[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/46 (2006.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200810225633.7

[43] 公开日 2009 年 6 月 3 日

[11] 公开号 CN 101447907A

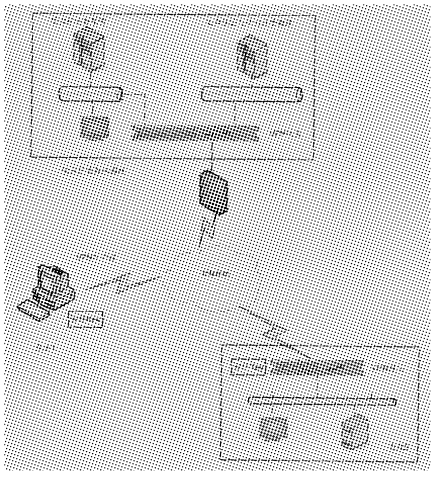
[22] 申请日 2008.10.31
[21] 申请号 200810225633.7
[71] 申请人 北京东方中讯联合认证技术有限公司
地址 101300 北京市顺义区李桥镇龙塘路 78 号
[72] 发明人 曾燕珲 戚天龙 余耀辉 尹志兵 姜 峰
[74] 专利代理机构 北京集佳知识产权代理有限公司
代理人 逯长明
权利要求书 3 页 说明书 10 页 附图 5 页

[54] 发明名称

VPN 安全接入方法及系统

[57] 摘要

本发明涉及网络安全技术领域，提供一种 VPN 安全接入方法和系统及其 VPN 客户端。其中的 VPN 安全接入方法是在 VPN 客户端中采用硬件设备 Key，VPN 客户端向网络侧发起接入请求，接入请求经所述硬件设备 Key 签名和加密；网络侧接收到所述接入请求后，对 VPN 客户端进行身份认证，认证通过后，与 VPN 客户端建立安全通道；VPN 客户端通过硬件设备 Key 以及安全通道与网络侧进行安全业务交互。本发明将安全接入、高强度用户身份认证以及计时计费模块无缝集成在一起，提供了一整套的安全接入解决方案，在保证网络安全的同时降低了系统部署和运行维护的难度，大大方便了用户的使用。



1、一种 VPN 安全接入方法，其特征在于，在 VPN 客户端中采用硬件设备 Key；所述方法还包括：

所述 VPN 客户端向网络侧发起接入请求，所述接入请求经所述硬件设备 Key 签名和加密；

网络侧接收到所述接入请求后，对所述 VPN 客户端进行身份认证，认证通过后，与所述 VPN 客户端建立安全通道；

所述 VPN 客户端通过硬件设备 Key 以及所述安全通道与网络侧进行安全业务交互。

2、根据权利要求 1 所述的 VPN 安全接入方法，其特征在于，所述 VPN 客户端根据所连接的网址自动触发接入请求，或者，所述 VPN 客户端向网络侧发起的接入请求由用户触发发起。

3、根据权利要求 1 所述的 VPN 安全接入方法，其特征在于，所述网络侧通过第三方对所述 VPN 客户端进行身份认证。

4、根据权利要求 1 所述的 VPN 安全接入方法，其特征在于，所述对 VPN 客户端身份认证通过后，进一步包括：判断所述 VPN 客户端是否满足访问条件，若满足再执行后续操作，否则结束。

5、根据权利要求 1 所述的 VPN 安全接入方法，其特征在于，所述 VPN 客户端通过硬件设备 Key 以及所述安全通道与网络侧进行安全业务交互的步骤包括：

所述 VPN 客户端将待发送业务数据通过所述硬件设备 Key 加密后，再通过所述安全通道发送至网络侧；

所述 VPN 客户端由接收单元通过所述安全通道接收来自网络侧的业务数据，将所述接收到的业务数据通过所述硬件设备 Key 解密后，呈现给用户。

6、一种 VPN 安全接入系统，其特征在于，该系统包括：

VPN 网关，用于将接收到的来自 VPN 客户端的接入请求发送给安全认证模块，将身份认证结果返回给所述 VPN 客户端；当所述身份认证结果为认证通过时，与所述 VPN 客户端建立安全通道；

安全认证模块，用于根据接收到的接入请求对所述 VPN 客户端进行身份

认证，给所述 VPN 网关返回身份认证结果；

包含硬件设备 Key 的 VPN 客户端，用于向网络侧发起接入请求，所述接入请求经所述硬件设备 Key 加密；通过硬件设备 Key 以及所述安全通道与业务系统进行安全业务交互；

业务系统，用于与所述 VPN 客户端通过所述安全通道进行安全业务交互。

7、根据权利要求 6 所述的 VPN 安全接入系统，其特征在于，所述系统还包括：计时计费模块，

所述 VPN 网关，接收到来自所述安全认证模块返回的身份认证通过结果后，通知计时计费模块，接收到来自所述计时计费模块的满足访问条件的通知时，再与所述 VPN 客户端建立安全通道；接收到来自所述计时计费模块的不满足访问条件的通知时，结束；

所述计时计费模块，用于接收来自所述 VPN 网关的计时计费请求，判断所述 VPN 客户端是否满足访问条件，通知所述 VPN 网关返回判断结果。

8、根据权利要求 7 所述的 VPN 安全接入系统，其特征在于，所述 VPN 网关通过同一协议与安全认证模块和计时计费模块进行通信，实现 VPN 网关、安全认证模块和计时计费模块三方的无缝集成。

9、一种 VPN 客户端，其特征在于，该 VPN 客户端包括：

安全接入请求单元，用于向 VPN 网关发起安全接入请求，经过客户端身份认证，虚拟地址分配以及访问权限检查后，触发安全通道建立单元进行下一步工作；

安全通道建立单元，用于在 VPN 客户端与 VPN 网关之间建立安全通道；

发送单元，用于将待发送数据传送给硬件设备 Key 进行加密和认证，并将加密后重新打包的数据通过安全通道发送出去；

接收单元，用于将经安全通道接收到的加密安全业务数据传递给硬件设备 Key 进行解密和认证，然后呈现给用户；

硬件设备 Key，用于存储 VPN 客户端安全信息以及完成各种安全算法，并对接收到的待加密信息进行加密，将加密后的信息传送给发送单元；将接收到的加密安全业务数据进行解密，将解密后的安全业务数据传送给接收单元；

通道管理单元，用于安全通道的监管和维护。

10、根据权利要求9所述的VPN客户端，进一步包括:

通道识别单元，用于确认所述VPN客户端所连接的网址涉及安全业务时，触发安全接入请求单元；所述VPN客户端所连接的网址不涉及安全业务时，进行普通网络传输。

VPN 安全接入方法及系统

技术领域

本发明涉及网络安全技术领域，特别涉及一种 VPN（虚拟专用网络）网络安全接入方法及系统。

背景技术

对于许多大型分布式系统来说，比如国家某部委关键电子政务业务系统，要面向许多不同需求、不同规模的用户，应用系统数量多，有多种不同的技术架构。既有基于 B/S 的业务系统，也有基于 C/S 的业务系统。此类系统由于处理业务的特殊性和用户的广泛性，对安全性要求较高。

目前企业通过 Internet 实现安全接入的方式主要有 IPSec（IPSecurity）VPN 和 SSL (Security Socket Layer)VPN 两种，两种技术在不同领域各有其优势。在实施固定的网络到网络的 VPN 和复杂应用的用户安全接入时，采用 IPSec VPN 技术更为合适；在实施普通应用的移动用户接入时，采用 SSL VPN 技术更合适，原因是 SSL VPN 无需在终端用户安装客户端软件、实施和维护较为简单，总体拥有成本较低。

IPSec 是一组开放协议的总称，特定的通信方之间在 IP 层通过加密与数据源验证，以保证数据包在 Internet 网上传输时的私有性、完整性和真实性。IPSec 通过 AH（AuthenticationHeader）和 ESP（Encapsulating Security Payload）这两个安全协议来实现，此实现不会对用户、主机或其它 Internet 组件造成影响，用户还可以选择不同的硬件和软件加密算法，而不会影响其它部分的实现。

从概念角度来说，SSL VPN 即指采用 SSL 协议来实现远程接入的一种新型 VPN 技术。对于内、外部应用来说，使用 SSL 可保证信息的真实性、完整性和保密性。目前 SSL 协议被广泛应用于各种浏览器应用，也可以应用于 Outlook 等使用 TCP 协议传输数据的 C/S 应用。正因为 SSL 协议被内置于 IE 等浏览器中，使用 SSL 协议进行认证和数据加密的 SSL VPN 就可以免于安装客户端。相对于传统的 IPSEC VPN 而言，SSL VPN 具有部署简单，无客户端，维护成本低，网络适应强等特点，这两种类型的 VPN 之间的差别就类似 C/S 构架和 B/S 构架的区别。

目前 VPN 安全接入技术（包括 IPSec VPN 和 SSL VPN）已经非常成熟，并在许多企事业单位广泛使用。VPN 接入时常用的用户认证方式是用户名和口令，事实证明这种方式强度较弱，容易被人复制和猜测，安全性较低。有的 VPN 产品支持第三方 CA 证书认证，但更多的是采用软证书，即用户证书是以文件的方式存储在电脑硬盘，仍然存在安全隐患。当然目前也有少部分 VPN 产品使用了硬件设备 Key 来存储用户证书和私钥信息，并完成密钥生成和签名等操作，其安全性在一定程度上较前两种用户认证方式有了较大的提高。不过熟悉安全领域的人士会发现其还有一个不足，就是 VPN 在传输安全数据时，数据的加解密过程因速度等原因无法通过硬件 Key 来完成，只能靠计算机软件来完成，只要是软件完成的工作，就有可能受到攻击，存在安全问题。

现有 VPN 接入系统的缺点是:

数据加解密是以软件方式实现，安全强度不够高;

数据加解密算法通常采用国际上通用的标准算法（如 DES 等)或者早期的国产加解密算法（如 SSF33 等），对最新的国产算法 SCB2 支持的很少;

用户的身份认证采用常用的用户名和口令方式，安全等级较低。有的虽然支持第三方证书认证，但大多是以文件的方式存储用户证书，仍然存在安全隐患;

安全接入、用户身份认证以及计时计费等系统相互独立，系统部署、运行维护成本较高;

用户必须手工进行 VPN 拨号，然后才能访问受 VPN 保护的业务系统，不能实现 IE 浏览器自动识别。

发明内容

针对上述问题，本发明的目的就是要进一步地提高安全接入系统的安全等级，完全满足涉及国家安全、高度机密的电子政务对安全产品和服务的要求。

本发明提供一种 VPN 安全接入方法，在 VPN 客户端中采用硬件设备 Key;该方法还包括:

所述 VPN 客户端向网络侧发起接入请求，所述接入请求经所述硬件设备 Key 签名和加密;

网络侧接收到所述接入请求后，对所述 VPN 客户端进行身份认证，认证

通过后，与所述 VPN 客户端建立安全通道；

所述 VPN 客户端通过硬件设备 Key 以及所述安全通道与网络侧进行安全业务交互。

优选的， VPN 客户端向网络侧发起的接入请求由用户触发发起，或者，由 VPN 客户端根据所连接的网址自动启动。

优选的，网络侧通过第三方对所述 VPN 客户端进行身份认证。

对 VPN 客户端身份认证通过后，进一步包括：判断所述 VPN 客户端是否满足访问条件，若满足再执行后续操作，否则结束。

相应地，一种 VPN 安全接入系统，包括：

VPN 网关，用于将接收到的来自 VPN 客户端的接入请求发送给安全认证模块，将身份认证结果返回给所述 VPN 客户端；当所述身份认证结果为认证通过时，与所述 VPN 客户端建立安全通道；

安全认证模块，用于根据接收到的接入请求对所述 VPN 客户端进行身份认证，给所述 VPN 网关返回身份认证结果；

包含硬件设备 Key 的 VPN 客户端，用于向网络侧发起接入请求，所述接入请求经所述硬件设备 Key 加密；通过硬件设备 Key 以及所述安全通道与业务系统进行安全业务交互；

业务系统，用于与所述 VPN 客户端通过所述安全通道进行安全业务交互。

另一方面，本发明还提供一种 VPN 客户端，包括：

安全接入请求单元，用于向 VPN 网关发起安全接入请求，经过客户端身份认证，虚拟地址分配以及访问权限检查后，触发安全通道建立单元进行下一步工作；

安全通道建立单元，用于在 VPN 客户端与 VPN 网关之间建立安全通道；

发送单元，用于将待发送数据传送给硬件设备 Key 进行加密和认证，并将加密后重新打包的数据通过安全通道发送出去；

接收单元，用于将经安全通道接收到的加密安全业务数据传递给硬件设备 Key 进行解密和认证，然后呈现给用户；

硬件设备 Key，用于存储 VPN 客户端安全信息以及完成各种安全算法，并对接收到的待加密信息进行加密，将加密后的信息传送给发送单元；将接收

到的加密安全业务数据进行解密，将解密后的安全业务数据传送给接收单元；

通道管理单元，用于安全通道的监管和维护

与现有技术相比，本发明具有以下优点：

现有的技术虽然也能够建立 VPN 安全通道，在公共网络上实现虚拟专用网，从而达到安全接入目的。但本发明与之相比，完全通过硬件方式实现安全加解密，其安全等级明显要高。同时采用国产最新加解密算法 SCB2，对与涉及国家安全的重要信息系统而言是非常必须的。

现有的安全接入系统中，安全接入、安全认证以及计费均属于不同的系统组成部分，根据功能需要集成在一起，有的还需要进行二次开发，系统结构复杂，系统部署和运行维护难度较高。而本发明所提供的不同系统无缝集成的一整套解决方案，相对而言其购买成本和后期的维护成本要低许多。

附图说明

图 1 是根据本发明实施例所述系统的 VPN 拓扑示意图；

图 2 是根据本发明实施例的工作原理示意图；

图 3 是本发明实施例 VPN 客户端的逻辑结构示意图；

图 4 表示本发明实施例的 VPN 客户端认证流程示意图；

图 5 表示根据本发明实施例的业务流程示意图。

具体实施方式

为使本发明的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本发明作进一步详细的说明。

本发明的一个实施以服务于国家某部委关键电子政务业务系统为基础，该业务系统是一个用户数量庞大而且分布于全国各地的系统，同时业务系统数量较多，技术架构也不尽相同，既有 B/S 类型的系统，也有 C/S 的系统，因此需要尽量提高其系统的安全性。目前企业通过 Internet 实现安全接入的方式主要有 IPSec VPN 和 SSL VPN 两种，在下面的实施例中以 IPSec VPN 为例来对本发明的 VPN 的安全接入方案进行说明。

本发明提供的“VPN 的安全接入方案”是实现 Internet 接入企业核心业务网的一整套安全接入解决方案。本实施例的基于 IPSec 协议的 VPN 网络安全接入系统主要由五个部分组成，即 VPN 客户端、VPN 网关、安全认证模块、

计时计费模块以及业务系统；其中，为了说明上的方便，在本发明中，VPN客户端又被称作“客户端侧”，而相对于 VPN 客户端来说的其它部分（VPN网关、安全认证模块、计时计费模块以及业务系统）均被称为“网络侧”。

首先，用户启动 VPN 客户端进行拨号，然后由安全认证模块进行身份认证，再由计时计费模块进行时间和费用的检查和记录，最后与 VPN 网关之间建立一条安全可靠的 VPN 安全通道。客户端可以通过该 VPN 安全通道访问受 VPN 网关保护的业务系统。在本发明的一个具体实施例中，业务系统指的就是国家某部委关键电子政务业务系统。由于本实施例是基于IPSec协议实现的，因此在以下的表述中，“VPN 安全通道”也被称作“IPSec 安全通道”。

为了正确封装及提取 IPSec 数据报，需要采取一套专门的方案，将安全服务和（或）密钥与要保护的通信数据联系到一起；同时要将远程通信实体与要交换密钥的 IPSec 数据传输联系到一起。

VPN 安全通道的建立采用 IPSec 协议，VPN 客户端首先与 VPN 网关进行连接以获取虚拟 IP 地址、权限、隧道参数等信息，然后客户端与 VPN 网关之间进行 IKE（Internet Key Exchange，密钥交换）SA 协商，再进行 IPSec SA 协商，从而建立起安全可靠的 VPN 隧道。VPN 网关收到客户端的请求后，通过调用安全认证模块基于 Soap（简单对象访问协议）标准协议的 webservice 服务进行身份认证，然后再通过 webservice 方式访问计费模块。计费模块采用接入端计时、计费端结算的模式，通过实时通知与批量处理结合的方式，保证计时、计费服务的准确、可靠。

IKE 的用途就是在 IPSec 通信双方之间建立起共享的安全参数及验证过的密钥。运用 IPSec 进行安全通信的步骤是：①建立 IKE SA；②在已经建立好的 IKE SA 上建立 IPSec SA；③在已经建立好的 IPSec SA 上，进行实际的通信；④通信完毕，撤消 IPSec SA；⑤当此 IKE SA 上的所有 IPSec SA 都撤消以后，最后撤消 IKE SA。

图 1 和图 2 分别是根据本发明实施例的 VPN 拓扑图和工作原理示意图，下面将结合图 1 和图 2 分别对本发明所述系统的各个部分组成及工作流程作详细说明：

（1）VPN 客户端和采用高速、安全芯片的 Key

图1中企业1与企业2由于终端设备和所需处理数据量规模的不同而采取了不同的安全接入方式：企业1采取IPSec下的VPN客户端软件的安全接入方式，企业2采取IPSec下的VPN网关的安全接入方式，但两者的工作原理实际上是类似的。本发明中重点以采取IPSec下的VPN客户端软件的安全接入方式为例进行说明。

VPN客户端包括安全接入请求单元、安全通道建立单元、发送单元、接收单元、通道管理单元和硬件设备Key。

其中，安全接入请求单元用于向VPN网关发起安全接入请求，并将接入请求发送给硬件设备Key进行签名和加密与VPN网关完成身份认证，认证通过后，客户端获取VPN网关分配的虚拟地址并检查访问权限后，触发安全通道建立单元进行下一步工作。安全通道建立单元用于与VPN网关进行进行IKE协商，在VPN客户端与VPN网关（网络侧）之间建立安全通道；硬件设备Key，用于VPN客户端数据的加解密，具体来讲，就是对接收到的待加密信息进行加密，将加密后的信息传送给发送单元；将接收到的加密安全业务数据进行解密，将解密后的安全业务数据传送给业务数据处理单元。VPN客户端数据的加解密均在硬件设备Key内部进行。

发送单元，用于将来自硬件设备Key的加密后的信息通过安全通道发送出去；接收单元，用于通过安全通道接收来自VPN网关（网络侧）的已加密的安全业务数据，将所述已加密的安全业务数据传递给硬件设备Key。

通道管理单元，用于设置保活时间，完成通道的保活等安全通道监管和维护功能。具体来说，在VPN客户端在建立安全通道的过程中和安全通道建立后，通道管理单元实施实时监测、管理安全通道的建立和运行状况，如：安全通道内的数据流量、拥挤状况以及长时间没有数据流量时安全通道自动关闭等；如果某条安全通道发生故障或者过度拥挤，通道管理单元将选择其他可替代安全通道继续进行安全数据的传输，实现安全通道的自动切换等。

此外，在本发明的另一优选实施例中，VPN客户端还包括通道识别单元，用于根据配置信息判别VPN客户端所连接的网址是否涉及安全业务，当连接网址涉及安全业务时，触发安全接入请求单元，建立安全通道进行安全业务数据的传输；当VPN客户端所连接的网址仅涉及普通业务时，则不需要触发安

全接入请求单元，直接按照通用方式进行普通网络传输即可。这样就保证了当用户没有主动发起接入请求时启动安全接入而直接访问安全业务时的访问安全性。图 3 所示为包括通道识别单元 VPN 客户端的逻辑示意结构图。

在企业 1 端，用户启动 VPN 客户端向 VPN 网关发起安全接入请求。VPN 客户端采用面向对象的 C++语言开发，并与 Key 硬件设备进行通信，通过 Key 硬件设备中的与安全相关的数据信息进行身份认证和数据加解密操作。其中的认证流程如图 4 所示，按照开始身份认证、获取 KeyID、发送认证请求、接收认证结果、生成签名 CA 随即串、发送 Key 签名信息、接收虚拟 IP 和分配权限、由 DHCP（动态主机分配协议）分配虚地址的顺序逐步进行认证操作。

在此，Key 是安全介质，用于存储所有安全相关的数据，如证书、密钥等，并执行如签名、验签和数据加解密等的各种安全算法。它基于国内首款拥有全自主知识产权的 SSX45 密码安全芯片，满足信息安全处理中针对信息提出的机密性、完整性、可用性、可控性等高安全性需求。该芯片基于国产 32 位 CPU 核，支持 RSA、ECC 非对称密码算法和 SSF33、SCB2 对称密码算法，通过内部硬件设计的公钥加速引擎和其他硬件算法模块实现高性能的信息加解密运算，采用 SOC（System on Chip 片上系统）的芯片结构和其他的非凡安全处理模块实现了信息处理的高安全性。

本发明所采用的上述数据加解密采用高速芯片、以硬件方式实现的安全措施，使得所有的安全相关数据以及签名、加解密等安全算法过程全部在硬件 Key 内部完成，外界无法干预，因此确保了加解密过程的绝对安全。

（2）VPN 网关

VPN 网关是企业受保护的业务系统的入口，也是连接 VPN 客户端和安全认证模块以及计费模块的桥梁。它的主要作用是与 VPN 客户端进行协商，并建立 VPN 安全通道。同时在本发明中，VPN 网关、安全认证模块和计时计费模块三方是无缝集成的，即 VPN 网关通过基于 SOAP 标准协议的 WebService 服务与安全认证模块和计费模块进行通信，实现安全接入、用户身份认证和计时计费的无缝集成。本发明中所述的“无缝集成”指不同模块均是在同一开发框架下实现的，采用同样的数据传输标准和实现方式，模块间的交互不需要任何协议或者数据格式等方面的转换即可直接进行。而且，不同的模块既可以部

署在同一台物理服务器，也可以部署在不同的物理服务器中。

（3）安全认证与计时计费模块

安全认证模块作为一个第三方的 CA 证书认证中心，它接受 VPN 网关的用户证书认证请求，并提供高效、安全的证书认证服务。其主要功能完成随机数的生成、签名验签、证书有效性查询以及证书更新等。本平台以标准的 Webservice 服务接口对外提供服务，基于 J2EE 的分布式系统，具有较高的可靠性、稳定性和安全性。

本发明在用户身份认证方面，无缝集成了安全认证模块，将用户证书和密钥信息存储在高速芯片内，VPN 客户端通过 VPN 网关与安全认证模块完成双向认证，对非法接入用户杜绝进入，在访问控制层进一步提高系统的安全性。

计时计费模块的功能主要是实现对合法的安全接入用户的访问控制，并对使用时间、流量进行实时监控。其计时计费策略可以通过配置文件进行灵活配置，具有较强的可配置性和可扩展性。本系统对外提供 Webservice 服务接口，基于 J2EE 的分布式系统，具有高可靠性、稳定性和安全性。计费模块是本发明一个优选实施例的配置，在不需要对合法安全接入用户进行时间、流量方面的访问控制时，也可以不使用计时计费模块。

根据图 2 所示，本发明基于 IPSec 协议的 VPN 网络安全接入系统的工作原理描述如下：

(1) 客户端在访问受保护业务系统之前，首先通过 Internet 网络发起接入请求；

(2) VPN 网关先对发起接入请求的客户端进行身份认证，本发明采用可信的第三方 CA 证书认证，认证强度高，安全可靠；

(3) 认证返回，如果认证通过，则进行第(4)步，否则返回认证错误信息后退出；

(4) 通知计时计费模块，启动对该客户端的计时计费工作，其中包括对客户端是否有可用时间的判断；

(5) 计时计费模块返回响应信息；

(6) 如果计时计费模块返回正确的响应信息，表示该客户端尚具有可用时间，则进行第(7)步，建立 IPSec VPN 安全通道，如果计时计费模块返回错误信

息则退出；

(7) 客户端与 VPN 网关之间建立 IPSec 安全通道；

(8) IPSec 安全通道建立完毕，返回等待用户进一步的操作；

(9) 如果用户需要访问受保护的安全业务，如本例的国家某部委电子政务业务系统，VPN 客户端自动识别用户要访问的业务安全性，并强制所有有关安全业务的数据走 IPSec 安全通道，利用硬件 Key 的高速芯片完成加解密和认证过程。因此，在这一过程中，所有数据均被保护，高度安全。

(10) 业务系统从 IPSec 安全通道中返回响应数据。

以上(1)～(10)仅仅表示客户端在主动发起接入请求启动安全接入情况下的工作流程；当用户没有主动发起接入请求启动安全接入情况下而直接访问安全业务时，设置在客户端的通道识别模块，能够根据用户访问的网址自动识别安全业务所要求的安全级别，从而启动 VPN 安全接入请求，建立 IPSec 安全通道以供安全业务数据的传输。当然，如果用户访问的是普通业务，则不需要启动安全接入、建立安全通道，直接使用普通的网络传输方式就可以了。

另一方面，图 2 所示的(11)、(12)两步操作是用户通过网络访问普通业务的工作方式，和现有的网络接入方式相同，如果用户访问普通业务，则不走 IPSec 安全通道，走普通 Internet 网络通道进行访问；响应数据从普通 Internet 网络通道返回。

图 5 是本发明的业务流程示意图，表示用户在主动启动安全接入情况下的具体工作流程，该流程所示的主要步骤与图 2 所示的工作原理步骤基本一致，如步骤：用户插入 Key、启动 VPN 客户端、VPN 客户端向 VPN 网关发起连接请求，对应于图 2 中的(1) 用户客户端通过 Internet 网络进行 VPN 拨号；步骤:VPN 客户端向安全认证模块发起认证请求、安全认证模块进行身份认证，对应于图 2 中的(2) VPN 网关对拨号用户进行身份认证。因此对于图 5 的具体工作流程，本领域技术人员可以根据前面实施例的描述扩展所得，在此不再赘述。

实现安全接入的方法有很多，比如专线接入，光纤接入等等，但这些方式成本昂贵，不适合用户数量较大，且分布较为分散的系统。而目前尚未发现使用硬件实现加解密的安全接入产品应用于利用 Internet 公共网络实现安全接入

的技术。在此基础上，本发明高度重视最终用户的使用体验，尽量简化系统的操作，给用户使用本系统提供尽可能的方便。这主要体现在两个方面：第一、对于安全接入服务提供商而言，本发明将安全接入、高强度的用户身份认证以及计费系统高度集成在一起，形成一整套的安全接入解决方案，大大方便了用户的部署和运行维护，同时也降低了系统采购的成本；第二、对于 VPN 客户端的最终用户而言，本发明通过通道识别模块，能够自动识别用户访问 Internet 时，是否需要进行 VPN 拨号，建立安全通道。如果需要，则自动发起安全接入请求完成安全通道的建立过程，对用户是透明的。这样方便了用户的使用，增强了用户的体验感受。

本领域普通技术人员可以理解实现上述方法实施方式中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，所述的程序可以存储于计算机可读取存储介质中，这里所称的存储介质，如：ROM/RAM、磁碟、光盘等。

以上所述仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围，比如也可以采用SSL VPN的安全接入方式以类似的技术手段来实现本发明目的。因此，凡在本发明的精神和原则之内所作的任何修改、等同替换、改进等，均包含在本发明的保护范围内。

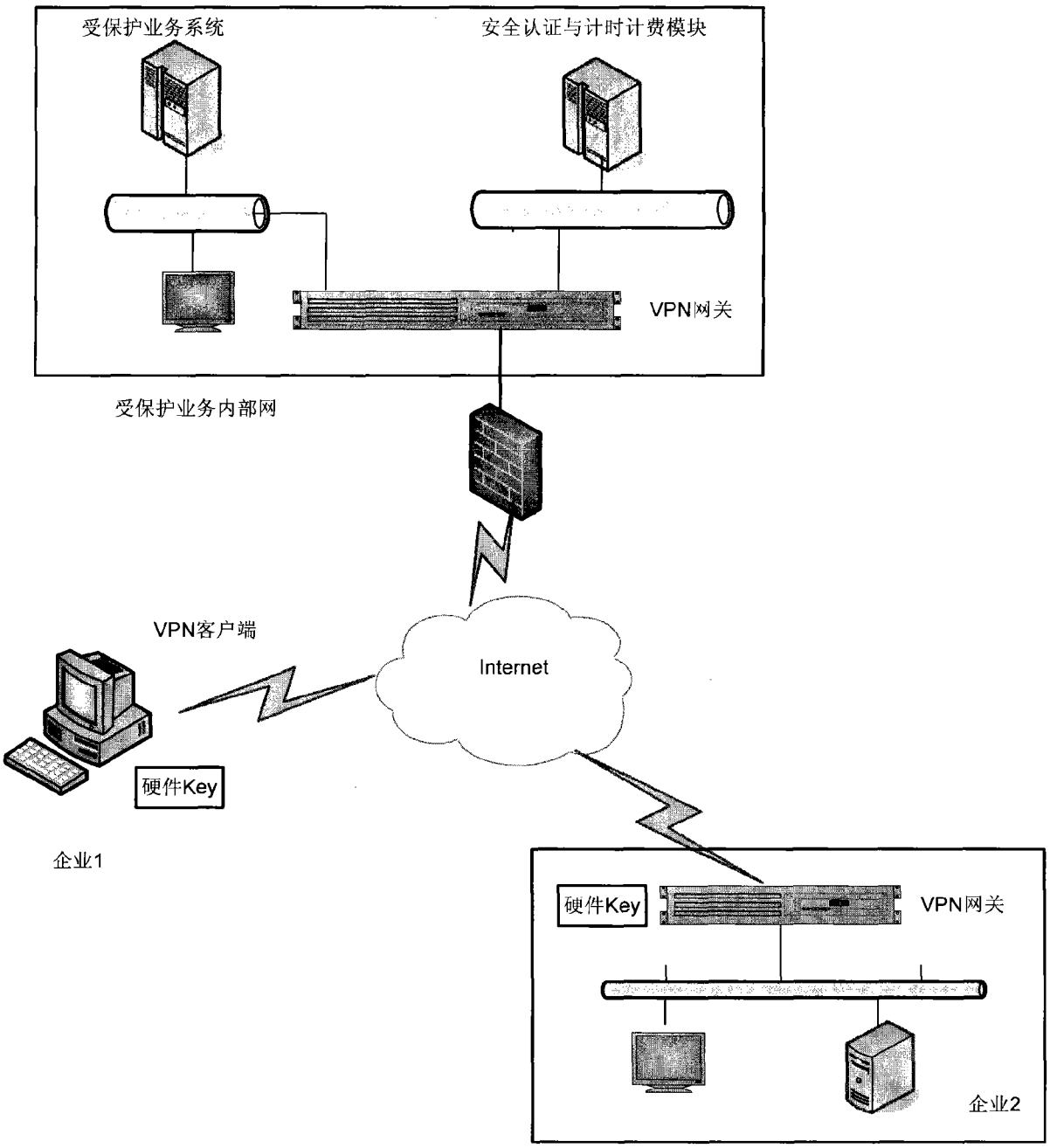

受保护业务系统
安全认证与计时计费模块
VPN网关
受保护业务内部网
VPN客户端
Internet
硬件Key
企业1
硬件Key
VPN网关
企业2

图 1

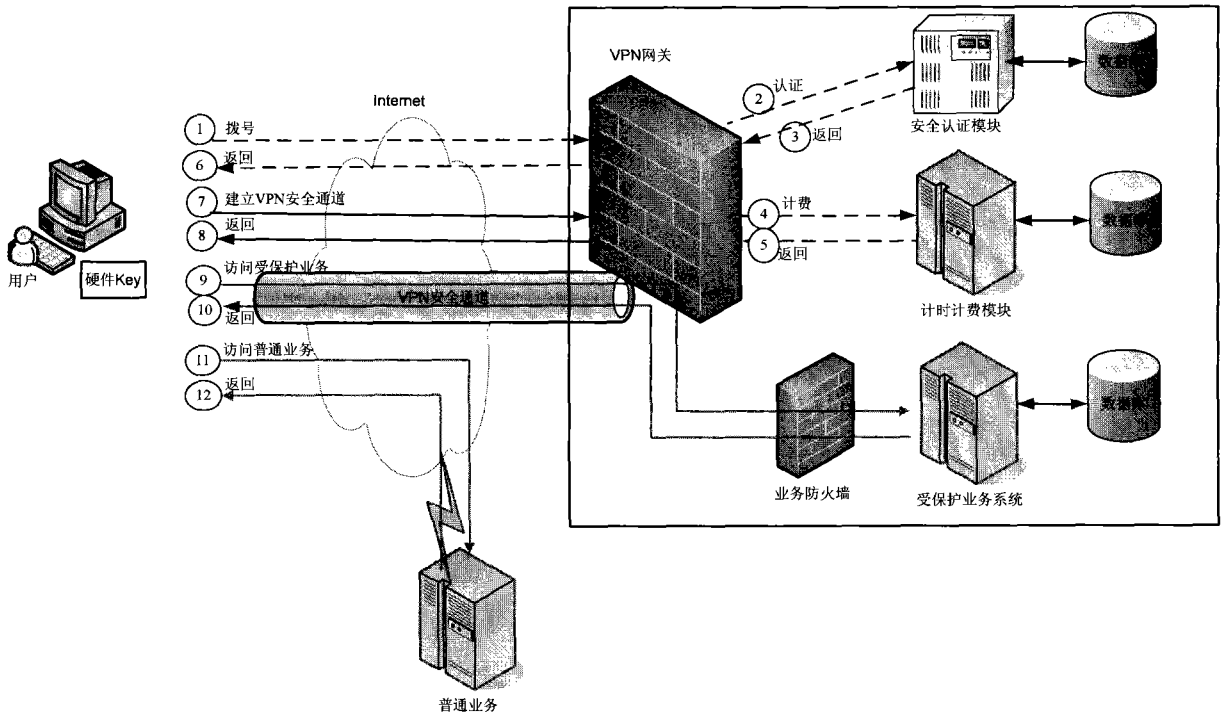

VPN网关
Internet
1 拨号
6 返回
7 建立VPN安全通道
8 返回
9 访问受保护业务
10 返回
11 访问普通业务
12 返回
2 认证
3 返回
4 计费
5 返回
安全认证模块
计时计费模块
业务防火墙
受保护业务系统
普通业务
用户
硬件Key
VPN安全通道

图 2

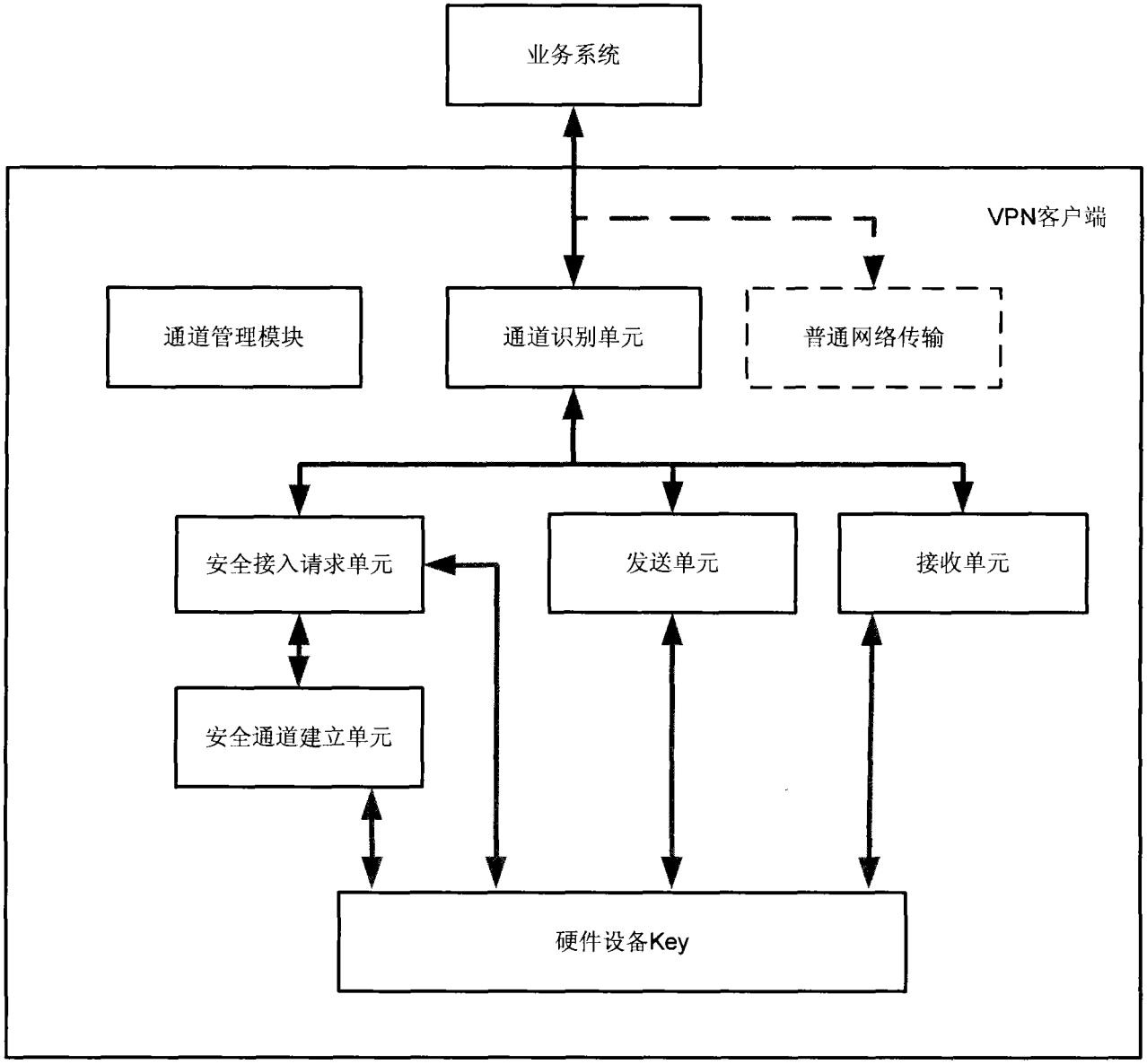

业务系统
VPN客户端
通道管理模块
通道识别单元
普通网络传输
安全接入请求单元
发送单元
接收单元
安全通道建立单元
硬件设备Key

图 3

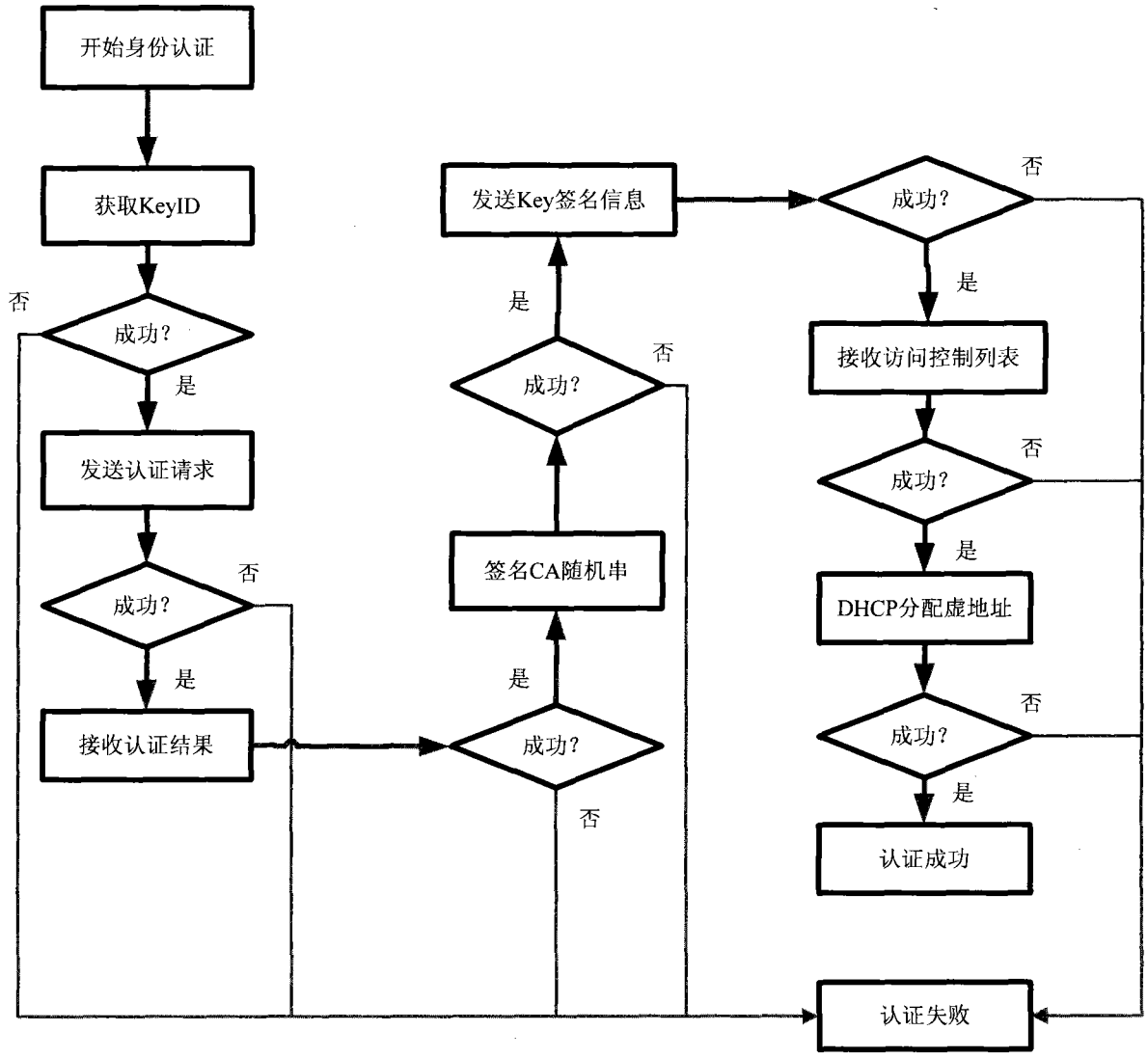

开始身份认证
获取KeyID
成功?
否
是
发送认证请求
成功?
否
是
接收认证结果
成功?
是
否
签名CA随机串
成功?
是
否
发送Key签名信息
成功?
否
是
接收访问控制列表
成功?
否
是
DHCP分配虚地址
成功?
否
是
认证成功
认证失败

图 4

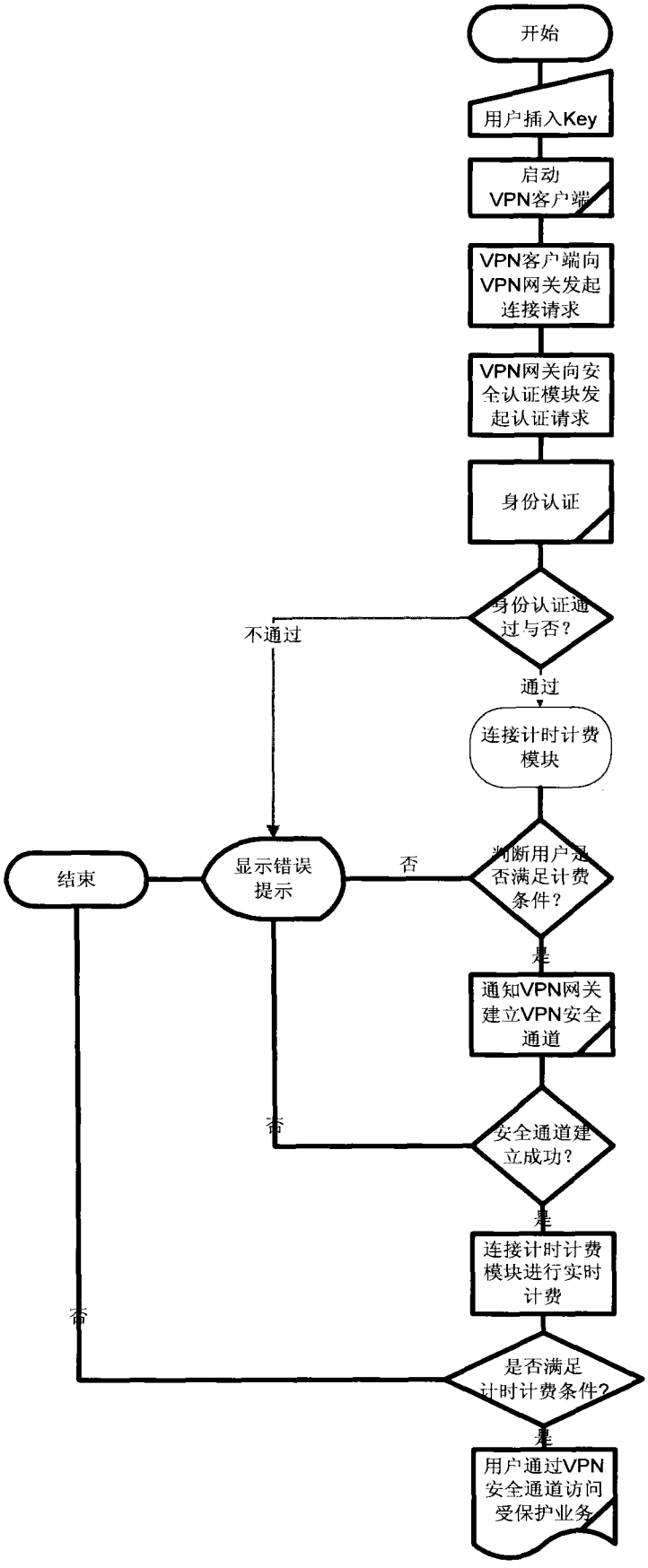

开始
用户插入Key
启动VPN客户端
VPN客户端向VPN网关发起连接请求
VPN网关向安全认证模块发起认证请求
身份认证
身份认证通过与否？
不通过
通过
连接计时计费模块
判断用户是否满足计费条件？
否
显示错误提示
结束
是
通知VPN网关建立VPN安全通道
否
安全通道建立成功？
是
连接计时计费模块进行实时计费
否
是否满足计时计费条件？
是
用户通过VPN安全通道访问受保护业务

图 5