(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 116436731 B
(45)授权公告日 2023.09.05

(21)申请号 202310708504.8
(22)申请日 2023.06.15
(65)同一申请的已公布的文献号
申请公布号 CN 116436731 A
(43)申请公布日 2023.07.14
(73)专利权人 众信方智(苏州)智能技术有限公司
地址 215000 江苏省苏州市自由贸易试验区苏州片区苏州工业园区金鸡湖大道88号人工智能产业园E3-901单元
(72)发明人 吴先亮 苏景堃 陈振亚
(74)专利代理机构 北京艾格律诗专利代理有限公司 11924
专利代理师 谢毅
(51)Int.Cl.
H04L 12/46(2006.01)
H04L 9/40(2022.01)
H04L 9/32(2006.01)
H04L 69/16(2022.01)
H04L 69/164(2022.01)
H04L 69/04(2022.01)
(56)对比文件
CN 103379009 A,2013.10.30
CN 116155649 A,2023.05.23
CN 116233071 A,2023.06.06
WO 2018161639 A1,2018.09.13
审查员 邹海芳

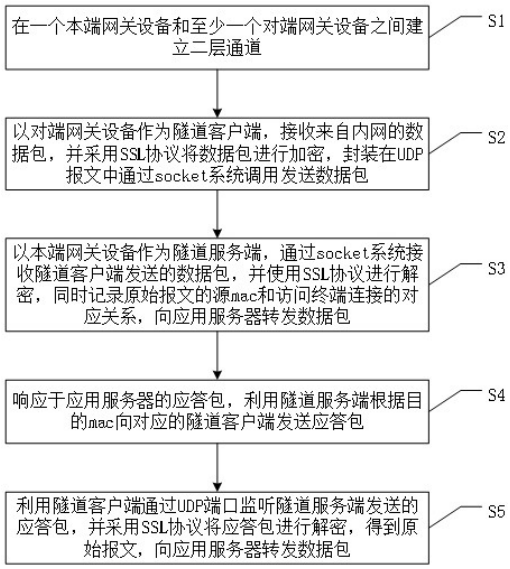
权利要求书3页 说明书9页 附图7页

(54)发明名称

一种多内网二层数据流通信方法

(57)摘要

本发明公开了一种多内网二层数据流通信方法。本发明在隧道客户端与隧道服务器之间架设起一个二层通道,在隧道客户端下的内网和隧道服务器下的内网之间建立了一个新的局域网,访问对端网络的网络资源就像访问本端网络的网络资源一样,实现了内部网络的互联互通,为工业互联网万物互联提供了坚实的网络架构,而且增加或减少内网数量也不会影响正常的业务,具有很好的扩展性。



CN 116436731 B

1.一种多内网二层数据流通信方法,其特征在于,包括以下步骤:

A1、在一个本端网关设备和至少一个对端网关设备之间建立二层通道;

A2、以对端网关设备作为隧道客户端,接收来自内网的数据包,并采用SSL协议将数据包进行加密,封装在UDP报文中通过socket系统调用发送数据包;具体包括:

响应于需要访问隧道服务端LAN侧应用服务器的隧道客户端LAN侧访问终端发出的ARP广播包,判断ARP广播包的目的地址是否为网桥mac;若是,则通过隧道客户端的LAN侧接口向同一网桥下的tap隧道接口转发ARP广播包;否则将ARP广播包转交给隧道客户端上层协议处理;

利用隧道客户端的tap隧道接口中的虚拟网卡驱动把从TCP/IP协议栈收到的数据包结构skb放入tap字符设备的读取队列,并利用隧道客户端的用户进程通过调用字符设备接口read获取完整的以太网数据帧,将核心态的skb传递给用户进程;

在隧道客户端的用户进程接收到数据包后使用SSL协议将以太网数据帧进行加密,然后封装在UDP报文中通过socket系统调用发送到隧道服务端;

A3、以本端网关设备作为隧道服务端,通过socket系统接收隧道客户端发送的数据包,并使用SSL协议进行解密,同时记录原始报文的源mac和访问终端连接的对应关系,向应用服务器转发数据包;

A4、响应于应用服务器的应答包,利用隧道服务端根据目的mac向对应的隧道客户端发送应答包;

A5、利用隧道客户端通过UDP端口监听隧道服务端发送的应答包,并采用SSL协议将应答包进行解密,得到原始报文,向应用服务器转发数据包。

2.根据权利要求1所述的一种多内网二层数据流通信方法,其特征在于,步骤A1具体包括:

在本端网关设备和至少一个对端网关设备分别创建一个tap设备和对应的tap隧道接口;

将本端网关设备的tap隧道接口和LAN侧接口通过同一网桥连接;

将对端网关设备的tap隧道接口和LAN侧接口通过同一网桥连接;

将本端网关设备的LAN侧设备IP地址和对端网关设备的LAN侧设备IP地址设置在同一子网中。

3.根据权利要求1所述的一种多内网二层数据流通信方法,其特征在于,步骤A3具体包括:

利用隧道服务端的用户进程在设定UDP端口上监听隧道客户端发送的数据包,在收到隧道客户端发送的数据包后先使用SSL协议进行解密,得到原始报文,然后记录下原始报文的源mac和连接的对应关系;

再调用虚拟网卡的字符处理程序write写入虚拟网卡的字符设备,设备驱动程序完成数据从用户态到核心态的复制,并将数据写入skb链表,然后调用网卡netif_rx()接收程序,数据包再次进入系统TCP/IP协议栈,并通过网桥转发到隧道服务端的LAN侧接口,由隧道服务端的LAN侧接口将数据包转发给应用服务器。

4.根据权利要求3所述的一种多内网二层数据流通信方法,其特征在于,步骤A5具体包括:

利用隧道客户端的用户进程在设定UDP端口上监听隧道服务端发送的ARP应答包，在收到隧道服务端发送的ARP应答包后先使用SSL协议进行解密，得到原始报文，然后通过隧道客户端的tap隧道接口向同一网桥下的LAN侧接口转发ARP应答包，由隧道客户端的LAN侧接口将数据包转发给隧道客户端LAN侧应用服务器，得到隧道服务端LAN侧应用服务器的mac地址。

5.一种多内网二层数据流通信方法，其特征在于，包括以下步骤：

B1、在一个本端网关设备和至少两个对端网关设备之间建立二层通道；

B2、以一个对端网关设备作为访问隧道客户端，接收来自内网的数据包，并采用SSL协议将数据包进行加密，封装在UDP报文中通过socket系统调用发送数据包；

B3、以本端网关设备作为隧道服务端，通过socket系统接收访问隧道客户端发送的数据包，并使用SSL协议进行解密，同时记录原始报文的源mac和访问终端连接的对应关系，向其它隧道客户端转发数据包；

B4、以另一个对端网关设备作为目标隧道客户端，通过UDP端口监听隧道服务端发送的数据包，并采用SSL协议将数据包进行解密，得到原始报文，向应用服务器转发数据包；

B5、响应于应用服务器的应答包，利用目标隧道客户端采用SSL协议将数据包进行加密，封装在UDP报文中通过socket系统调用发送数据包；

B6、利用隧道服务端通过socket系统接收目标隧道客户端发送的数据包，并使用SSL协议进行解密，根据目的mac向访问隧道客户端发送应答包；

B7、利用访问隧道客户端通过UDP端口监听隧道服务端发送的应答包，并采用SSL协议将应答包进行解密，得到原始报文，向应用服务器转发数据包。

6.根据权利要求5所述的一种多内网二层数据流通信方法，其特征在于，步骤B1具体包括：

在本端网关设备和至少两个对端网关设备分别创建一个tap设备和对应的tap隧道接口；

将本端网关设备的tap隧道接口和LAN侧接口通过同一网桥连接；

将对端网关设备的tap隧道接口和LAN侧接口通过同一网桥连接；

将本端网关设备的LAN侧设备IP地址和对端网关设备的LAN侧设备IP地址设置在同一子网中。

7.根据权利要求6所述的一种多内网二层数据流通信方法，其特征在于，步骤B2具体包括：

响应于访问隧道客户端LAN侧访问终端发出的ARP广播包，判断ARP广播包的目的地址是否为网桥mac；若是，则通过访问隧道客户端的LAN侧接口向同一网桥下的tap隧道接口转发ARP广播包；否则将ARP广播包转交给隧道客户端上层协议处理；

利用访问隧道客户端的tap隧道接口中的虚拟网卡驱动把从TCP/IP协议栈收到的数据包结构skb放入tap字符设备的读取队列，并利用隧道客户端的用户进程通过调用字符设备接口read获取完整的以太网数据帧，将核心态的skb传递给用户进程；

在访问隧道客户端的用户进程接收到数据包后使用SSL协议将以太网数据帧进行加密，然后封装在UDP报文中通过socket系统调用发送到隧道服务端。

8.根据权利要求7所述的一种多内网二层数据流通信方法，其特征在于，步骤B3具体包

括：

利用隧道服务端的用户进程在设定UDP端口上监听访问隧道客户端发送的数据包，在收到访问隧道客户端发送的数据包后先使用SSL协议进行解密，得到原始报文，然后记录下原始报文的源mac和连接的对应关系；

再调用虚拟网卡的字符处理程序write写入虚拟网卡的字符设备，设备驱动程序完成数据从用户态到核心态的复制，并将数据写入skb链表，然后调用网卡netif_rx()接收程序，数据包再次进入系统TCP/IP协议栈，并通过网桥转发到隧道服务端的LAN侧接口，由隧道服务端的LAN侧接口将数据包转发给应用服务器。

9.根据权利要求8所述的一种多内网二层数据流通信方法，其特征在于，步骤B4具体包括：

利用目标隧道客户端的用户进程在设定UDP端口上监听隧道服务端发送的ARP广播包，在收到隧道服务端发送的ARP广播包后先使用SSL协议进行解密，得到原始报文，然后通过目标隧道客户端的tap隧道接口向同一网桥下的LAN侧接口转发ARP广播包，由目标隧道客户端的LAN侧接口将数据包转发给目标隧道客户端LAN侧应用服务器。

一种多内网二层数据流通信方法

技术领域

[0001] 本发明涉及计算机网络领域,具体涉及一种多内网二层数据流通信方法。

背景技术

[0002] 远程访问内网资源是一种隧道技术,在互联网上架设了一个二层通道,建立了一个新的局域网,实现不同网关的内部网络的互联互通。

[0003] 此技术具有以下优势:

[0004] (1)可扩展性:新设备可以动态的添加,不会影响已组网的设备;

[0005] (2)高安全性:隧道通信流量使用SSL加密, 防止数据被监听;

[0006] (3)可管理性:服务端可以决定是否允许客户端的连接;

[0007] (4)透明性:对用户而言,访问对端网络的内部网络资源就像访问本端网络的资源一样,用户感知不到,也不关心具体的网络结构,增加或者减少设备数量都不会影响正常的业务。

[0008] 如图1所示,当因特网上有三个内网A、B、C,内网里分别建立了一个WEB服务,一个打印服务,一个文件共享服务,他们之间想要互相访问彼此的服务,且又不想把服务开放给互联网时,传统的VPN技术无法满足这个需求,传统的VPN只能将VPN服务器统一部署在一个地方,客户端从其他地方访问。使用传统的VPN,B和C能访问A处的WEB服务,但B和C无法互相访问对方的服务,A也无法访问B和C处的打印机和文件共享服务。

发明内容

[0009] 针对现有技术中的上述不足,本发明提供了一种多内网二层数据流通信方法。

[0010] 为了达到上述发明目的,本发明采用的技术方案为:

[0011] 一种多内网二层数据流通信方法,包括以下步骤:

[0012] A1、在一个本端网关设备和至少一个对端网关设备之间建立二层通道;

[0013] A2、以对端网关设备作为隧道客户端,接收来自内网的数据包,并采用SSL协议将数据包进行加密,封装在UDP报文中通过socket系统调用发送数据包;

[0014] A3、以本端网关设备作为隧道服务端,通过socket系统接收隧道客户端发送的数据包,并使用SSL协议进行解密,同时记录原始报文的源mac和访问终端连接的对应关系,向应用服务器转发数据包;

[0015] A4、响应于应用服务器的应答包,利用隧道服务端根据目的mac向对应的隧道客户端发送应答包;

[0016] A5、利用隧道客户端通过UDP端口监听隧道服务端发送的应答包,并采用SSL协议将应答包进行解密,得到原始报文,向应用服务器转发数据包。

[0017] 作为可选地,步骤A1具体包括:

[0018] 在本端网关设备和至少一个对端网关设备分别创建一个tap设备和对应的tap隧道接口;

[0019] 将本端网关设备的tap隧道接口和LAN侧接口通过同一网桥连接；

[0020] 将对端网关设备的tap隧道接口和LAN侧接口通过同一网桥连接；

[0021] 将本端网关设备的LAN侧设备IP地址和对端网关设备的LAN侧设备IP地址设置在同一子网中。

[0022] 作为可选地，步骤A2具体包括：

[0023] 响应于需要访问隧道服务端LAN侧应用服务器的隧道客户端LAN侧访问终端发出的ARP广播包，判断ARP广播包的目的地址是否为网桥mac；若是，则通过隧道客户端的LAN侧接口向同一网桥下的tap隧道接口转发ARP广播包；否则将ARP广播包转交给隧道客户端上层协议处理；

[0024] 利用隧道客户端的tap隧道接口中的虚拟网卡驱动把从TCP/IP协议栈收到的数据包结构skb放入tap字符设备的读取队列，并利用隧道客户端的用户进程通过调用字符设备接口read获取完整的以太网数据帧，将核心态的skb传递给用户进程；

[0025] 在隧道客户端的用户进程接收到数据包后使用SSL协议将以太网数据帧进行加密，然后封装在UDP报文中通过socket系统调用发送到隧道服务端。

[0026] 作为可选地，步骤A3具体包括：

[0027] 利用隧道服务端的用户进程在设定UDP端口上监听隧道客户端发送的数据包，在收到隧道客户端发送的数据包后先使用SSL协议进行解密，得到原始报文，然后记录下原始报文的源mac和连接的对应关系；

[0028] 再调用虚拟网卡的字符处理程序write写入虚拟网卡的字符设备，设备驱动程序完成数据从用户态到核心态的复制，并将数据写入skb链表，然后调用网卡netif_rx()接收程序，数据包再次进入系统TCP/IP协议栈，并通过网桥转发到隧道服务端的LAN侧接口，由隧道服务端的LAN侧接口将数据包转发给应用服务器。

[0029] 作为可选地，步骤A5具体包括：

[0030] 利用隧道客户端的用户进程在设定UDP端口上监听隧道服务端发送的ARP应答包，在收到隧道服务端发送的ARP应答包后先使用SSL协议进行解密，得到原始报文，然后通过隧道客户端的tap隧道接口向同一网桥下的LAN侧接口转发ARP应答包，由隧道客户端的LAN侧接口将数据包转发给隧道客户端LAN侧应用服务器，得到隧道服务端LAN侧应用服务器的mac地址。

[0031] 一种多内网二层数据流通信方法，包括以下步骤：

[0032] B1、在一个本端网关设备和至少两个对端网关设备之间建立二层通道；

[0033] B2、以一个对端网关设备作为访问隧道客户端，接收来自内网的数据包，并采用SSL协议将数据包进行加密，封装在UDP报文中通过socket系统调用发送数据包；

[0034] B3、以本端网关设备作为隧道服务端，通过socket系统接收访问隧道客户端发送的数据包，并使用SSL协议进行解密，同时记录原始报文的源mac和访问终端连接的对应关系，向其它隧道客户端转发数据包；

[0035] B4、以另一个对端网关设备作为目标隧道客户端，通过UDP端口监听隧道服务端发送的数据包，并采用SSL协议将数据包进行解密，得到原始报文，向应用服务器转发数据包；

[0036] B5、响应于应用服务器的应答包，利用目标隧道客户端采用SSL协议将数据包进行加密，封装在UDP报文中通过socket系统调用发送数据包；

[0037] B6、利用隧道服务端通过socket系统接收目标隧道客户端发送的数据包，并使用SSL协议进行解密，根据目的mac向访问隧道客户端发送应答包；

[0038] B7、利用访问隧道客户端通过UDP端口监听隧道服务端发送的应答包，并采用SSL协议将应答包进行解密，得到原始报文，向应用服务器转发数据包。

[0039] 作为可选地，步骤B1具体包括：

[0040] 在本端网关设备和至少两个对端网关设备分别创建一个tap设备和对应的tap隧道接口；

[0041] 将本端网关设备的tap隧道接口和LAN侧接口通过同一网桥连接；

[0042] 将对端网关设备的tap隧道接口和LAN侧接口通过同一网桥连接；

[0043] 将本端网关设备的LAN侧设备IP地址和对端网关设备的LAN侧设备IP地址设置在同一子网中。

[0044] 作为可选地，步骤B2具体包括：

[0045] 响应于访问隧道客户端LAN侧访问终端发出的ARP广播包，判断ARP广播包的目的地址是否为网桥mac；若是，则通过访问隧道客户端的LAN侧接口向同一网桥下的tap隧道接口转发ARP广播包；否则将ARP广播包转交给隧道客户端上层协议处理；

[0046] 利用访问隧道客户端的tap隧道接口中的虚拟网卡驱动把从TCP/IP协议栈收到的数据包结构skb放入tap字符设备的读取队列，并利用隧道客户端的用户进程通过调用字符设备接口read获取完整的以太网数据帧，将核心态的skb传递给用户进程；

[0047] 在访问隧道客户端的用户进程接收到数据包后使用SSL协议将以太网数据帧进行加密，然后封装在UDP报文中通过socket系统调用发送到隧道服务端。

[0048] 作为可选地，步骤B3具体包括：

[0049] 利用隧道服务端的用户进程在设定UDP端口上监听访问隧道客户端发送的数据包，在收到访问隧道客户端发送的数据包后先使用SSL协议进行解密，得到原始报文，然后记录下原始报文的源mac和连接的对应关系；

[0050] 再调用虚拟网卡的字符处理程序write写入虚拟网卡的字符设备，设备驱动程序完成数据从用户态到核心态的复制，并将数据写入skb链表，然后调用网卡netif_rx()接收程序，数据包再次进入系统TCP/IP协议栈，并通过网桥转发到隧道服务端的LAN侧接口，由隧道服务端的LAN侧接口将数据包转发给应用服务器。

[0051] 作为可选地，步骤B4具体包括：

[0052] 利用目标隧道客户端的用户进程在设定UDP端口上监听隧道服务端发送的ARP广播包，在收到隧道服务端发送的ARP广播包后先使用SSL协议进行解密，得到原始报文，然后通过目标隧道客户端的tap隧道接口向同一网桥下的LAN侧接口转发ARP广播包，由目标隧道客户端的LAN侧接口将数据包转发给目标隧道客户端LAN侧应用服务器。

[0053] 本发明具有以下有益效果：

[0054] (1)本发明在隧道客户端与隧道服务器、隧道客户端之间架设起一个二层通道，在隧道客户端下的内网和隧道服务器下的内网之间建立了一个新的局域网，访问对端网络的网络资源就像访问本端网络的网络资源一样，实现了内部网络的互联互通，为工业互联网万物互联提供了坚实的网络架构，而且增加或减少内网数量也不会影响正常的业务，具有很好的扩展性。

[0055] (2)本发明采用1对n的组网方式,能够很方便的扩充局域网设备。

[0056] (3)本发明的多个隧道客户端之间既可以配置成能够互相访问,也可以配置成相互隔离。如果配置成互相访问,这时隧道客户端的内网设备既能访问隧道服务端的内网资源,又能访问其它隧道客户端的内网资源;如果配置成相互隔离,这时隧道客户端的内网设备只能访问服务端的内网资源。

[0057] (4)本发明通过SSL证书进行鉴权,每个隧道客户端可以有不同的证书,隧道服务端可以决定是否允许客户端的连接,提高安全性。

[0058] (5)本发明的隧道通信流量使用TLS/SSL加密, 保证数据传输的安全。

[0059] (6)本发明通过数据的压缩,提高数据传输的速度。

[0060] (7)本发明使用特定的udp或tcp端口实现隧道客户端和隧道服务端之间的连接。

附图说明

[0061] 图1为多内网网络拓扑示意图;

[0062] 图2为本实施例1中一种多内网二层数据流通信方法流程示意图;

[0063] 图3为本实施例1中应用场景示意图;

[0064] 图4为本实施例1中数据包收发流程示意图;

[0065] 图5为本实施例1中隧道客户端发送流程图;

[0066] 图6为本实施例1中隧道服务端发送流程图;

[0067] 图7为本实施例2中一种多内网二层数据流通信方法流程示意图。

具体实施方式

[0068] 下面对本发明的具体实施方式进行描述,以便于本技术领域的技术人员理解本发明,但应该清楚,本发明不限于具体实施方式的范围,对本技术领域的普通技术人员来讲,只要各种变化在所附的权利要求限定和确定的本发明的精神和范围内,这些变化是显而易见的,一切利用本发明构思的发明创造均在保护之列。

[0069] 由于当前VPN技术基本都是在三层上进行互联,对于有二层互联需求的客户无法满足,更为重要的是,不支持在VPN客户端内部网络之间的互相访问,VPN服务器端的内网设备也无法访问客户端的内部网络,因此本发明为了解决该问题提出了一种实现多内网之间互访,透传二层数据流的技术方案。

[0070] 实施例1:

[0071] 如图2至图6所示,本发明实施例提供了一种多内网二层数据流通信方法,包括以下步骤A1至A5:

[0072] A1、在一个本端网关设备和至少一个对端网关设备之间建立二层通道;

[0073] 在本实施例中,步骤A1具体包括:

[0074] 在本端网关设备和至少一个对端网关设备分别创建一个tap设备和对应的tap隧道接口;

[0075] 将本端网关设备的tap隧道接口和LAN侧接口通过同一网桥连接;

[0076] 将对端网关设备的tap隧道接口和LAN侧接口通过同一网桥连接;

[0077] 将本端网关设备的LAN侧设备IP地址和对端网关设备的LAN侧设备IP地址设置在

同一子网中。

[0078] 具体而言，如图3所示，分别位于互联网不同地方的内网A、B、C，他们在自己本地的网络中分别装有WEB服务器、文件共享服务器、打印服务器，他们都通过网关连接到互联网上。其中内网A的网关作为隧道服务端，内网B和C的网关作为隧道客户端。

[0079] 以隧道客户端B的访问终端访问隧道服务端A的WEB服务器为例，在隧道服务端A和隧道客户端B的支持tap设备的网关设备上，创建一个tap设备，一个tap设备既是一个虚拟网卡设备，也是一个字符设备。隧道客户端B向隧道服务端A发起连接，当隧道客户端B成功连接到隧道服务端A后，创建一个tap隧道接口，使用如下命令：

[0080] brctl addif br-lan tap0

[0081] brctl addif br-lan eth0

[0082] 将该tap隧道接口和LAN侧的eth0接口放在同一个网桥br-lan下面，这样数据包就能在LAN接口和tap设备接口之间进行转发。

[0083] 并且配置隧道客户端B和隧道服务端A的LAN侧设备的IP在同一个子网中，这样它们就能够像在同一个局域网中一样互相访问，从而建立在隧道服务端A和隧道客户端B虚拟网卡之上的虚拟局域网网络。

[0084] A2、以对端网关设备作为隧道客户端，接收来自内网的数据包，并采用SSL协议将数据包进行加密，封装在UDP报文中通过socket系统调用发送数据包；

[0085] 在本实施例中，步骤A2具体包括：

[0086] 响应于需要访问隧道服务端LAN侧应用服务器的隧道客户端LAN侧访问终端发出的ARP广播包，判断ARP广播包的目的地址是否为网桥mac；若是，则通过隧道客户端的LAN侧接口向同一网桥下的tap隧道接口转发ARP广播包；否则将ARP广播包转交给隧道客户端上层协议处理；

[0087] 利用隧道客户端的tap隧道接口中的虚拟网卡驱动把从TCP/IP协议栈收到的数据包结构skb放入tap字符设备的读取队列，并利用隧道客户端的用户进程通过调用字符设备接口read获取完整的以太网数据帧，将核心态的skb传递给用户进程；

[0088] 在隧道客户端的用户进程接收到数据包后使用SSL协议将以太网数据帧进行加密，然后封装在UDP报文中通过socket系统调用发送到隧道服务端。

[0089] 具体而言，当隧道客户端B的访问终端在浏览器中输入192.168.1.10想要访问隧道服务端A的LAN侧的WEB服务时，由于192.168.1.10和隧道客户端B的访问终端的ip地址在同一个子网，所以隧道客户端B的访问终端首先会发送一个ARP广播包，请求192.168.1.10的mac地址。

[0090] 然后隧道客户端B在LAN侧的eth0接口收到该ARP广播包后，会向eth0接口所在网桥的其他接口转发该报文。由于之前在配置时已将隧道客户端B的tap0接口加入该网桥，所以会执行到tap0接口的发送函数。

[0091] tap接口的虚拟网卡驱动把从TCP/IP协议栈收到的数据包结构skb放于tap字符设备的读取队列，然后隧道客户端B的用户进程通过调用字符设备接口read获取完整的以太网数据帧，字符驱动read函数的功能是从设备的读取队列读取数据，将核心态的skb传递给用户进程。

[0092] 隧道客户端B的用户进程接收到数据包后使用SSL协议将这些以太网数据帧进行

加密,然后封装在UDP报文中通过socket系统调用发送到隧道服务端A。

[0093] A3、以本端网关设备作为隧道服务端,通过socket系统接收隧道客户端发送的数据包,并使用SSL协议进行解密,同时记录原始报文的源mac和访问终端连接的对应关系,向应用服务器转发数据包;

[0094] 在本实施例中,步骤A3具体包括:

[0095] 利用隧道服务端的用户进程在设定UDP端口上监听隧道客户端发送的数据包,在收到隧道客户端发送的数据包后先使用SSL协议进行解密,得到原始报文,然后记录下原始报文的源mac和连接的对应关系;

[0096] 再调用虚拟网卡的字符处理程序write写入虚拟网卡的字符设备,设备驱动程序完成数据从用户态到核心态的复制,并将数据写入skb链表,然后调用网卡netif_rx()接收程序,数据包再次进入系统TCP/IP协议栈,并通过网桥转发到隧道服务端的LAN侧接口,由隧道服务端的LAN侧接口将数据包转发给应用服务器。

[0097] 具体而言,隧道服务端A的用户进程在指定的UDP端口上面进行监听,当收到隧道客户端B过来的数据包时,先使用SSL协议进行解密,得到原始报文,然后记录下原始报文的源mac和连接的对应关系。

[0098] 然后调用虚拟网卡的字符处理程序write写入虚拟网卡的字符设备,设备驱动程序完成数据从用户态到核心态的复制,并将数据写入skb链表,然后调用网卡netif_rx()接收程序,数据包再次进入系统TCP/IP协议栈,此时协议栈收到的数据包就是隧道客户端LAN侧的收到的数据包,由于之前已经将隧道服务端的LAN接口和tap接口配置在同一个网桥下面,所以收到的数据包会通过网桥转发到隧道服务端的LAN侧接口。由于收到的是广播包,所以会向所有的隧道客户端连接转发该数据包,同时也会向隧道服务端tap接口所在的网桥转发该数据包。

[0099] A4、响应于应用服务器的应答包,利用隧道服务端根据目的mac向对应的隧道客户端发送应答包;

[0100] 在本实施例中,当arp广播包经过隧道服务端A的LAN侧接口eth0到达WEB服务器后,由于WEB服务器的地址就是arp请求的地址,所以WEB服务器会发送arp应答。

[0101] 隧道服务端A收到arp应答后,根据目的mac找到对应客户端的连接发送该数据包。

[0102] A5、利用隧道客户端通过UDP端口监听隧道服务端发送的应答包,并采用SSL协议将应答包进行解密,得到原始报文,向应用服务器转发数据包。

[0103] 在本实施例中,步骤A5具体包括:

[0104] 利用隧道客户端的用户进程在设定UDP端口上监听隧道服务端发送的ARP应答包,在收到隧道服务端发送的ARP应答包后先使用SSL协议进行解密,得到原始报文,然后通过隧道客户端的tap隧道接口向同一网桥下的LAN侧接口转发ARP应答包,由隧道客户端的LAN侧接口将数据包转发给隧道客户端LAN侧应用服务器,得到隧道服务端LAN侧应用服务器的mac地址。

[0105] 具体而言,隧道客户端B的用户进程在指定的UDP端口上面进行监听,当收到隧道服务端A过来的应答包时,先使用SSL协议进行解密,得到原始报文,然后向网桥上的其它接口转发该ARP应答包。

[0106] 当隧道客户端B的访问终端收到了该应答包后,就完成了一次数据的交互,此时隧

道客户端B的访问终端也知道了WEB服务器端的mac地址，然后就可以开始进行http报文的交互过程了。

[0107] 实施例2：

[0108] 如图7所示，本发明实施例提供了一种多内网二层数据流通信方法，包括以下步骤B1至B8：

[0109] B1、在一个本端网关设备和至少两个对端网关设备之间建立二层通道；

[0110] 在本实施例中，步骤B1具体包括：

[0111] 在本端网关设备和至少两个对端网关设备分别创建一个tap设备和对应的tap隧道接口；

[0112] 将本端网关设备的tap隧道接口和LAN侧接口通过同一网桥连接；

[0113] 将对端网关设备的tap隧道接口和LAN侧接口通过同一网桥连接；

[0114] 将本端网关设备的LAN侧设备IP地址和对端网关设备的LAN侧设备IP地址设置在同一子网中。

[0115] 具体而言，分别位于互联网不同地方的内网A、B、C，他们在自己本地的网络中分别装有WEB服务器、文件共享服务器、打印服务器，他们都通过网关连接到互联网上。其中内网A的网关作为隧道服务端，内网B的网关作为目标隧道客户端，内网C的网关作为访问隧道客户端。

[0116] 以访问隧道客户端C的访问终端访问目标隧道客户端B的文件共享服务器为例，目标隧道客户端B和访问隧道客户端C向隧道服务端A发起连接，当隧道客户端成功连接到隧道服务端后，创建一个tap隧道接口，分别使用如下命令：

[0117] brctl addif br-lan tap0

[0118] brctl addif br-lan eth0

[0119] 将该tap隧道接口和LAN侧的eth0接口放在一个网桥br-lan下面，这样数据包就能在LAN接口和tap设备接口之间进行转发。

[0120] 并且配置目标隧道客户端B、访问隧道客户端C和隧道服务端A的LAN侧设备的IP在同一个子网中，这样它们就能够像在同一个局域网中一样互相访问，从而建立在目标隧道客户端B、访问隧道客户端C和隧道服务端A之上的虚拟局域网网络。

[0121] B2、以一个对端网关设备作为访问隧道客户端，接收来自内网的数据包，并采用SSL协议将数据包进行加密，封装在UDP报文中通过socket系统调用发送数据包；

[0122] 在本实施例中，步骤B2具体包括：

[0123] 响应于访问隧道客户端LAN侧访问终端发出的ARP广播包，判断ARP广播包的目的地址是否为网桥mac；若是，则通过访问隧道客户端的LAN侧接口向同一网桥下的tap隧道接口转发ARP广播包；否则将ARP广播包转交给隧道客户端上层协议处理；

[0124] 利用访问隧道客户端的tap隧道接口中的虚拟网卡驱动把从TCP/IP协议栈收到的数据包结构skb放入tap字符设备的读取队列，并利用隧道客户端的用户进程通过调用字符设备接口read获取完整的以太网数据帧，将核心态的skb传递给用户进程；

[0125] 在访问隧道客户端的用户进程接收到数据包后使用SSL协议将以太网数据帧进行加密，然后封装在UDP报文中通过socket系统调用发送到隧道服务端。

[0126] 具体而言，当访问隧道客户端C的访问终端想要访问目标隧道客户端B的 LAN侧的

文件共享服务器时，由于文件共享服务器的IP和访问隧道客户端C的ip地址在同一个子网，所以访问隧道客户端C的访问终端首先会发送一个ARP广播包，请求文件共享服务器的mac地址。

[0127] 访问隧道客户端C在eth0口收到该ARP广播包后，会向eth0所在网桥的其他接口转发该报文。由于之前在配置时已将隧道客户端的tap0接口加入该网桥，所以会执行到tap0接口的发送函数。

[0128] tap接口的虚拟网卡驱动把从TCP/IP协议栈收到的数据包放入tap字符设备的读取队列，访问隧道客户端C的用户进程通过调用字符设备接口read获取完整的以太网数据帧。

[0129] 访问隧道客户端C的用户进程接收到数据包后使用SSL协议将这些以太网数据帧进行加密，然后封装在UDP报文中通过socket系统调用发送到隧道服务端。

[0130] B3、以本端网关设备作为隧道服务端，通过socket系统接收访问隧道客户端发送的数据包，并使用SSL协议进行解密，同时记录原始报文的源mac和访问终端连接的对应关系，向其它隧道客户端转发数据包；

[0131] 在本实施例中，步骤B3具体包括：

[0132] 利用隧道服务端的用户进程在设定UDP端口上监听访问隧道客户端发送的数据包，在收到访问隧道客户端发送的数据包后先使用SSL协议进行解密，得到原始报文，然后记录下原始报文的源mac和连接的对应关系；

[0133] 再调用虚拟网卡的字符处理程序write写入虚拟网卡的字符设备，设备驱动程序完成数据从用户态到核心态的复制，并将数据写入skb链表，然后调用网卡netif_rx()接收程序，数据包再次进入系统TCP/IP协议栈，并通过网桥转发到隧道服务端的LAN侧接口，由隧道服务端的LAN侧接口将数据包转发给应用服务器。

[0134] 具体而言，隧道服务端A的用户进程在指定的UDP端口上面进行监听，当收到访问隧道客户端C过来的数据包时，先使用SSL协议进行解密，得到原始报文，然后记录下原始报文的源mac和连接的对应关系。由于收到的是广播包，所以会向所有的隧道客户端连接转发该数据包，同时也会向隧道服务端tap接口所在的网桥转发该数据包。

[0135] B4、以另一个对端网关设备作为目标隧道客户端，通过UDP端口监听隧道服务端发送的数据包，并采用SSL协议将数据包进行解密，得到原始报文，向应用服务器转发数据包；

[0136] 在本实施例中，步骤B4具体包括：

[0137] 利用目标隧道客户端的用户进程在设定UDP端口上监听隧道服务端发送的ARP广播包，在收到隧道服务端发送的ARP广播包后先使用SSL协议进行解密，得到原始报文，然后通过目标隧道客户端的tap隧道接口向同一网桥下的LAN侧接口转发ARP广播包，由目标隧道客户端的LAN侧接口将数据包转发给目标隧道客户端LAN侧应用服务器。

[0138] 具体而言，目标隧道客户端B的用户进程在指定的UDP端口上面进行监听，当收到隧道服务端A过来的ARP广播包时，先使用SSL协议进行解密，得到原始报文，然后向网桥上的其它接口转发该ARP应答包。

[0139] B5、响应于应用服务器的应答包，利用目标隧道客户端采用SSL协议将数据包进行加密，封装在UDP报文中通过socket系统调用发送数据包；

[0140] 在本实施例中，当文件共享服务器收到了ARP请求包后，由于所请求的地址就是它

自己的地址,所以文件共享服务器会发送一个ARP应答包。

[0141] 目标隧道客户端B收到来自LAN侧接口的ARP应答包后,会通过socket系统发送给隧道服务端A。

[0142] B6、利用隧道服务端通过socket系统接收目标隧道客户端发送的数据包,并使用SSL协议进行解密,根据目的mac向访问隧道客户端发送应答包;

[0143] B7、利用访问隧道客户端通过UDP端口监听隧道服务端发送的应答包,并采用SSL协议将应答包进行解密,得到原始报文,向应用服务器转发数据包。

[0144] 在本实施例中,访问隧道客户端C的用户程序在指定的UDP端口上面进行监听,当收到隧道服务端A过来的应答包时,先使用SSL协议进行解密,得到原始报文,然后向网桥上的其它接口转发该ARP应答包。

[0145] 当内网C的访问终端收到了该应答包后,就完成了一次数据的交互,经此交互,内网C的访问终端就知道了目标隧道客户端BLAN侧文件共享服务器的mac地址,然后就可以进行文件共享协议报文的交互了。

[0146] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0147] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0148] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0149] 本发明中应用了具体实施例对本发明的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本发明的方法及其核心思想;同时,对于本领域的一般技术人员,依据本发明的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本发明的限制。

[0150] 本领域的普通技术人员将会意识到,这里所述的实施例是为了帮助读者理解本发明的原理,应被理解为本发明的保护范围并不局限于这样的特别陈述和实施例。本领域的普通技术人员可以根据本发明公开的这些技术启示做出各种不脱离本发明实质的其它各种具体变形和组合,这些变形和组合仍然在本发明的保护范围内。

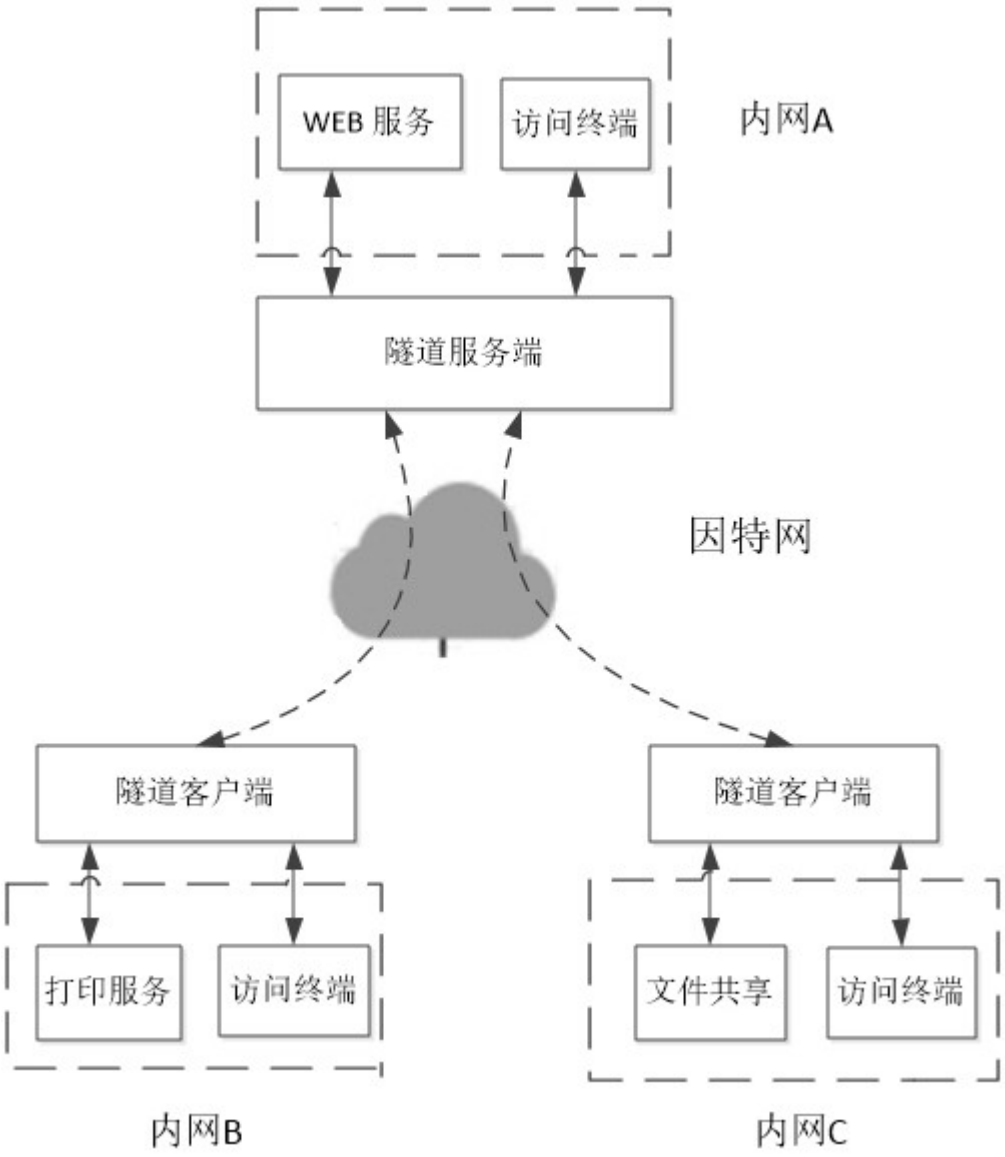

WEB 服务
访问终端
内网A
隧道服务端
因特网
隧道客户端
隧道客户端
打印服务
访问终端
文件共享
访问终端
内网B
内网C

图 1

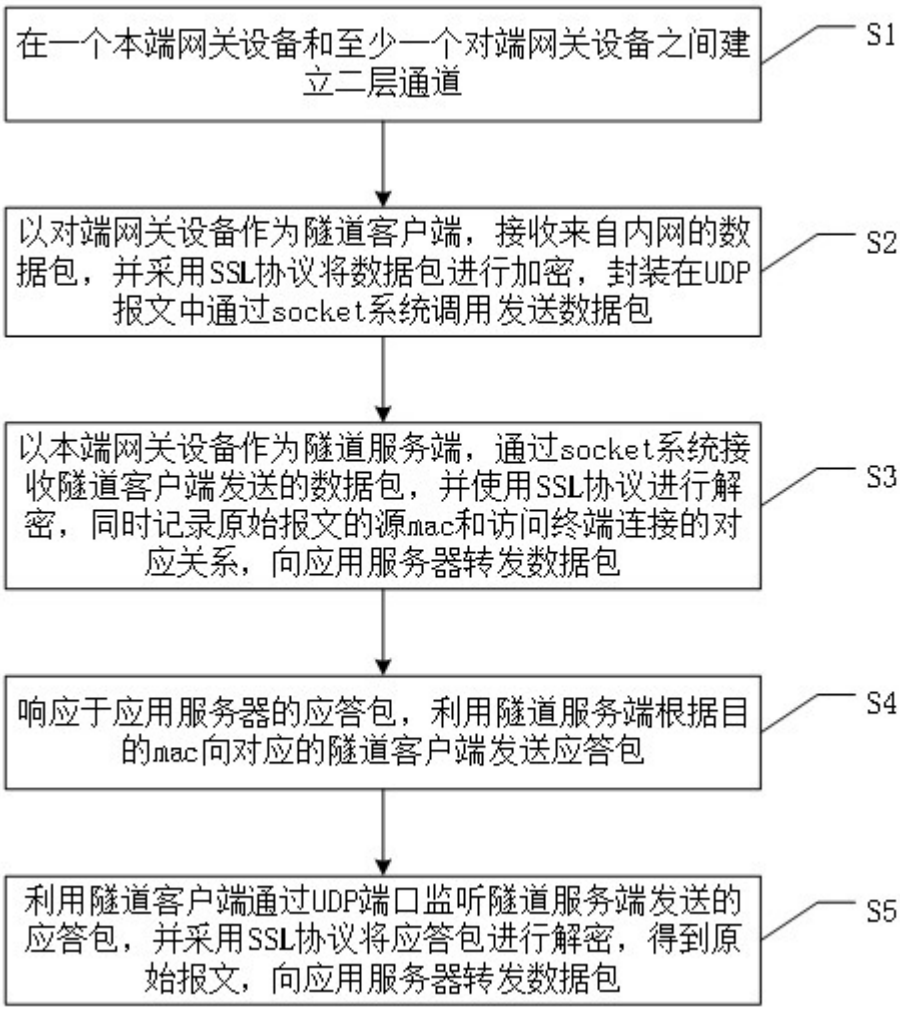

在一个本端网关设备和至少一个对端网关设备之间建立二层通道
S1
以对端网关设备作为隧道客户端，接收来自内网的数据包，并采用SSL协议将数据包进行加密，封装在UDP报文中通过socket系统调用发送数据包
S2
以本端网关设备作为隧道服务端，通过socket系统接收隧道客户端发送的数据包，并使用SSL协议进行解密，同时记录原始报文的源mac和访问终端连接的对应关系，向应用服务器转发数据包
S3
响应于应用服务器的应答包，利用隧道服务端根据目的mac向对应的隧道客户端发送应答包
S4
利用隧道客户端通过UDP端口监听隧道服务端发送的应答包，并采用SSL协议将应答包进行解密，得到原始报文，向应用服务器转发数据包
S5

图 2

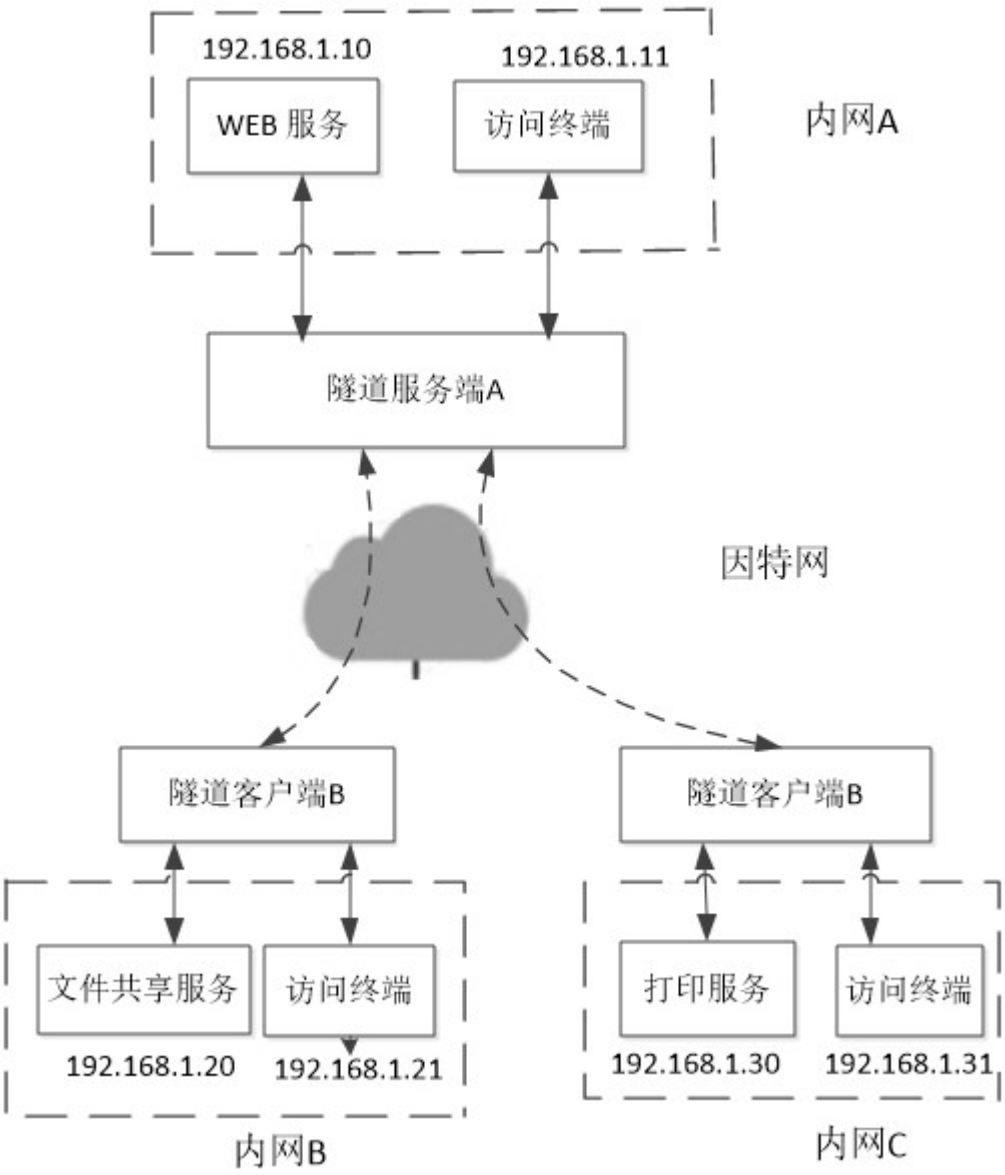

192.168.1.10
192.168.1.11
WEB 服务
访问终端
内网A
隧道服务端A
因特网
隧道客户端B
隧道客户端B
文件共享服务
访问终端
192.168.1.20
192.168.1.21
内网B
打印服务
访问终端
192.168.1.30
192.168.1.31
内网C

图 3

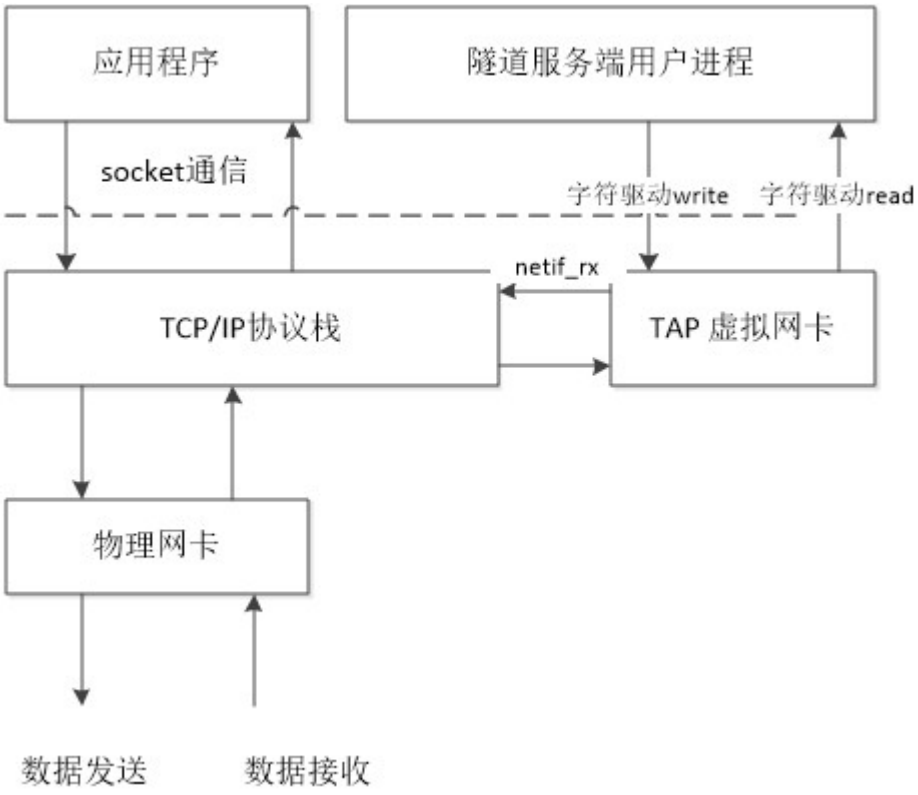

应用程序
隧道服务端用户进程
socket通信
字符驱动write
字符驱动read
netif_rx
TCP/IP协议栈
TAP 虚拟网卡
物理网卡
数据发送
数据接收

图 4

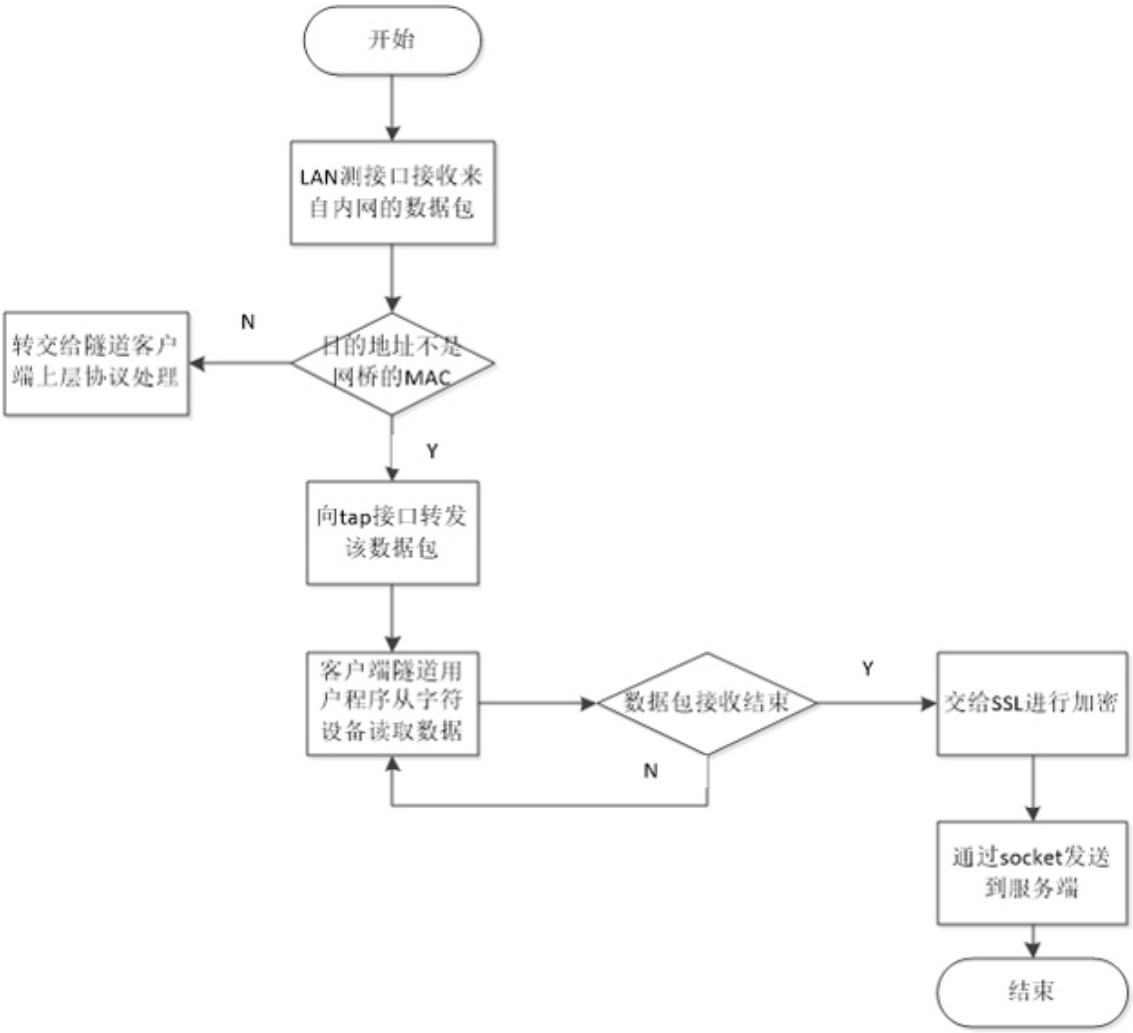

开始
LAN测接口接收来自内网的数据包
目的地址不是网桥的MAC
N
转交给隧道客户端上层协议处理
Y
向tap接口转发该数据包
客户端隧道用户程序从字符设备读取数据
数据包接收结束
Y
N
交给SSL进行加密
通过socket发送到服务端
结束

图 5

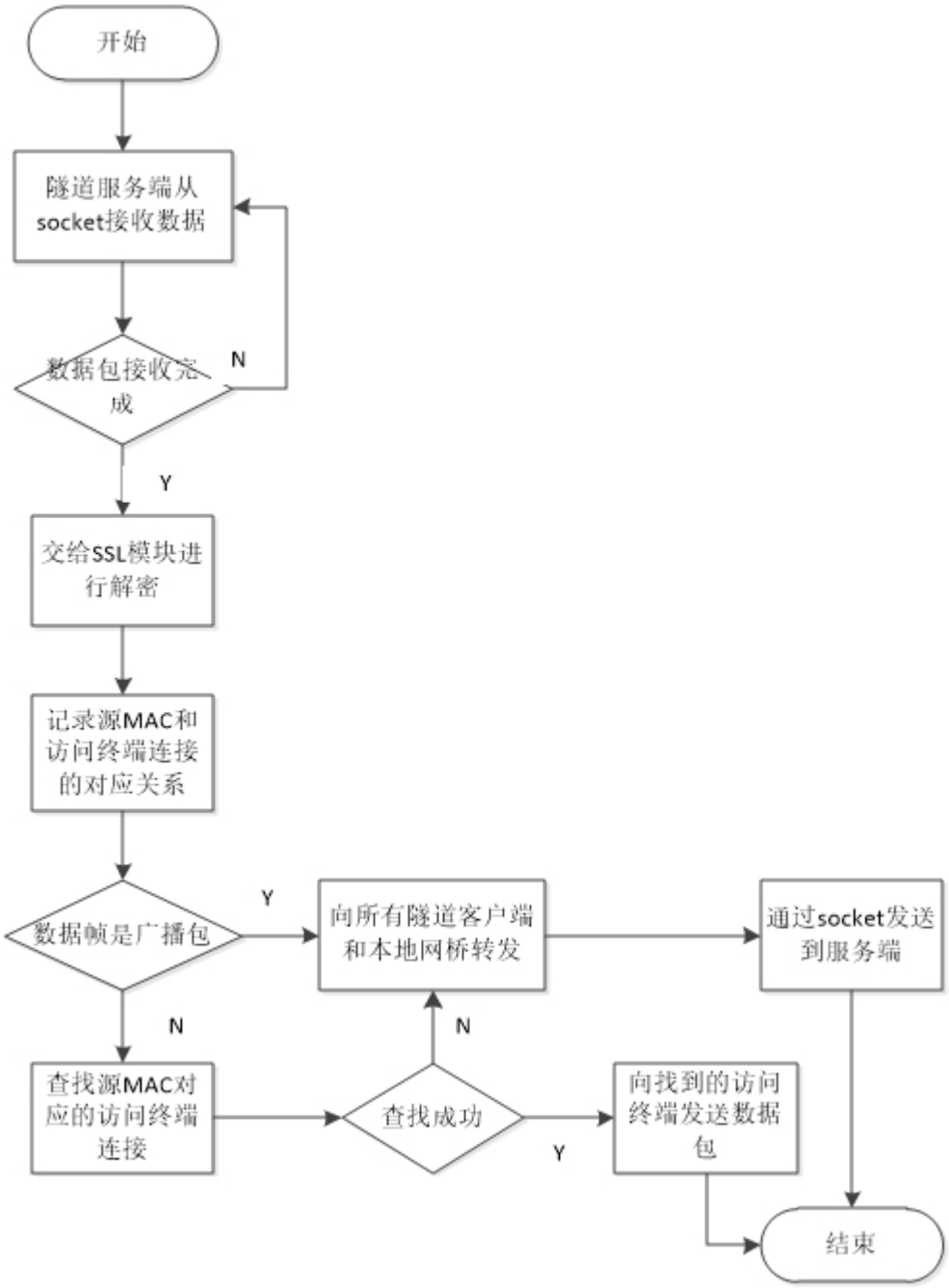

开始
隧道服务端从socket接收数据
数据包接收完成
N
Y
交给SSL模块进行解密
记录源MAC和访问终端连接的对应关系
数据帧是广播包
Y
向所有隧道客户端和本地网桥转发
通过socket发送到服务端
N
N
查找源MAC对应的访问终端连接
查找成功
Y
向找到的访问终端发送数据包
结束

图 6

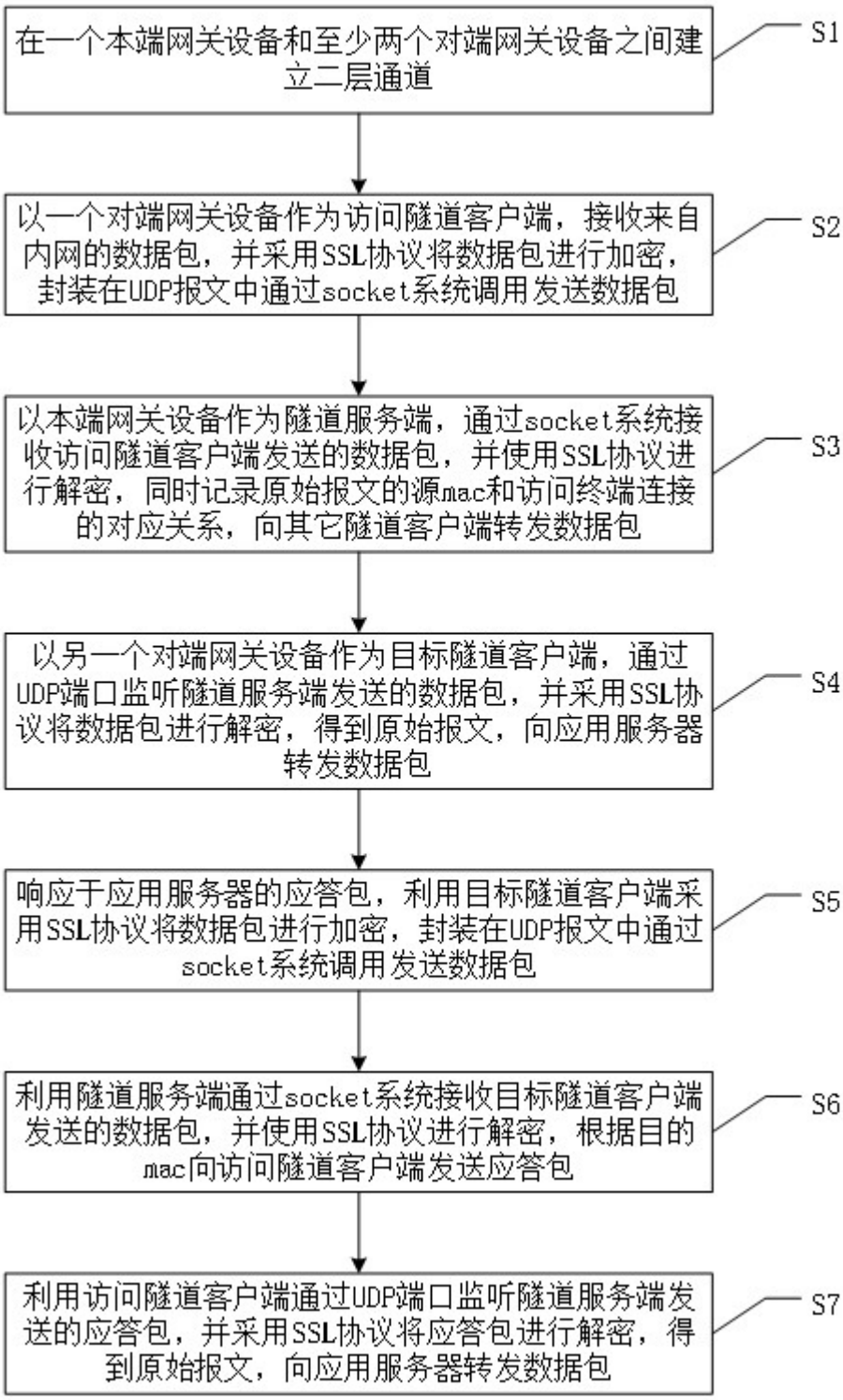

在一个本端网关设备和至少两个对端网关设备之间建立二层通道
S1
以一个对端网关设备作为访问隧道客户端，接收来自内网的数据包，并采用SSL协议将数据包进行加密，封装在UDP报文中通过socket系统调用发送数据包
S2
以本端网关设备作为隧道服务端，通过socket系统接收访问隧道客户端发送的数据包，并使用SSL协议进行解密，同时记录原始报文的源mac和访问终端连接的对应关系，向其它隧道客户端转发数据包
S3
以另一个对端网关设备作为目标隧道客户端，通过UDP端口监听隧道服务端发送的数据包，并采用SSL协议将数据包进行解密，得到原始报文，向应用服务器转发数据包
S4
响应于应用服务器的应答包，利用目标隧道客户端采用SSL协议将数据包进行加密，封装在UDP报文中通过socket系统调用发送数据包
S5
利用隧道服务端通过socket系统接收目标隧道客户端发送的数据包，并使用SSL协议进行解密，根据目的mac向访问隧道客户端发送应答包
S6
利用访问隧道客户端通过UDP端口监听隧道服务端发送的应答包，并采用SSL协议将应答包进行解密，得到原始报文，向应用服务器转发数据包
S7

图 7