务报文进行端到端保护。基于此，第一站点 edge 接收到 VRF 中的 VPN 业务报文之后，第一站点 edge 根据与第二站点 edge 协商好的与 VRF 关联的 IPsecSA 对 VPN 业务报文进行安全保护，获得第一报文。

在一种实现方式中，对 VPN 业务报文进行安全保护包括对 VPN 业务报文进行封装安全载荷（encapsulate security payload，ESP）协议加密。在一种实现方式中，对 VPN 业务报文进行安全保护包括对 VPN 业务报文封装认证头（Authentication Header，AH）。在一种实现方式中，对 VPN 业务报文进行安

全保护包括对 VPN 业务报文进行 ESP 协议加密和对 VPN 业务报文封装认证头 AH。对 VPN 业务报文进行安全保护还可以通过其他方式实现，本申请不做限定。

S203、第一站点 edge 在第一报文外部封装在第一站点 edge 到第二站点 edge 之间建立的上层 overlay 端到端隧道的隧道信息，获得第二报文。

第一站点 edge 在第一报文外部封装由第一站点 edge 到第二站点 edge 之间建立的上层 overlay 端到端隧道的隧道信息，获得第二报文。其中，第一站点 edge 到第二站点 edge 之间的 overlay 端到端隧道对应的底层 underlay 隧道包括多段隧道。例如，图 1 所示的场景示意图中，若第一站点 edge 为 CPE1，第二站点 edge 为 CPE2，则第一站点 edge 到第二站点 edge 之间的 overlay 端到端隧道对应的底层 underlay 隧道包括隧道 1（CPE1 至 EPOP1）、隧道 2（EPOP1 至 BPOP1）、隧道 3（BPOP1 至 BPOP2）、隧道 4（BPOP2 至 EPOP2）和隧道 5（EPOP2 至 CPE2）。

overlay 端到端隧道上包括至少一个入网点 POP，隧道信息中包括至少一个入网点的信息。在一种示例中，overlay 端到端隧道上包括一个入网点 POP，为了便于描述，称为第一入网点 POP，其中，第一站点 edge 为 overlay 端到端隧道的入端点，第二站点 edge 为 overlay 端到端隧道的出端点，overlay 端到端隧道经过第一入网点 POP，第一入网点 POP 可以为 EPOP，也可以为 BPOP，本申请不做限定。overlay 端到端隧道的隧道信息中包括第一入网点的第二信息。

在又一种示例中，overlay 端到端隧道上包括多个入网点 POP，多个入网点 POP 包括第一入网点 POP 和第二入网点 POP，其中，第一站点 edge 为 overlay 端到端隧道的入端点，第二站点 edge 为 overlay 端到端隧道的出端点，第一站点 edge 通过第一 POP 接入广域网，第二站点 edge 通过第二 POP 接入广域网。例如，在图 1 所示的场景示意图中，若第一站点 edge 为 CPE1，第二站点 edge 为 CPE2，则第一站点 edge 到第二站点 edge 之间的 overlay 端到端隧道上包括多个入网点，第一站点 edge 通过 EPOP1 接入广域网，第二站点 edge 通过 EPOP2 接入广域网，则 EPOP1 为第一 POP，EPOP2 为第二 POP。overlay 端到端隧道的隧道信息中包括第一入网点的第二信息和第二入网点的第二信息。

在一种实现方式中，overlay 端到端隧道为互联网协议第六版本（internet protocol version 6，IPv6）的段路由 SRv6 隧道，则第一站点 edge 在第一报文外部封装 SRv6 隧道的隧道信息，获得第二报文。第二报文中包括 IPv6 头和分段路由头（segment routing header，SRH），在 overlay 端到端隧道包括第一入网点和第二入网点的情况下，IPv6 头的目的地址指向第一入网点，SRH 中包括第二信息和第三信息。

例如，参见图 6A 至图 6C 所示，图 6A 至图 6C 为本申请提供的一种示例图。图 6A 表示的是 VPN 业务报文，包括报文头 Inner IP Hdr 和负荷 Inner Payload。图 6B 表示的是第一报文，第一报文是对 VPN 业务报文进行 ESP 协议加密后获得的。图 6C 表示的是第二报文，第二报文是在第一报文外部封装第一站点 edge 到第二站点 edge 之间的 SRv6 隧道的隧道信息后获得的，其中，IPv6 Hdr（Src IP，Dst IP）表示 IPv6 报文头，SRH（...，vpnsid）表示分段路由头 SRH，IPv6 报文头和 SRH 组成部分为 overlay 端到端隧道的隧道信息。

又例如，在图 1 所示的场景示意图中，假设 CPE1 为第一站点 edge，CPE2 为第二站点 edge，CPE1 至 CPE2 之间的 overlay 端到端隧道为 SRv6 隧道，则 CPE1 在第一报文外部封装 CPE1 至 CPE2 之间的 SRv6 隧道的隧道信息，获得第二报文。如图 7 所示，图 7 为本申请提供的一种示意图。在 CPE1 处时，第二报文中，IPv6 Hdr（cpe1，epop1-sid）为 IPv6 报文头，SRH（vpnsid，epop2-sid，bpop2-sid，bpop1-sid，epop1-sid，）为分段路由头 SRH，其中，epop1-sid 表示 CPE1 的第一端点段标识 END.SID，bpop1-sid 表示 BPOP1 的第一端点段标识 END.SID，bpop2-sid 表示 BPOP2 的第一端点段标识 END.SID，epop2-sid 表示 EPOP2 的第一端点段标识 END.SID，vpnsid 是在 BGP 路由通告时由 CPE2 生成的，vpnsid 与 CPE2 的 VRF 是关联的。其中，EPOP1 为第一入网点 POP，EPOP1 的第一端点段标识 epop1-sid 为第一入网点 POP 的第二信息，EPOP2 为第二入网点 POP，EPOP2 的第一端点段标识 epop2-sid 为第二入网点 POP 的第三信息，EPOP1 的第一端点段标识 epop1-sid 关联的操作包括：根据 epop1-sid 的下一跳 SID 匹配从第一 POP 到第二 POP 之间的上层 overly SRv6 策略 Policy。从图 7 所示出的各个 POP 点处的报文可以看出段标识 END.SID 关联的操作。

上层 overlay 网络是在底层 underlay 网络的基础上建立的，第二报文通过 overlay 端到端隧道进行传输时，实际是在底层 underlay 网络上进行传输的，只是上层 overlay 网络不感知报文在底层 underlay 网络是怎样传输的。因此，需要在第二报文的外层再封装上 underlay 隧道的隧道信息，封装了 underlay 隧道的隧道信息的报文通过 overlay 端到端隧道进行传输（实际封装了 underlay 隧道的隧道信息的报文是在底层 underlay 隧道上传输的。）例如，在图 1 所示的场景中，由于广域网为 SD-WAN 广域网，报文在进行传输时，需要穿越运营商网络，运营商网络中的设备无法识别上层 overly IPv6 地址，因此，在外层又封装了一

层底层 underlay 隧道的报文头 underlay IP。

在一种实现方式中，overlay 端到端隧道为分段路由多协议标签交换流量工程（segment routing multi-protocol label switching traffic engine, SR-MPLS TE）策略 Policy，则第二报文中包括 MPLS 标签栈，MPLS 标签栈包括第一 POP 的第一信息和第二 POP 的第二信息。其中，第一信息为第一 POP 的第一节点 SID，第一节点 SID 关联的操作包括：根据标签栈中第一节点 SID 的下一跳 SID 匹配从第一 POP 到第二 POP 之间的上层 overlay SR MPLS 隧道。

例如，在图 1 所示的场景示意图中，假设 CPE1 为第一站点 edge，CPE2 为第二站点 edge，CPE1 至 CPE2 之间的 overlay 端到端隧道为 SR-MPLS TE Policy，则 CPE1 在第一报文外部封装 CPE1 至 CPE2 之间的 SR-MPLS TE Policy 信息，获得第二报文。参见图 8 所示，图 8 为本申请提供的一种示意图。在 CPE1 处时，第二报文中，(epop1-sid, bpop1-sid, bpop2-sid, epop2-sid, cpe2-sid) 表示 overlay 端到端隧道的隧道信息，也即 MPLS 标签栈，其中，epop1-sid 表示 EPOP1 的第一节点 SID，bpop1-sid 表示 BPOP1 的第一节点 SID，bpop2-sid 表示 BPOP2 的第一节点 SID，epop2-sid 表示 EPOP2 的第一节点 SID，cpe2-sid 表示 CPE2 的第一节点 SID。EPOP1 为第一入网点 POP，EPOP1 的第一节点段标识 epop1-sid 为第一入网点 POP 的第一信息，EPOP2 为第二入网点 POP，EPOP2 的第一节点段标识 epop2-sid 为第二入网点 POP 的第二信息。第一节点 SID 关联的操作包括：根据标签栈中第一节点 SID 的下一跳 SID 匹配从第一 POP 到第二 POP 之间的上层 overlay SR MPLS 隧道，从图 8 所示出的各个 POP 点处的报文可以看出节点段标识 SID 所关联的操作。图 8 报文中的 underlay IP 为 underlay 隧道的隧道信息。

在又一种实现方式中，overlay 端到端隧道为 SRv6 隧道，则第二报文可以基于通用网络虚拟化封装（generic network virtualization encapsulation, GENEVE）协议进行隧道封装，则第二报文采用 SRv6 in GENEVE 封装。示例性的，第二报文包括：外层 IP 头、用户数据报协议（user datagram protocol, UDP）头、GENEVE 封装、SRH、ESP 和净荷，其中，所述净荷包括前述 VPN 业务报文；所述 GENEVE 封装中包括所述 VPN 业务报文所承载的 VPN 业务的 VPN 标识。在一个示例中，所述 SRH 和 ESP 之间还可以包括 metadata 字段，用于承载业务意图信息。当然，第二报文也可以采用 SRv6 over GENEVE 封装，SRv6 over GENEVE 封装相对于 SRv6 in GENEVE 封装而言，区别在于在 GENEVE 封装和 SRH 之间还包括 IPv6 头，SRv6 over GENEVE 封装相对于 SRv6 in GENEVE 封装的封装开销大，但是 SRv6 over GENEVE 封装符合 SRv6 的标准封装格式。

在又一种实现方式中，overlay 端到端隧道为基于通用路由封装（generic routing encapsulation, GRE）协议封装的隧道，则第二报文采用 SRv6 over GRE 封装。在一个示例中，所述第二报文包括：外层 IP 头、UDP 头、外层 GRE 封装、IPv6 头、SRH、内层 GRE 封装、ESP 和净荷，其中，所述净荷包括前述 VPN 业务报文；所述内层 GRE 封装中包括所述 VPN 业务报文所承载的 VPN 业务的 VPN 标识。VPN 标识携带在内层 GRE 封装中，第二报文在网络中传输时，overlay 端到端隧道所经过的中间节点不解析所述 VPN 标识（VPN identifier, VNI），即中间节点不感知 VPN。在一个示例中，所述 SRH 和内层 GRE 封装之间还可以包括 metadata 字段，用于承载业务意图信息。

本申请实施例中的业务意图信息，可以包括指示业务意图的一种或者多种信息。在一个示例中，所述业务意图信息可以包括服务质量参数，所述服务质量参数包括但不限于时延、丢包、抖动、带宽利用率以及误码率等其中一个或者多个参数。在又一个示例中，所述业务意图参数可以包括由站点 edge1 到达站点 edge2 的端到端路径所需满足的网关约束信息，网关约束信息包括但不限于需要经过的网关和/或需要绕行的网关。

S204、第一站点 edge 通过 overlay 端到端隧道向第二站点 edge 发送第二报文。

第一站点 edge 通过 overlay 端到端隧道向第二站点 edge 发送第二报文。在可能的实现方式中，第一站点 edge 通过 SRv6 隧道或者 SR-MPLS TE Policy，向第二站点 edge 发送第二报文。

需要说明的是，第一站点 edge 与第二站点 edge 之间的各个入网点 POP 不感知第二报文，不对第二报文进行解密，只按照 overlay 端到端隧道的隧道信息进行转发，直至第二报文到达第二站点 edge。因此，业务报文在传输过程中，只需在第一站点 edge 处进行一次安全保护，其他各个入网点 pop 无需进行解密，降低了计算资源的消耗，提高了转发效率，降低了传输延时。

本实施例提供的安全传输报文的方法可以应用于 SD-WAN 中，第一站点 edge 和第二站点 edge 为 SD-WAN 中的站点 edge，所述方法也可以应用于其他广域网中，本申请不做限定。

本申请方案在 BGP 路由中新增了一种路由类型 RT，BGP 路由中携带了 IPsec SA 和导出路由目标 ExportRT，新增的路由类型 RT 用于指示 BGP 路由通告的 IPsec SA 用于对于 ExportRT 匹配的 VRF 中的业

务报文进行端到端的安全保护。通过将 BGP 路由在广域网中进行通告,实现了两个站点 edge 之间基于 VRF 粒度的端到端的 IPsec SA 协商,以便后续采用协商好的 IPsec SA 进行 VPN 业务报文的传输,为 VPN 业务报文的传输奠定了基础。相对于现有基于 TNP 粒度的 IPsec SA 协商而言,第一站点 edge 与第二站点 edge 之间的各个入网点 POP 不感知内层 VPN 业务报文,通过两个站点 edges 之间的端到端一次加解密,降低了计算资源的消耗,提高了转发效率,降低了传输延时。

在上述协商 IPsecSA 方法与安全传输报文的方法的基础上,本申请还提供了一种安全传输报文的方法。参见图 9,图 9 为本申请提供的一种安全传输报文的方法的流程示意图,所述方法包括但不限于以下内容的描述。

S301、广域网中的第二站点 edge 接收第一站点 edge 通过在第一站点 edge 和第二站点 edge 之间建立的上层 overlay 端到端隧道发送的第二报文,第二报文中包括第一报文以及在第一报文外层封装的 overlay 端到端隧道的隧道信息。

本实施例提供中,安全传输报文的方法可以应用于 SD-WAN 中,第一站点 edge 和第二站点 edge 为 SD-WAN 中的站点 edge,所述方法也可以应用于其他广域网中,本申请不做限定。

第二站点出口设备 edge 接收第一站点 edge 通过在第一站点 edge 和第二站点 edge 之间建立的上层 overlay 端到端隧道发送的第二报文。其中,第一站点 edge 和第二站点 edge 之间建立的上层 overlay 端到端隧道对应的底层 underlay 隧道包括多段隧道。例如,参见图 1 所示的场景示意图,第一站点 edge 可以是 CPE1,第二站点 edge 可以是 CPE2;或者,第一站点 edge 可以是 CPE2,第二站点 edge 可以是 CPE1。CPE1 与 CPE2 之间建立的 overlay 端到端隧道对应的底层 underlay 隧道包括多段隧道,具体包括:隧道 1 (CPE1 至 EPOP1)、隧道 2 (EPOP1 至 BPOP1)、隧道 3 (BPOP1 至 BPOP2)、隧道 4 (BPOP2 至 EPOP2) 和隧道 5 (EPOP2 至 CPE2)。

overlay 端到端隧道上包括至少一个入网点 POP,隧道信息中包括至少一个入网点的信息。在一种示例中,overlay 端到端隧道上包括一个第一入网点 POP,则隧道信息中包括第一入网点的的第一信息。在又一种示例中,overlay 端到端隧道上包括多个入网点 POP,多个入网点 POP 包括第一入网点 POP 和第二入网点 POP,则隧道信息中包括第一入网点的的第一信息和第二入网点的的第二信息。其中,第一站点 edge 为 overlay 端到端隧道的入端点,第二站点 edge 为 overlay 端到端隧道的出端点,第一站点 edge 通过第一 POP 接入广域网,第二站点 edge 通过第二 POP 接入广域网。

在一种实现方式中,overlay 端到端隧道为 SRv6 隧道,第二站点 edge 接收第一站点 edge 通过 SRv6 隧道发送的第二报文,第二报文中包括第一报文以及在第一报文外层封装的 SRv6 隧道的隧道信息。其中,第一报文为通过第二站点 edge 与第一站点 edge 协商好的 IPsecSA 对 VPN 业务报文进行安全保护所得到的报文,SRv6 隧道的隧道信息包括 IPv6 头和分段路由头 SRH,IPv6 头的目的地址指向第一 POP,SRH 头包括第一信息和第二信息。关于业务报文、第一报文以及第二报文的格式,可以参考图 6A 至图 6C 所示的示意图,为了说明书的简洁,在此不再赘述。

在一种实现方式中,overlay 端到端隧道为 SR-MPLS TE Policy,第二报文中包括第一报文以及在第一报文外层封装的 SR-MPLS TE Policy 信息。其中,SR-MPLS TE Policy 信息包括 MPLS 标签栈,MPLS 标签栈包括第一 POP 的第一信息和第二 POP 的第二信息。关于第二报文的格式,可以参见上述方法实施例的描述,为了说明书的简洁,在此不再赘述。

在可能的实现方式中,第二报文中还可以包括底层 underlay 隧道的报文头。例如,上述图 1 所示的 SD-WAN 场景中,由于报文在进行传输时需要穿越运营商网络,运营商网络中的设备无法识别上层 overly IPv6 地址,因此,在外层又封装了一层底层 underlay 隧道的报文头 underlay IP。

S302、第二站点 edge 对第二报文进行解封装,获得第一报文。

第二站点 edge 对第二报文进行解封装,获得第一报文。在一种实现方式中,overlay 端到端隧道为 SRv6 隧道,第二报文中包括第一报文和 SRv6 隧道的隧道信息,则第二站点 edge 对第二报文进行解封装,去掉了 SRv6 隧道的隧道信息,获得第一报文。第一报文格式的示意图如图 6B 所示,这里不再赘述。

在一种实现方式中,overlay 端到端隧道为 SR-MPLS TE Policy,第二报文中包括第一报文以及在第一报文外层封装的 SR-MPLS TE Policy 信息,则第二站点 edge 对第二报文进行解封装,去掉了 MPLS SR-TE 隧道的隧道信息,获得第一报文。第一报文格式的示意图如图 6B 所示,这里不再赘述。

在一种实现方式中,overlay 端到端隧道为 GENEVE 协议封装的隧道,第二报文采用 SRv6 in GENEVE 封装,则第二站点 edge 对第二报文进行解封装,去掉了 SRv6 in GENEVE 封装的报文头,获得第一报文。

第一报文格式的示意图如图 6B 所示, 这里不再赘述。

在又一种实现方式中, overlay 端到端隧道为基于 GRE 协议封装的隧道, 第二报文采用 SRv6 over GRE 封装, 则第二站点 edge 对第二报文进行解封装, 去掉了 SRv6over GRE 封装的报文头, 获得第一报文。第一报文格式的示意图如图 6B 所示, 这里不再赘述。

S303、第二站点 edge 根据 IPsecSA 对第一报文进行处理, 以获得虚拟专用网络 VPN 业务报文。

在一种实现方式中, 第二站点 edge 根据 IPsecSA 对第一报文进行 ESP 协议处理, 获得 VPN 业务报文。在一种实现方式中, 第二站点 edge 根据 IPsecSA 和第一报文的认证头 AH 中携带的认证数据对第一报文进行认证, 获得 VPN 业务报文。在一种实现方式中, 第二站点 edge 根据 IPsecSA 对第一报文进行 ESP 协议解密, 以及根据 IPsecSA 和第一报文的认证头 AH 中携带的认证数据对第一报文进行认证, 获得 VPN 业务报文。

需要说明的是, 可以是第一站点 edge 生成 BGP 路由, 将 BGP 路由通告第二站点 edge, 也可以是第二站点 edge 生成 BGP 路由, 将 BGP 路由通告至第一站点 edge, 两种方式都可以实现将第一站点 edge 的 VRF、第二站点 edge 的 VRF 均与 IPsec SA 关联。对于两种方式中的任意一种方式实现第一站点 edge 的 VRF、第二站点 edge 的 VRF 与 IPsec SA 关联后, 第一站点 edge 可以对 VPN 业务报文基于协商好的 IPsec SA 进行安全保护和封装, 然后发送至第二站点 edge, 由第二站点 edge 根据协商好的 IPsec SA 进行解封装和解密, 获得 VPN 业务报文。

可以看到, 本申请提供了一种安全传输报文的方法, 通过 BGP 路由通告, 使得第一站点 edge 与第二站点 edge 之间协商好了 IPsec SA, 并将 IPsec SA 与第一站点 edge 的 VRF、第二站点 edge 的 VRF 进行了关联。在进行跨越多个隧道场景的 VPN 业务报文传输时, 只需在第一站点 edge 处根据协商好的 IPsec SA 对 VPN 业务报文进行安全保护, 得到第一报文, 然后在第一报文外部封装上第一站点 edge 与第二站点 edge 之间建立的 overlay 端到端隧道的隧道信息, 获得第二报文, 将第二报文通过 overlay 端到端隧道发送至第二站点 edge。

在整个跨越多个 underlay 隧道传输的场景中, 只需在第一站点 edge 处进行一次 IPsec SA 安全保护, 在第二站点 edge 处进行一次 IPsec SA 处理, 中间经过的各个入网点无需对报文进行加密或解密, 只需按照隧道信息转发即可。因此, 实施本申请实施例, 降低了网络节点的计算资源的消耗, 提高了转发效率, 降低了传输延时。

上述为本申请提供的方法实施例的描述, 下面为本申请实施例提供的与方法实施例对应的装置实施例。

参见图 10, 图 10 为本申请提供实施例的一种安全传输报文的装置 600 的结构示意图, 安全传输报文的装置 600 可以配置为广域网中的第一站点 edge, 所述装置 600 包括:

接收模块 610, 用于接收虚拟路由转发 VRF 中的虚拟专用网络 VPN 业务报文;

处理模块 620, 用于根据与第二站点 edge 协商的与 VRF 关联的因特网协议安全协议安全联盟 IPsecSA 对 VPN 业务报文进行安全保护, 以得到第一报文;

处理模块 620, 还用于在第一报文外层封装在第一站点 edge 到第二站点 edge 之间建立的上层 overlay 端到端隧道的隧道信息, 以获得第二报文, 其中, overlay 端到端隧道对应的底层 underlay 隧道包括多段隧道, 隧道信息包括第一入网点 POP 的第一信息, 第一站点 edge 为 overlay 端到端隧道的入端点, 第二站点 edge 为 overlay 端到端隧道的出端点, overlay 端到端隧道经过第一 POP;

发送模块 630, 用于通过 overlay 端到端隧道, 向第二站点 edge 发送第二报文。

在可能的实现方式中, 处理模块 620 用于: 对 VPN 业务报文进行封装安全载荷 ESP 协议加密; 和/或, 对 VPN 业务报文封装认证头 Authentication Header。

在可能的实现方式中, 隧道信息还包括第二 POP 的第二信息, overlay 端到端隧道经过第一 POP 和第二 POP, 第一站点 edge 通过第一 POP 接入广域网, 第二站点 edge 通过第二 POP 接入广域网。

在可能的实现方式中, overlay 端到端隧道为互联网协议第六版本 IPv6 的段路由 SRv6 隧道, 第二报文包括 IPv6 头和分段路由头 SRH, IPv6 头的目的地址指向第一 POP, SRH 包括第一信息和第二信息。

在可能的实现方式中, 第一信息为第一 POP 的第一端点段标识 END.SID, 第一端点段标识 END.SID 关联的操作包括: 根据 END.SID 的下一跳 SID 匹配从第一 POP 到第二 POP 之间的上层 overlay SRv6 Policy。

在可能的实现方式中, overlay 端到端隧道为 SR-MPLS TE Policy, 第二报文包括 MPLS 标签栈, MPLS 标签栈包括第一信息和第二信息。

在可能的实现方式中, 第一信息为第一 POP 的第一节点 SID, 第一节点 SID 关联的操作包括: 根据标

签栈中第一节点 SID 的下一跳 SID 匹配从第一 POP 到第二 POP 之间的上层 overlay SR MPLS 隧道。

在可能的实现方式中，overlay 端到端隧道为基于通用网络虚拟化封装 GENEVE 协议封装的隧道，第二报文采用 SRv6 in GENEVE 封装。

在可能的实现方式中，overlay 端到端隧道为基于通用路由封装 GRE 协议封装的隧道，第二报文采用 SRv6 over GRE 封装。

在可能的实现方式中，接收模块 610 还用于，接收第二站点 edge 通告的边界网关协议 BGP 路由，BGP 路由包括路由类型 RT、IPsec SA、第二站点 edge 的标识、以及导出路由目标 ExportRT，其中，路由类型 RT 指示 BGP 路由通告的 IPsec SA 用于对与 Export RT 匹配的虚拟路由转发 VRF 中的 VPN 业务报文进行端到端安全保护；处理模块 620，用于根据路由类型 RT 和 Export RT，将 IPsec SA 与 VRF 关联。

在可能的实现方式中，BGP 路由为 BGP 软件定义的广域网 SD-WAN 路由，该 BGP SD-WAN 路由的子地址族为 SD-WAN 子地址族，或者，BGP 路由为 BGP 以太网虚拟专用网络 EVPN 路由，该 BGP EVPN 路由的子地址族为 EVPN 子地址族。

在可能的实现方式中，第二站点 edge 的标识包括第二站点 edge 所属的站点标识 site ID 和/或第二站点 edge 的节点标识 Node ID。

在可能的实现方式中，BGP 路由包括网络层可达信息 NLRI，NLRI 包括路由类型 RT 和第二站点 edge 的标识。

在可能的实现方式中，BGP 路由包括隧道封装属性类型长度值 Tunnel Encapsulation Attribute TLV，Tunnel Encapsulation Attribute TLV 包括 IPsec SA。

在可能的实现方式中，BGP 路由包括扩展团体属性，扩展团体属性用于携带 Export RT。

在可能的实现方式中，第一站点 edge 和第二站点 edge 为软件定义的广域网 SD-WAN 中站点 edge。

安全传输报文的装置 600 可以用于实现图 5 对应的方法实施例，即数据转发而发送侧对应的方法实施例，还可以用于实现图 2 方法实施例中第一站点 edge 所执行的方法步骤，即控制面接收侧对应的方法实施例，具体可参考图 2 或图 5 中方法实施例具体内容的描述，为了说明书的简洁，在此不再赘述。当安全传输报文的装置 600 用于实现控制面接收侧对应的方法实施例时，安全传输报文的装置 600 又可称为协商 IPsec SA 的装置。

可以理解，图 10 中各个功能模块的划分及各个功能模块对应执行的步骤仅仅是一种示例，在其他实施例中，装置 600 还可以根据具体执行步骤划分为更多或更少的功能模块。

参见图 11，图 11 为本申请实施例提供的又一种安全传输报文的装置 700 的结构示意图，安全传输报文的装置 700 可以配置为广域网中的第二站点 edge，所述装置 700 包括：

接收模块 710，用于接收第一站点 edge 通过在第一站点 edge 和第二站点 edge 之间建立的上层 overlay 端到端隧道发送的第二报文，第二报文中包括第一报文以及在第一报文外层封装的 overlay 端到端隧道的隧道信息，overlay 端到端隧道对应的底层 underlay 隧道包括多段隧道，隧道信息包括第一入网点 POP 的第一信息，第一站点 edge 为 overlay 端到端隧道的入端点，第二站点 edge 为 overlay 端到端隧道的出端点，overlay 端到端隧道经过第一 POP，第一报文为通过第二站点 edge 与第一站点 edge 协商的因特网协议安全协议安全联盟 IPsec SA 对虚拟专用网络 VPN 业务报文进行安全保护所得到的报文；

处理模块 720，用于对第二报文进行解封装，获得第一报文；

处理模块 720，用于根据 IPsecSA 对第一报文进行处理，以获得 VPN 业务报文。

在可能的实现方式中，处理模块 720 用于：根据 IPsecSA，对第一报文进行封装安全载荷 ESP 协议解密；和/或，根据 IPsec SA 和第一报文的认证头 Authentication Header 中携带的认证数据对第一报文进行认证。

在可能的实现方式中，隧道信息还包括第二 POP 的第二信息，overlay 端到端隧道经过第一 POP 和第二 POP，第一站点 edge 通过第一 POP 接入广域网，第二站点 edge 通过第二 POP 接入广域网。

在可能的实现方式中，overlay 端到端隧道为互联网协议第六版本 IPv6 的段路由 SRv6 隧道，第二报文包括 IPv6 头和分段路由头 SRH，IPv6 头的目的地址指向第一 POP，SRH 头包括第一信息和第二信息。

在可能的实现方式中，第一信息为第一 POP 的第一端点段标识 END.SID，第一端点段标识 END.SID 关联的操作包括：根据 END.SID 的下一跳 SID 匹配从第一 POP 到第二 POP 之间的上层 overlay SRv6 Policy。

在可能的实现方式中，overlay 端到端隧道为分段路由多协议标签交换流量工程策略 SR-MPLS TE Policy，第二报文包括 MPLS 标签栈，MPLS 标签栈包括第一信息和第二信息。

在可能的实现方式中，第一信息为第一 POP 的第一节点 SID，第一节点 SID 关联的操作包括：根据标签栈中第一节点 SID 的下一跳 SID 匹配从第一 POP 到第二 POP 之间的上层 overlay SR MPLS 隧道。

在可能的实现方式中，overlay 端到端隧道为基于通用网络虚拟化封装 GENEVE 协议封装的隧道，第二报文采用 SRv6 in GENEVE 封装。

在可能的实现方式中，overlay 端到端隧道为基于通用路由封装 GRE 协议封装的隧道，第二报文采用 SRv6 over GRE 封装。

在可能的实现方式中，

处理模块 720，用于生成边界网关协议 BGP 路由，其中，BGP 路由包括路由类型 RT、IPsec SA、第二站点 edge 的标识、以及导出路由目标 ExportRT，其中，路由类型 RT 指示 BGP 路由通告的 IPsec SA 用于对与 Export RT 匹配的虚拟路由转发 VRF 中的 VPN 业务报文进行端到端安全保护；

发送模块 730，用于第二站点 edge 向第一站点 edge 通告 BGP 路由。

在可能的实现方式中，BGP 路由为 BGP 软件定义的广域网 SD-WAN 路由，该 BGP SD-WAN 路由的子地址族为 SD-WAN 子地址族，或者，BGP 路由为 BGP 以太网虚拟专用网络 EVPN 路由，该 BGP EVPN 路由的子地址族为 EVPN 子地址族。

在可能的实现方式中，第二站点 edge 的标识包括第二站点 edge 所属的站点标识 site ID 和/或第二站点 edge 的节点标识 Node ID。

在可能的实现方式中，BGP 路由包括网络层可达信息 NLRI，NLRI 包括路由类型 RT 和第二站点 edge 的标识。

在可能的实现方式中，BGP 路由包括隧道封装属性类型长度值 Tunnel Encapsulation Attribute TLV，Tunnel Encapsulation Attribute TLV 包括 IPsec SA。

在可能的实现方式中，BGP 路由包括扩展团体属性，扩展团体属性用于携带 Export RT。

在可能的实现方式中，第一站点 edge 和第二站点 edge 为软件定义的广域网 SD-WAN 中站点 edge。

安全传输报文的装置 700 可以用于实现图 9 对应的方法实施例，即数据转发面接收侧对应的方法实施例，还可以用于实现图 2 对应的方法实施例中第二站点 edge 所执行的方法步骤，即控制面发送侧对应的方法实施例。具体可参考图 2 或图 9 中方法实施例具体内容的描述，为了说明书的简洁，在此不再赘述。当安全传输报文的装置 700 用于实现控制面发送侧对应的方法实施例时，安全传输报文的装置 700 又可称为协商 IPsec SA 的装置。

可以理解，图 11 中各个功能模块的划分及各个功能模块对应执行的步骤仅仅是一种示例，在其他实施例中，装置 700 还可以根据具体执行步骤划分为更多或更少的功能模块。

参见图 12，图 12 为本申请提供了一种网络设备 800 的结构示意图，该网络设备 800 可以配置为广域网中的第一站点 edge，也可以配置为广域网中的第二站点 edge。网络设备 800 可以由一般性的总线体系结构来实现。

网络设备 800 包括至少一个处理器 801、存储器 803 以及至少一个通信接口 804。

处理器 801 可以是一个通用 CPU、NP、微处理器，或者也可以是一个或多个用于实现本申请方案的集成电路。例如，专用集成电路(application-specific integrated circuit, ASIC)、可编程逻辑器件(programmable logic device, PLD)或其组合。其中，PLD 可以是复杂可编程逻辑器件(complex programmable logic device, CPLD)、现场可编程逻辑门阵列(field-programmable gate array, FPGA)、通用阵列逻辑(generic array logic, GAL)或其任意组合。

网络设备 800 还可以包括通信总线 802，用于在各个组件之间传送信息。通信总线 802 可以分为地址总线、数据总线、控制总线等。为便于表示，图 12 中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

存储器 803 可以是只读存储器(read-only memory, ROM)或可存储静态信息和指令的其它类型的静态存储设备，也可以是随机存取存储器(random access memory, RAM)或者可存储信息和指令的其它类型的动态存储设备，也可以是电可擦可编程只读存储器(electrically erasable programmable read-only Memory, EEPROM)、只读光盘(compact disc read-only memory, CD-ROM)或其它光盘存储、光碟存储(包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、磁盘存储介质或者其它磁存储设备，也可以是能够用于携带或存储具有指令或数据结构形式的程序代码且能够由计算机存取的任何其它介质，但不限于此。存储器 803 可以是独立存在，并通过通信总线 802 与处理器 801 相连接；存储器 803 也可以和处理器 801

集成在一起。

通信接口 804 用于与其它设备或通信网络进行通信。通信接口 804 可以包括有线通信接口，还可以包括无线通信接口。其中，有线通信接口例如可以为以太网接口，以太网接口可以是光接口、电接口或其组合。无线通信接口可以为无线局域网（wireless local area networks, WLAN）接口、蜂窝网络通信接口或其组合等。

在具体实现中，作为一种实施例，处理器 801 可以包括一个或多个 CPU，例如，图 12 中所示的 CPU0 和 CPU1。

在具体实现中，作为一种实施例，网络设备 800 可以包括多个处理器，如图 12 中所示的处理器 801 和处理器 805。这些处理器中的每一个可以是一个单核处理器（single-CPU），也可以是一个多核处理器（multi-CPU）。这里的处理器可以指一个或多个设备、电路、和/或用于处理数据（如计算机程序指令）的处理核。

在一些实施例中，存储器 803 用于存储本申请方案的程序代码 810，处理器 801 用于执行存储器 803 中存储的程序代码 810。也即是，网络设备 800 可以通过处理器 801 以及存储器 803 中的程序代码 810，来实现图 2 或图 5 或图 9 方法实施例提供的方法。

本申请实施例的网络设备 800 可对应于上述各个方法实施例中的第一站点 edge 或第二站点 edge，并且，该网络设备 800 中的处理器 801、通信接口 804 等可以实现上述各个方法实施例中的设备所具有的功能和/或所实施的各种步骤和方法。为了简洁，在此不再赘述。

当网络设备 800 配置为第一站点 edge 时，对应于上述安全传输报文的装置 600，则安全传输报文的装置 600 中的接收模块 610、发送模块 630 可以位于网络设备 800 中的通信接口 804 中；处理模块 620 可以位于网络设备 800 中的处理器 801 或处理器 805 中。

当网络设备 800 配置为第二站点 edge 时，对应于上述安全传输报文的装置 700，则安全传输报文的装置 700 中的接收模块 710、发送模块 730 可以位于网络设备 800 中的通信接口 804 中；处理模块 720 可以位于网络设备 800 中的处理器 801 或处理器 805 中。

网络设备 800 中的各硬件、模块和上述其他操作和/或功能分别为了实现安全传输报文的装置 600 或安全传输报文的装置 700 所实施的各种步骤和方法，关于网络设备 800 如何实现报文处理等详细流程，具体细节可参见上述方法实施例，为了说明书的简洁，在此不再赘述。

其中，上文图 2 或图 5 或图 9 的各步骤通过网络设备 800 的处理器中的硬件的集成逻辑电路或者软件形式的指令完成。结合本申请实施例所公开的方法和步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块（软件单元）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、电可擦写可编程存储器和寄存器等本领域成熟的一种或多种存储介质中。存储介质位于存储器中，处理器读取存储器中的信息，结合硬件执行上述方法中的步骤。为了说明书的简洁，这里不再详细描述。

本申请实施例还提供了一种系统，所述系统包括第一站点 edge 和第二站点 edge，第一站点 edge 可以为上述的安全报文传输的装置 600 或网络设备 800，第二站点 edge 可以为上述的安全报文传输的装置 700 或网络设备 800，第一站点 edge 可用于实现上述图 2 或图 5 所述的方法实施例，第二站点 edge 可用于实现上述图 2 或图 9 所述的方法实施例，具体可参考上述图 2 或图 5 或图 9 方法实施例的描述，在此不再赘述。

本申请实施例还提供了一种计算机存储介质，包括程序指令，当所述程序指令在处理器上执行时，使得所述处理器实现上述图 2 或图 5 或图 9 所述的方法实施例中的各个步骤。

本申请实施例还提供了一种包括程序指令的计算机程序产品，当所述程序指令在处理器上执行时，使得所述处理器实现上述图 2 或图 5 或图 9 所述的方法实施例中的各个步骤。

本领域普通技术人员可以意识到，结合本文中所公开的实施例中描述的各方法步骤和单元，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各实施例的步骤及组成。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。本领域普通技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参见前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以

上所描述的装置实施例仅仅是示意性的，例如，该单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另外，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口、装置或单元的间接耦合或通信连接，也可以是电的，机械的或其它的形式连接。

该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单元来实现本申请实施例方案的目的。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以是两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

该集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用，可以存储在一个计算机可读存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分，或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例中的方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（read-only memory, ROM）、随机存取存储器（random access memory, RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。该计算机程序产品包括一个或多个计算机程序指令。在计算机上加载和执行该计算机程序指令时，全部或部分地产生按照本申请实施例中的流程或功能。该计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。该计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，该计算机程序指令可以从一个网站站点、计算机、服务器或数据中心通过有线或无线方式向另一个网站站点、计算机、服务器或数据中心进行传输。该计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。该可用介质可以是磁性介质（例如软盘、硬盘、磁带）、光介质（例如，数字视频光盘（digital video disc, DVD）、或者半导体介质（例如固态硬盘）等。

以上描述，仅为本申请的具体实施方式，但本申请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申请揭露的技术范围内，可轻易想到各种等效的修改或替换，这些修改或替换都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以权利要求的保护范围为准。

权 利 要 求 书

1.一种安全传输报文的方法,其特征在于,所述方法包括:

广域网中的第一站点出口设备 edge 接收虚拟路由转发 VRF 中的虚拟专用网络 VPN 业务报文;

所述第一站点 edge 根据与第二站点 edge 协商的与所述 VRF 关联的因特网协议安全协议安全联盟 IPsecSA 对所述 VPN 业务报文进行安全保护,以得到第一报文;

所述第一站点 edge 在所述第一报文外层封装所述第一站点 edge 与所述第二站点 edge 之间建立的上层 overlay 端到端隧道的隧道信息,以获得第二报文,其中,所述 overlay 端到端隧道对应的底层 underlay 隧道包括多段隧道,所述隧道信息包括第一入网点 POP 的第一信息,所述第一站点 edge 为所述 overlay 端到端隧道的入端点,所述第二站点 edge 为所述 overlay 端到端隧道的出端点,所述 overlay 端到端隧道经过所述第一 POP;

所述第一站点 edge 通过所述 overlay 端到端隧道,向所述第二站点 edge 发送所述第二报文。

2.根据权利要求1所述的方法,其特征在于,所述对所述 VPN 业务报文进行安全保护包括:

对所述 VPN 业务报文进行封装安全载荷 ESP 协议加密;和/或,

对所述 VPN 业务报文封装认证头 Authentication Header。

3.根据权利要求1或2所述的方法,其特征在于,所述隧道信息还包括第二 POP 的第二信息,所述 overlay 端到端隧道经过所述第一 POP 和所述第二 POP,所述第一站点 edge 通过所述第一 POP 接入所述广域网,所述第二站点 edge 通过所述第二 POP 接入所述广域网。

4.根据权利要求3所述的方法,其特征在于,所述 overlay 端到端隧道为互联网协议第六版本 IPv6 的段路由 SRv6 隧道,所述第二报文包括 IPv6 头和分段路由头 SRH,所述 IPv6 头的目的地址指向所述第一 POP,所述 SRH 包括所述第一信息和所述第二信息。

5.根据权利要求4所述的方法,其特征在于,所述第一信息为所述第一 POP 的第一端点段标识 END.SID,所述第一端点段标识 END.SID 关联的操作包括:根据所述 END.SID 的下一跳 SID 匹配从所述第一 POP 到所述第二 POP 之间的上层 overlay SRv6 Policy。

6.根据权利要求3所述的方法,其特征在于,所述 overlay 端到端隧道为分段路由多协议标签交换流量工程策略 SR-MPLS TE Policy,所述第二报文包括 MPLS 标签栈,所述 MPLS 标签栈包括所述第一信息和所述第二信息。

7.根据权利要求6所述的方法,其特征在于,所述第一信息为所述第一 POP 的第一节点 SID,所述第一节点 SID 关联的操作包括:

根据所述标签栈中所述第一节点 SID 的下一跳 SID 匹配从所述第一 POP 到所述第二 POP 之间的上层 overlay SR MPLS 隧道。

8.根据权利要求3所述的方法,其特征在于,所述 overlay 端到端隧道为基于通用网络虚拟化封装 GENEVE 协议封装的隧道,所述第二报文采用 SRv6 in GENEVE 封装。

9.根据权利要求3所述的方法,其特征在于,所述 overlay 端到端隧道为基于通用路由封装 GRE 协议封装的隧道,所述第二报文采用 SRv6 over GRE 封装。

10.根据权利要求1至9任一项所述的方法,其特征在于,在所述第一站点 edge 接收所述业务报文之前,所述方法还包括:

所述第一站点 edge 接收所述第二站点 edge 通告的边界网关协议 BGP 路由,所述 BGP 路由包括路由类型 RT、所述 IPsec SA、所述第二站点 edge 的标识、以及导出路由目标 ExportRT,其中,所述路由类型 RT 指示所述 BGP 路由通告的所述 IPsec SA 用于对与所述 Export RT 匹配的所述虚拟路由转发 VRF 中的所述 VPN 业务报文进行端到端安全保护;

根据所述路由类型 RT 和所述 Export RT,所述第一站点 edge 将所述 IPsec SA 与所述 VRF 关联。

11.根据权利要求10所述的方法,其特征在于,所述 BGP 路由为 BGP 软件定义的广域网 SD-WAN 路由,所述 BGP SD-WAN 路由的子地址族为 SD-WAN 子地址族,或者,所述 BGP 路由为 BGP 以太网虚拟专用网络 EVPN 路由,所述 BGP EVPN 路由的子地址族为 EVPN 子地址族。

12.根据权利要求10或11所述的方法,其特征在于,所述第二站点 edge 的标识包括所述第二站点 edge 所属的站点标识 site ID 和所述第二站点 edge 的节点标识 Node ID。

13.根据权利要求10-12任一项所述的方法,其特征在于,所述 BGP 路由包括网络层可达信息 NLRI,所述 NLRI 包括所述路由类型 RT 和所述第二站点 edge 的标识。

14.根据权利要求 10-13 任一项所述的方法,其特征在于,所述 BGP 路由包括隧道封装属性类型长度值 Tunnel Encapsulation Attribute TLV,所述 Tunnel Encapsulation Attribute TLV 包括所述 IPsec SA。

15.根据权利要求 10 至 14 任一项所述的方法,其特征在于,所述 BGP 路由包括扩展团体属性,所述扩展团体属性用于携带所述 Export RT。

16.根据权利要求 10-15 任一项所述的方法,其特征在于,所述第一站点 edge 和所述第二站点 edge 为软件定义的广域网 SD-WAN 中站点 edge。

17.一种安全传输报文的方法,其特征在于,所述方法包括:

广域网中的第二站点出口设备 edge 接收第一站点 edge 通过在所述第一站点 edge 和所述第二站点 edge 之间建立的上层 overlay 端到端隧道发送的第二报文,所述第二报文中包括第一报文以及在所述第一报文外层封装的所述 overlay 端到端隧道的隧道信息,所述 overlay 端到端隧道对应的底层 underlay 隧道包括多段隧道,所述隧道信息包括第一入网点 POP 的第一信息,所述第一站点 edge 为所述 overlay 端到端隧道的入端点,所述第二站点 edge 为所述 overlay 端到端隧道的出端点,所述 overlay 端到端隧道经过所述第一 POP,所述第一报文为通过所述第二站点 edge 与所述第一站点 edge 协商的因特网协议安全协议安全联盟 IPsec SA 对虚拟专用网络 VPN 业务报文进行安全保护所得到的报文;所述第二站点 edge 对所述第二报文进行解封装,获得第一报文;

所述第二站点 edge 根据所述 IPsecSA 对所述第一报文进行处理,以获得所述 VPN 业务报文。

18.根据权利要求 17 所述的方法,其特征在于,所述对所述第一报文进行处理包括:

根据所述 IPsecSA,对所述第一报文进行封装安全载荷 ESP 协议解密;和/或,

根据所述 IPsec SA 和所述第一报文的认证头 Authentication Header 中携带的认证数据对所述第一报文进行认证。

19.根据权利要求 17 或 18 所述的方法,其特征在于,所述隧道信息还包括第二 POP 的第二信息,所述 overlay 端到端隧道经过所述第一 POP 和所述第二 POP,所述第一站点 edge 通过所述第一 POP 接入所述广域网,所述第二站点 edge 通过所述第二 POP 接入所述广域网。

20.根据权利要求 19 所述的方法,其特征在于,所述 overlay 端到端隧道为互联网协议第六版本 IPv6 的段路由 SRv6 隧道,所述第二报文包括 IPv6 头和分段路由头 SRH,所述 IPv6 头的目的地址指向所述第一 POP,所述 SRH 头包括所述第一信息和所述第二信息。

21.根据权利要求 20 所述的方法,其特征在于,所述第一信息为第一 POP 的第一端点段标识 END.SID,所述第一端点段标识 END.SID 关联的操作包括:根据所述 END.SID 的下一跳 SID 匹配从所述第一 POP 到所述第二 POP 之间的上层 overlay SRv6 Policy。

22.根据权利要求 19 所述的方法,其特征在于,所述 overlay 端到端隧道为分段路由多协议标签交换流量工程策略 SR-MPLS TE Policy,所述第二报文包括 MPLS 标签栈,所述 MPLS 标签栈包括所述第一信息和所述第二信息。

23.根据权利要求 22 所述的方法,其特征在于,所述第一信息为所述第一 POP 的第一节点 SID,所述第一节点 SID 关联的操作包括:

根据所述标签栈中所述第一节点 SID 的下一跳 SID 匹配从所述第一 POP 到所述第二 POP 之间的上层 overlay SR MPLS 隧道。

24.根据权利要求 19 所述的方法,其特征在于,所述 overlay 端到端隧道为基于通用网络虚拟化封装 GENEVE 协议封装的隧道,所述第二报文采用 SRv6 in GENEVE 封装。

25.根据权利要求 19 所述的方法,其特征在于,所述 overlay 端到端隧道为基于通用路由封装 GRE 协议封装的隧道,所述第二报文采用 SRv6 over GRE 封装。

26.根据权利要求 17 至 25 任一项所述的方法,其特征在于,在所述广域网中的第二站点出口设备 edge 接收第一站点 edge 通过上层 overlay 端到端隧道发送的第二报文之前,所述方法还包括:

所述第二站点出口设备 edge 生成边界网关协议 BGP 路由,其中,所述 BGP 路由包括路由类型 RT、所述 IPsec SA、所述第二站点 edge 的标识、以及导出路由目标 ExportRT,其中,所述路由类型 RT 指示所述 BGP 路由通告的所述 IPsec SA 用于对与所述 Export RT 匹配的虚拟路由转发 VRF 中的所述 VPN 业务报文进行端到端安全保护;

所述第二站点 edge 向所述第一站点 edge 通告所述 BGP 路由。

27.根据权利要求 26 所述的方法,其特征在于,所述 BGP 路由为 BGP 软件定义的广域网 SD-WAN 路

由, 所述 BGP SD-WAN 路由的子地址族为 SD-WAN 子地址族, 或者, 所述 BGP 路由为 BGP 以太网虚拟专用网络 EVPN 路由, 所述 BGPEVPN 路由的子地址族为 EVPN 子地址族。

28. 根据权利要求 26 或 27 所述的方法, 其特征在于, 所述第二站点 edge 的标识包括所述第二站点 edge 所属的站点标识 site ID 和所述第二站点 edge 的节点标识 Node ID。

29. 根据权利要求 26 至 28 任一项所述的方法, 其特征在于, 所述 BGP 路由包括网络层可达信息 NLRI, 所述 NLRI 包括所述路由类型 RT 和所述第二站点 edge 的标识。

30. 根据权利要求 26 至 29 任一项所述的方法, 其特征在于, 所述 BGP 路由包括隧道封装属性类型长度值 Tunnel Encapsulation Attribute TLV, 所述 Tunnel Encapsulation Attribute TLV 包括所述 IPsec SA。

31. 根据权利要求 26 至 30 任一项所述的方法, 其特征在于, 所述 BGP 路由包括扩展团体属性, 所述扩展团体属性用于携带所述 Export RT。

32. 根据权利要求 26 至 31 任一项所述的方法, 其特征在于, 所述第一站点 edge 和所述第二站点 edge 为软件定义的广域网 SD-WAN 中站点 edge。

33. 一种协商因特网协议安全协议安全联盟 IPsec SA 的方法, 其特征在于, 所述方法包括:

广域网中的第一站点出口设备 edge 接收第二站点 edge 通告的边界网关协议 BGP 路由, 所述 BGP 路由包括路由类型 RT、所述 IPsec SA、所述第二站点 edge 的标识、以及导出路由目标 ExportRT, 其中, 所述路由类型 RT 指示所述 BGP 路由通告的所述 IPsec SA 用于对与所述 Export RT 匹配的虚拟路由转发 VRF 中的业务报文进行端到端安全保护;

根据所述路由类型 RT 和所述 Export RT, 所述第一站点 edge 将所述 IPsec SA 与所述 VRF 关联。

34. 根据权利要求 33 所述的方法, 其特征在于, 所述 BGP 路由为 BGP 软件定义的广域网 SD-WAN 路由, 所述 BGP SD-WAN 路由的子地址族为 SD-WAN 子地址族, 或者, 所述 BGP 路由为 BGP 以太网虚拟专用网络 EVPN 路由, 所述 BGPEVPN 路由的子地址族为 EVPN 子地址族。

35. 根据权利要求 33 或 34 所述的方法, 其特征在于, 所述第二站点 edge 的标识包括所述第二站点 edge 所属的站点标识 site ID 和所述第二站点 edge 的节点标识 Node ID。

36. 根据权利要求 33 至 35 任一项所述的方法, 其特征在于, 所述 BGP 路由包括网络层可达信息 NLRI, 所述 NLRI 包括所述路由类型 RT 和所述第二站点 edge 的标识。

37. 根据权利要求 33 至 36 任一项所述的方法, 其特征在于, 所述 BGP 路由包括隧道封装属性类型长度值 Tunnel Encapsulation Attribute TLV, 所述 Tunnel Encapsulation Attribute TLV 包括所述 IPsec SA。

38. 根据权利要求 33 至 37 任一项所述的方法, 其特征在于, 所述 BGP 路由包括扩展团体属性, 所述扩展团体属性用于携带所述 Export RT。

39. 根据权利要求 33 至 38 任一项所述的方法, 其特征在于, 所述第一站点 edge 和所述第二站点 edge 为软件定义的广域网 SD-WAN 中站点 edge。

40. 一种协商因特网协议安全协议安全联盟 IPsec SA 的方法, 其特征在于, 所述方法包括:

广域网中的第二站点出口设备 edge 生成边界网关协议 BGP 路由, 其中, 所述 BGP 路由包括路由类型 RT、所述 IPsec SA、所述第二站点 edge 的标识、以及导出路由目标 ExportRT, 其中, 所述路由类型 RT 指示所述 BGP 路由通告的所述 IPsec SA 用于对与所述 Export RT 匹配的虚拟路由转发 VRF 中的业务报文进行端到端安全保护;

所述第二站点 edge 向第一站点 edge 通告所述 BGP 路由。

41. 根据权利要求 40 所述的方法, 其特征在于, 所述 BGP 路由为 BGP 软件定义的广域网 SD-WAN 路由, 所述 BGP SD-WAN 路由的子地址族为 SD-WAN 子地址族, 或者, 所述 BGP 路由为 BGP 以太网虚拟专用网络 EVPN 路由, 所述 BGPEVPN 路由的子地址族为 EVPN 子地址族。

42. 根据权利要求 40 或 41 所述的方法, 其特征在于, 所述第二站点 edge 的标识包括所述第二站点 edge 所属的站点标识 site ID 和所述第二站点 edge 的节点标识 Node ID。

43. 根据权利要求 40 至 42 任一项所述的方法, 其特征在于, 所述 BGP 路由包括网络层可达信息 NLRI, 所述 NLRI 包括所述路由类型 RT 和所述第二站点 edge 的标识。

44. 根据权利要求 40 至 43 任一项所述的方法, 其特征在于, 所述 BGP 路由包括隧道封装属性类型长度值 Tunnel Encapsulation Attribute TLV, 所述 Tunnel Encapsulation Attribute TLV 包括所述 IPsec SA。

45. 根据权利要求 40 至 44 任一项所述的方法, 其特征在于, 所述 BGP 路由包括扩展团体属性, 所述

扩展团体属性用于携带所述 Export RT。

46.根据权利要求 40 至 45 任一项所述的方法，其特征在于，所述第一站点 edge 和所述第二站点 edge 为软件定义的广域网 SD-WAN 中站点 edge。

47.一种安全传输报文的装置，其特征在于，所述装置包括用于实现如权利要求 1-16 任一项所述方法的模块。

48.一种安全传输报文的装置，其特征在于，所述装置包括用于实现如权利要求 17-32 任一项所述方法的模块。

49.一种协商因特网协议安全协议安全联盟 IPsec SA 的装置，其特征在于，所述装置包括用于实现如权利要求 33-39 任一项所述方法的模块。

50.一种协商因特网协议安全协议安全联盟 IPsec SA 的装置，其特征在于，所述装置包括用于实现如权利要求 40-46 任一项所述方法的模块。

51.一种网络设备，其特征在于，包括存储器和处理器，所述存储器用于存储指令，所述处理器用于执行所述存储器中存储的所述指令，以实现如权利要求 1 至 16 任一项所述的方法，或者，以实现如权利要求 17 至 32 任一项所述的方法，或者，以实现如权利要求 33 至 39 任一项所述的方法，或者，以实现如权利要求 40 至 46 任一项所述的方法。

52.一种系统，其特征在于，包括第一站点出口设备 edge 和第二站点 edge，所述第一站点 edge 用于执行如权利要求 1 至 16 任一项所述的方法，所述第二站点 edge 用于执行如权利要求 17 至 32 任一项所述的方法；或者，所述第一站点 edge 用于执行如权利要求 33 至 39 任一项所述的方法，所述第二站点 edge 用于执行如权利要求 40 至 46 任一项所述的方法。

53.一种计算机存储介质，其特征在于，包括程序指令，当所述程序指令在处理器上执行时，使得所述处理器实现如权利要求 1 至 16 任一项所述的方法，或者，使得所述处理器实现如权利要求 17 至 32 任一项所述的方法，或者，使得所述处理器实现如权利要求 33 至 39 任一项所述的方法，或者，使得所述处理器实现如权利要求 40 至 46 任一项所述的方法。

54.一种包括程序指令的计算机程序产品，其特征在于，当所述程序指令在处理器上执行时，使得所述处理器实现如权利要求 1 至 16 任一项所述的方法，或者，使得所述处理器实现如权利要求 17 至 32 任一项所述的方法，或者，使得所述处理器实现如权利要求 33 至 39 任一项所述的方法，或者，使得所述处理器实现如权利要求 40 至 46 任一项所述的方法。

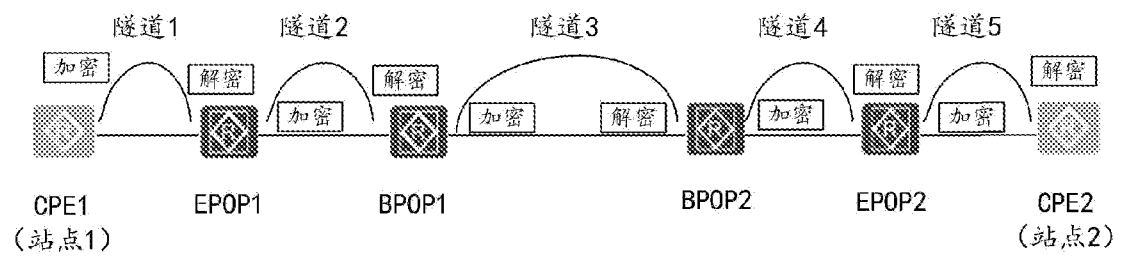


图 1

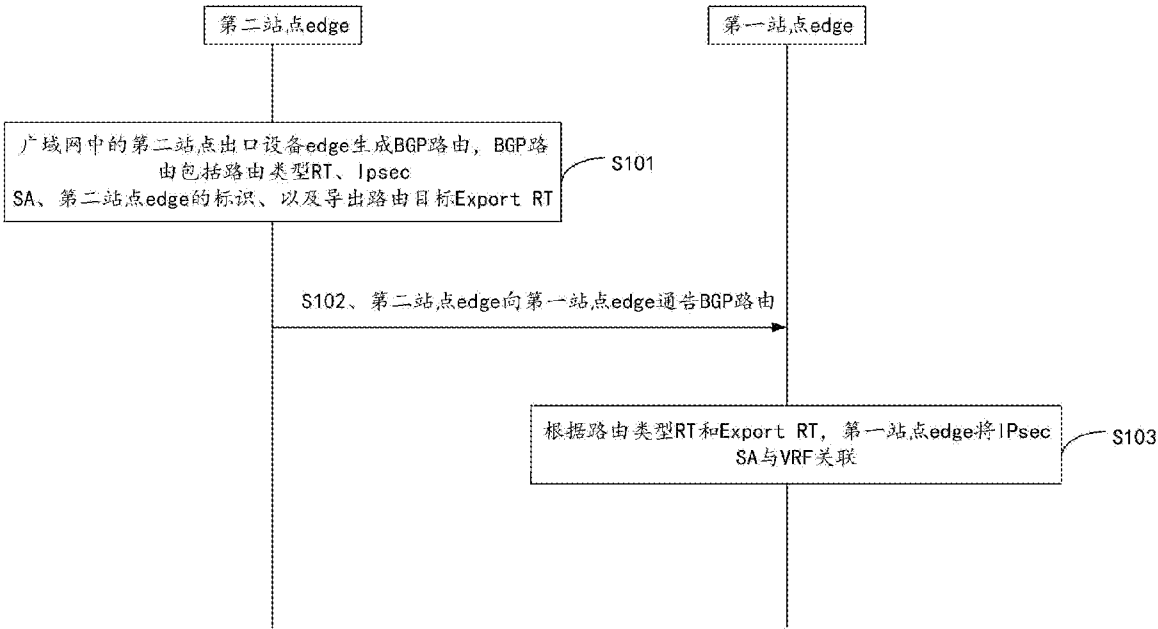


图 2

Route Type = 2	2 octets
Route Distinguisher	8 octets
SD-WAN-Color	4 octets
SD-WAN-Node-ID	4 or 16 octets

图 3

Route Type = 10	2 octets
Route Distinguisher	8 octets
SD-WAN-Color	4 octets
SD-WAN-Node-ID	4 or 16 octets

图 4

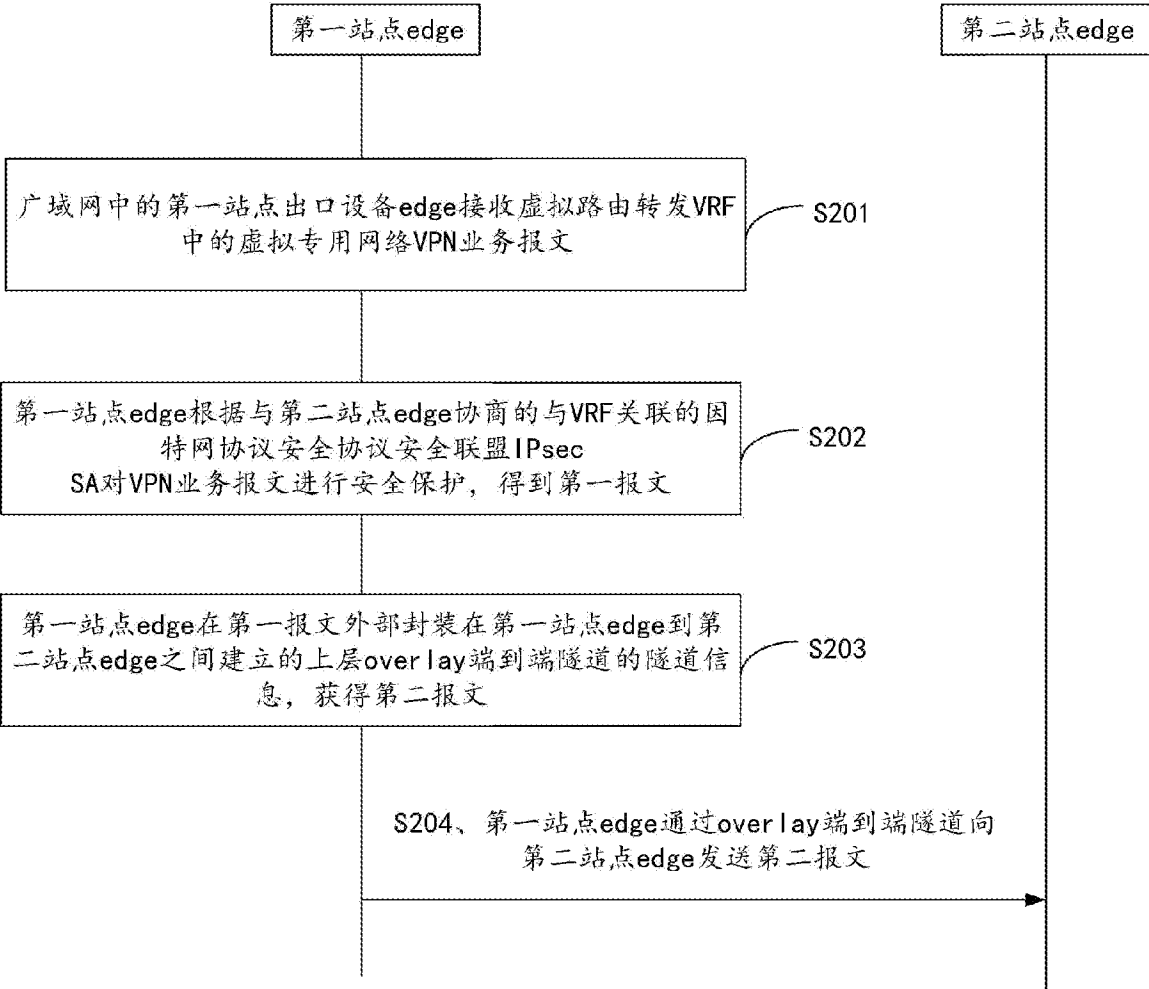


图 5

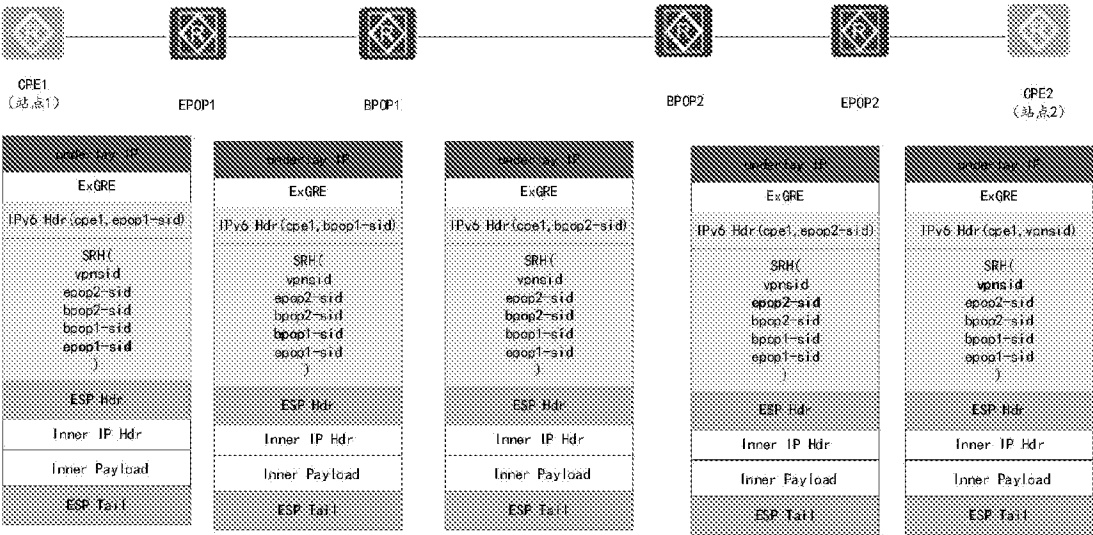
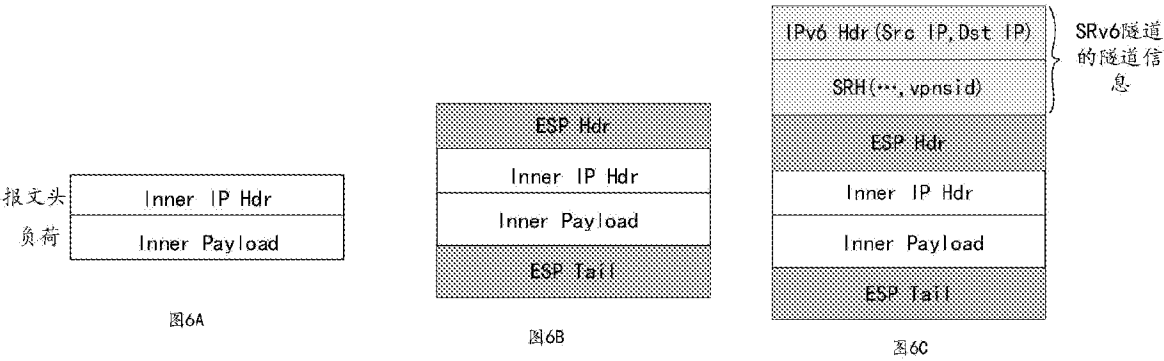


图 7

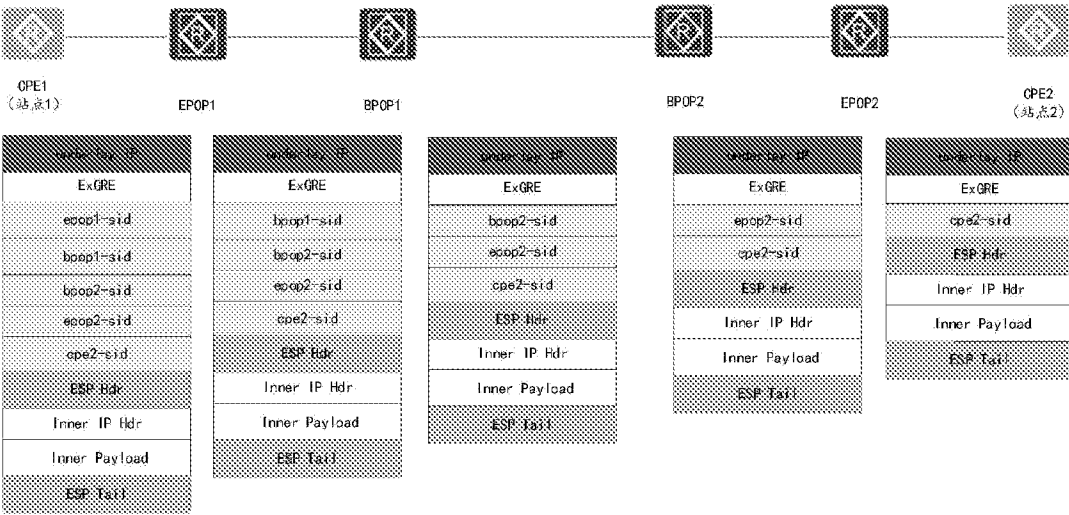


图 8

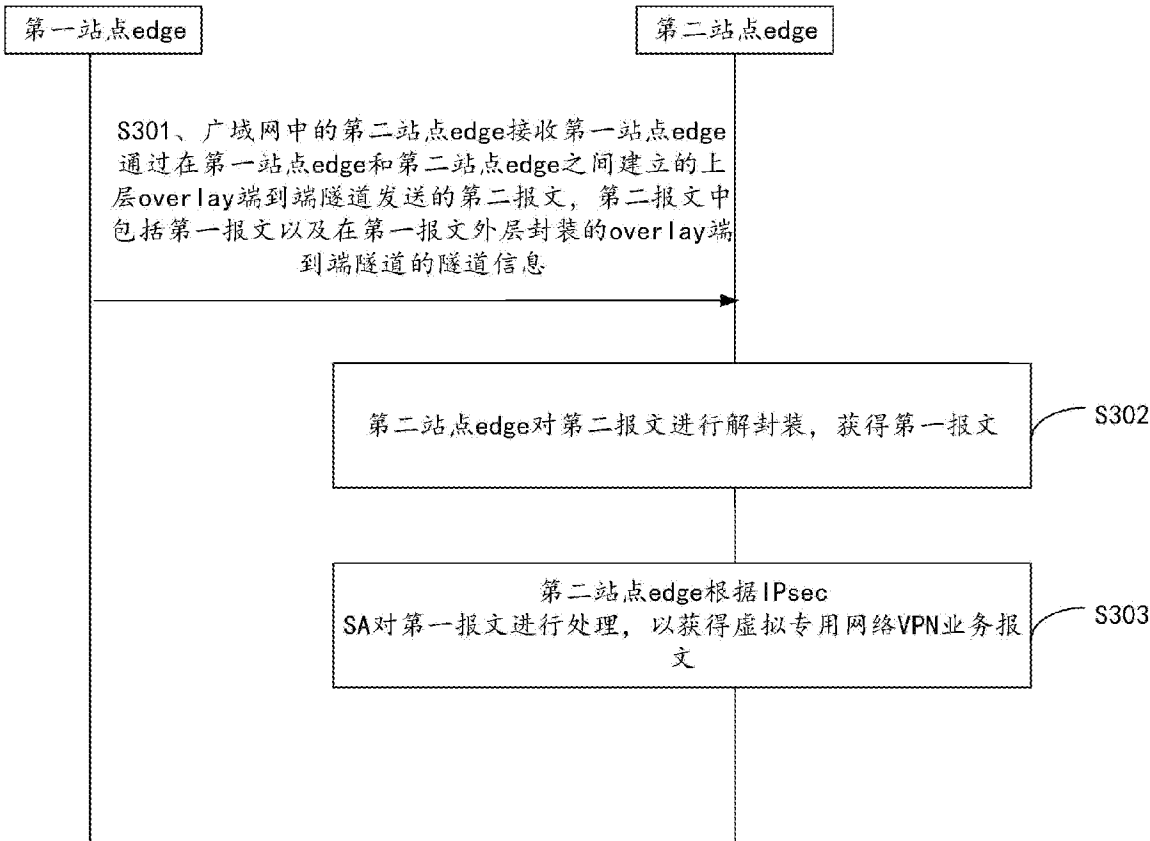


图 9

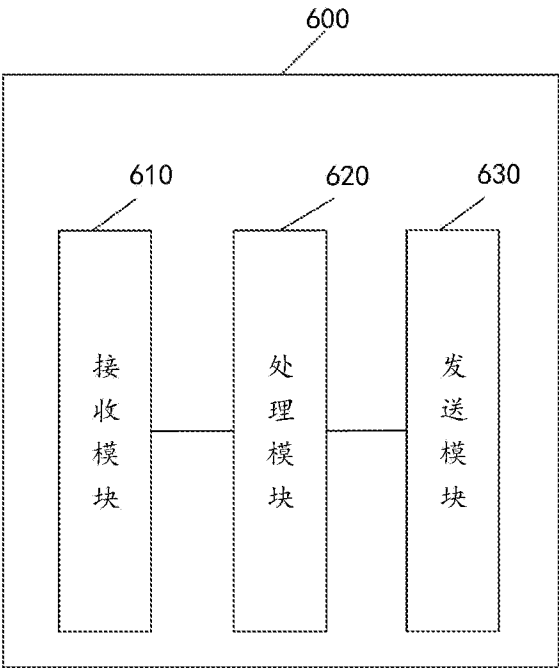


图 10

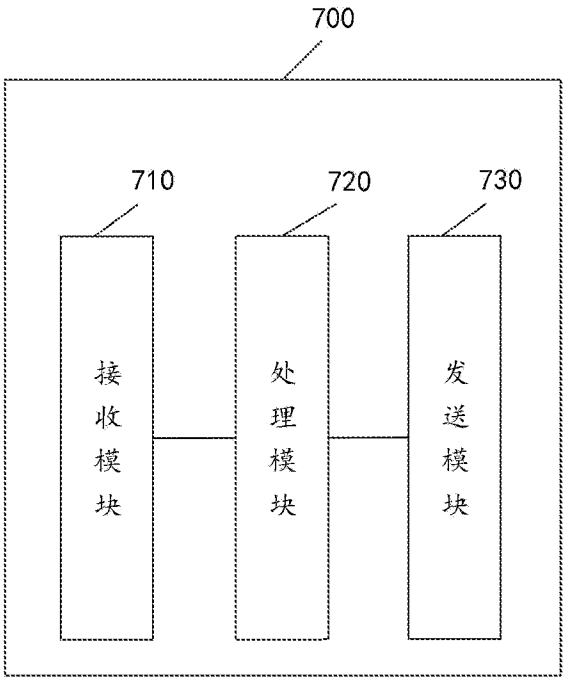


图 11

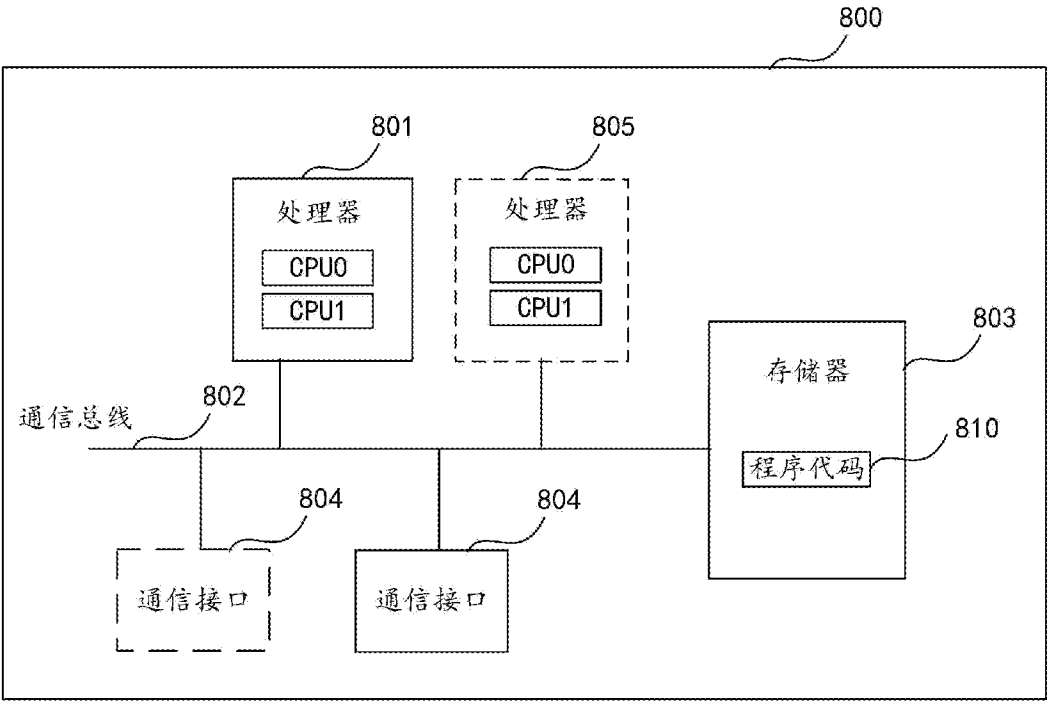


图 12

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2024/091039

A. CLASSIFICATION OF SUBJECT MATTER H04L 12/46(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) IPC:H04L 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, EPTXT, USTXT, WOTXT, IEEE: 分组, 报文, 路由, 类型, 边缘, 隧道, edge, ipsec sa, message, packet, pop, rt, tunnel, route, type, vpn, vrf		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 114338116 A (MAIPU COMMUNICATION TECHNOLOGY CO., LTD.) 12 April 2022 (2022-04-12) description, paragraphs [0043]-[0052]	1-54
A	CN 113472622 A (HUAWEI TECHNOLOGIES CO., LTD.) 01 October 2021 (2021-10-01) entire document	1-54
A	US 2011023090 A1 (CISCO TECHNOLOGY, INC.) 27 January 2011 (2011-01-27) entire document	1-54
☐ 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 “D” document cited by the applicant in the international application “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 29 July 2024		Date of mailing of the international search report 04 August 2024
Name and mailing address of the ISA/CN China National Intellectual Property Administration (ISA/ CN) China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088		Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2024/091039

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)		Publication date (day/month/year)
CN	114338116	A	12 April 2022	None		
CN	113472622	A	01 October 2021	None		
US	2011023090	A1	27 January 2011	US	8650618 B2	11 February 2014

A. 主题的分类

H04L 12/46(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)

IPC:H04L

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,EPTXT,USTXT,WOTXT,IEEE:分组,报文,路由,类型,边缘,隧道, edge,ipsec sa,message,packe
t,pop,rt,tunnel,route,type,vpn,vrf

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
A	CN 114338116 A (迈普通信技术股份有限公司) 2022年4月12日 (2022 - 04 - 12) 说明书第[0043]-[0052]段	1-54
A	CN 113472622 A (华为技术有限公司) 2021年10月1日 (2021 - 10 - 01) 全文	1-54
A	US 2011023090 A1 (CISCO TECH INC) 2011年1月27日 (2011 - 01 - 27) 全文	1-54

☐ 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

“D” 申请人在国际申请中引证的文件

“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

2024年7月29日

国际检索报告邮寄日期

2024年8月4日

ISA/CN的名称和邮寄地址

中国国家知识产权局
中国北京市海淀区蓟门桥西土城路6号 100088

授权官员

穆剑

电话号码 (+86) 0512-88995975

PCT/ISA/210 表(第2页) (2022年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2024/091039

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	114338116	A	2022年4月12日	无			
CN	113472622	A	2021年10月1日	无			
US	2011023090	A1	2011年1月27日	US	8650618	B2	2014年2月11日