



(12) 发明专利申请

(10) 申请公布号 CN 105610667 A

(43) 申请公布日 2016. 05. 25

(21) 申请号 201510979993. 6

(22) 申请日 2015. 12. 23

(71) 申请人 深圳市华成峰实业有限公司

地址 518000 广东省深圳市南山区高新南七
道 16 号德维森大厦七楼

(72) 发明人 李小勇

(74) 专利代理机构 广州华进联合专利商标代理
有限公司 44224

代理人 李文渊

(51) Int. Cl.

H04L 12/46(2006. 01)

H04L 29/06(2006. 01)

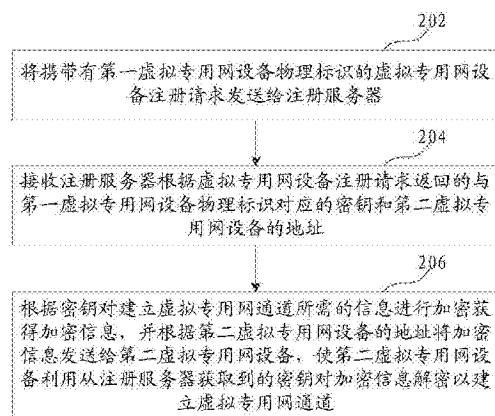
权利要求书2页 说明书7页 附图4页

(54) 发明名称

建立虚拟专用网通道的方法和装置

(57) 摘要

本发明涉及一种建立虚拟专用网通道的方法，包括：将携带有第一虚拟专用网设备物理标识的虚拟专用网设备注册请求发送给注册服务器；接收注册服务器根据虚拟专用网设备注册请求返回的与第一虚拟专用网设备物理标识对应的密钥和第二虚拟专用网设备的地址；根据密钥对建立虚拟专用网通道所需的信息进行加密获得加密信息，并根据第二虚拟专用网设备的地址将加密信息发送给第二虚拟专用网设备，使第二虚拟专用网设备利用从注册服务器获取到的密钥对加密信息解密以建立虚拟专用网通道。本实施例中，不需要对第一虚拟专用网设备进行配置，当第一虚拟专用网设备接入网络时，即可自动建立虚拟专用网通道，使得建立虚拟专用网通道更加简单、高效。



1.一种建立虚拟专用网通道的方法,所述方法包括:

将携带有第一虚拟专用网设备物理标识的虚拟专用网设备注册请求发送给注册服务器;

接收所述注册服务器根据所述虚拟专用网设备注册请求返回的与所述第一虚拟专用网设备物理标识对应的密钥和第二虚拟专用网设备的地址;

根据所述密钥对建立虚拟专用网通道所需的信息进行加密获得加密信息,并根据所述第二虚拟专用网设备的地址将所述加密信息发送给所述第二虚拟专用网设备,使所述第二虚拟专用网设备利用从所述注册服务器获取到的密钥对所述加密信息解密以建立虚拟专用网通道。

2.根据权利要求1所述的方法,其特征在于,所述方法还包括:

所述注册服务器从接收到的所述虚拟专用网设备注册请求中提取所述第一虚拟专用网设备物理标识,从所述注册服务器查找是否记录有所述第一虚拟专用网设备物理标识,若是则提取与所述第一虚拟专用网设备物理标识对应的密钥和所述第二虚拟专用网设备的地址并发送给所述第一虚拟专用网设备。

3.根据权利要求1所述的方法,其特征在于,所述方法还包括:

所述注册服务器提取所述第一虚拟专用网设备物理标识,并在加密库中查找与所述第一虚拟专用网设备物理标识对应的算法标识,根据查找到的算法标识所对应的密钥生成算法生成密钥。

4.根据权利要求1所述的方法,其特征在于,所述接收所述注册服务器根据所述虚拟专用网设备注册请求返回的与所述第一虚拟专用网设备物理标识对应的密钥和第二虚拟专用网设备的地址之后,还包括:

根据所述第二虚拟专用网设备的地址向所述第二虚拟专用网设备发送第一虚拟专用网设备的数字证书;

接收所述第二虚拟专用网设备在对所述数字证书的验证通过后发送的反馈信息;

响应于所述反馈信息执行所述根据所述密钥对建立虚拟专用网通道所需的信息进行加密获得加密信息的步骤。

5.根据权利要求1所述的方法,其特征在于,所述方法还包括:

当检测到所述虚拟专用网通道中断时,则重新发送用于建立所述虚拟专用网通道的加密信息以重新建立所述虚拟专用网络通道;

当建立所述虚拟专用网通道失败次数达到预设次数时,则将失败信息上传到所述注册服务器。

6.一种建立虚拟专用网通道的装置,其特征在于,所述装置包括:

请求发送模块,用于将携带有第一虚拟专用网设备物理标识的虚拟专用网设备注册请求发送给注册服务器;

建立信息接收模块,用于接收所述注册服务器根据所述虚拟专用网设备注册请求返回的与所述第一虚拟专用网设备物理标识对应的密钥和第二虚拟专用网设备的地址;

通道建立模块,用于根据所述密钥对建立虚拟专用网通道所需的信息进行加密获得加密信息,并根据所述第二虚拟专用网设备的地址将所述加密信息发送给所述第二虚拟专用网设备,使所述第二虚拟专用网设备利用从所述注册服务器获取到的密钥对所述加密信息

解密以建立虚拟专用网通道。

7. 根据权利要求6所述的装置，其特征在于，所述注册服务器用于从接收到的所述虚拟专用网设备注册请求中提取所述第一虚拟专用网设备物理标识，从所述注册服务器查找是否记录有所述第一虚拟专用网设备物理标识，若是则提取与所述第一虚拟专用网设备物理标识对应的密钥和所述第二虚拟专用网设备的地址并发送给所述第一虚拟专用网设备。

8. 根据权利要求6所述的装置，其特征在于，所述注册服务器用于提取所述第一虚拟专用网设备物理标识，并在加密库中查找与所述第一虚拟专用网设备物理标识对应的算法标识，根据查找到的算法标识所对应的密钥生成算法生成密钥。

9. 根据权利要求6所述的装置，其特征在于，所述装置还包括：

证书发送模块，用于根据所述第二虚拟专用网设备的地址向所述第二虚拟专用网设备发送第一虚拟专用网设备的数字证书；

反馈信息接收模块，用于接收所述第二虚拟专用网设备在对所述数字证书的验证通过后发送的反馈信息；

所述通道建立模块还用于响应于所述反馈信息执行所述根据所述密钥对建立虚拟专用网通道所需的信息进行加密获得加密信息的步骤。

10. 根据权利要求6所述的装置，其特征在于，所述装置还包括：

通道重新建立模块，用于当检测到所述虚拟专用网通道中断时，则重新发送用于建立所述虚拟专用网通道的加密信息以重新建立所述虚拟专用网络通道；

失败信息上传模块，用于当建立所述虚拟专用网通道失败次数达到预设次数时，则将失败信息上传到所述注册服务器。

建立虚拟专用网通道的方法和装置

技术领域

[0001] 本发明涉及虚拟专用网技术领域,特别是涉及一种建立虚拟专用网通道的方法和装置。

背景技术

[0002] 随着互联网的快速发展,在公用网络上建立VPN(Virtual Private Network,虚拟专用网)通道,通过VPN通道可以随时随地访问到内网资源。在建立VPN通道的传统方法中,设置有VPN服务器,通过互联网连接VPN服务器,需要对VPN服务器进行复杂的配置来建立VPN通道,建立VPN通道的过程比较繁琐。

发明内容

[0003] 基于此,有必要针对建立虚拟专用网通道的过程繁琐的问题,提供一种建立虚拟专用网通道的方法和装置。

[0004] 一种建立虚拟专用网通道的方法,所述方法包括:

[0005] 将携带有第一虚拟专用网设备物理标识的虚拟专用网设备注册请求发送给注册服务器;

[0006] 接收所述注册服务器根据所述虚拟专用网设备注册请求返回的与所述第一虚拟专用网设备物理标识对应的密钥和第二虚拟专用网设备的地址;

[0007] 根据所述密钥对建立虚拟专用网通道所需的信息进行加密获得加密信息,并根据所述第二虚拟专用网设备的地址将所述加密信息发送给所述第二虚拟专用网设备,使所述第二虚拟专用网设备利用从所述注册服务器获取到的密钥对所述加密信息解密以建立虚拟专用网通道。

[0008] 在其中一个实施例中,所述方法还包括:

[0009] 所述注册服务器从接收到的所述虚拟专用网设备注册请求中提取所述第一虚拟专用网设备物理标识,从所述注册服务器查找是否记录有所述第一虚拟专用网设备物理标识,若是则提取与所述第一虚拟专用网设备物理标识对应的密钥和所述第二虚拟专用网设备的地址并发送给所述第一虚拟专用网设备。

[0010] 在其中一个实施例中,所述方法还包括:

[0011] 所述注册服务器提取所述第一虚拟专用网设备物理标识,并在加密库中查找与所述第一虚拟专用网设备物理标识对应的算法标识,根据查找到的算法标识所对应的密钥生成算法生成密钥。

[0012] 在其中一个实施例中,所述接收所述注册服务器根据所述虚拟专用网设备注册请求返回的与所述第一虚拟专用网设备物理标识对应的密钥和第二虚拟专用网设备的地址之后,还包括:

[0013] 根据所述第二虚拟专用网设备的地址向所述第二虚拟专用网设备发送第一虚拟专用网设备的数字证书;

- [0014] 接收所述第二虚拟专用网设备在对所述数字证书的验证通过后发送的反馈信息；
[0015] 响应于所述反馈信息执行所述根据所述密钥对建立虚拟专用网通道所需的信息进行加密获得加密信息的步骤。
[0016] 在其中一个实施例中，所述方法还包括：
[0017] 当检测到所述虚拟专用网通道中断时，则重新发送用于建立所述虚拟专用网通道的加密信息以重新建立所述虚拟专用网络通道；
[0018] 当建立所述虚拟专用网通道失败次数达到预设次数时，则将失败信息上传到所述注册服务器。
[0019] 上述建立虚拟专用网通道的方法，在第一虚拟专用网设备接入网络时，向注册服务器发送虚拟专用网设备注册请求，虚拟专用网设备注册请求中携带了第一虚拟专用网设备物理标识，注册服务器接收到虚拟专用网设备注册请求之后，将与第一虚拟专用网络设备标识对应的建立虚拟专用网通道的信息发送给第一虚拟专用网设备，第一虚拟专用网设备根据建立虚拟专用网的信息与第二虚拟专用网设备建立虚拟专用网通道。这样，在建立虚拟专用网通道的过程中，不需要对第一虚拟专用网设备进行配置，当第一虚拟专用网设备接入网络时，即可自动建立虚拟专用网通道，使得建立虚拟专用网通道更加简单、高效。
[0020] 一种建立虚拟专用网通道的装置，所述装置包括：
[0021] 请求发送模块，用于将携带有第一虚拟专用网设备物理标识的虚拟专用网设备注册请求发送给注册服务器；
[0022] 建立信息接收模块，用于接收所述注册服务器根据所述虚拟专用网设备注册请求返回的与所述第一虚拟专用网设备物理标识对应的密钥和第二虚拟专用网设备的地址；
[0023] 通道建立模块，用于根据所述密钥对建立虚拟专用网通道所需的信息进行加密获得加密信息，并根据所述第二虚拟专用网设备的地址将所述加密信息发送给所述第二虚拟专用网设备，使所述第二虚拟专用网设备利用从所述注册服务器获取到的密钥对所述加密信息解密以建立虚拟专用网通道。
[0024] 在其中一个实施例中，所述注册服务器用于从接收到的所述虚拟专用网设备注册请求中提取所述第一虚拟专用网设备物理标识，从所述注册服务器查找是否记录有所述第一虚拟专用网设备物理标识，若是则提取与所述第一虚拟专用网设备物理标识对应的密钥和所述第二虚拟专用网设备的地址并发送给所述第一虚拟专用网设备。
[0025] 在其中一个实施例中，所述注册服务器用于提取所述第一虚拟专用网设备物理标识，并在加密库中查找与所述第一虚拟专用网设备物理标识对应的算法标识，根据查找到的算法标识所对应的密钥生成算法生成密钥。
[0026] 在其中一个实施例中，所述装置还包括：
[0027] 证书发送模块，用于根据所述第二虚拟专用网设备的地址向所述第二虚拟专用网设备发送第一虚拟专用网设备的数字证书；
[0028] 反馈信息接收模块，用于接收所述第二虚拟专用网设备在对所述数字证书的验证通过后发送的反馈信息；
[0029] 所述通道建立模块还用于响应于所述反馈信息执行所述根据所述密钥对建立虚拟专用网通道所需的信息进行加密获得加密信息的步骤。
[0030] 在其中一个实施例中，所述装置还包括：

[0031] 通道重新建立模块，用于当检测到所述虚拟专用网通道中断时，则重新发送用于建立所述虚拟专用网通道的加密信息以重新建立所述虚拟专用网络通道；

[0032] 失败信息上传模块，用于当建立所述虚拟专用网通道失败次数达到预设次数时，则将失败信息上传到所述注册服务器。

[0033] 上述建立虚拟专用网通道的方法，在第一虚拟专用网设备接入网络时，向注册服务器发送虚拟专用网设备注册请求，虚拟专用网设备注册请求中携带了第一虚拟专用网设备物理标识，注册服务器接收到虚拟专用网设备注册请求之后，将与第一虚拟专用网络设备标识对应的建立虚拟专用网通道的信息发送给第一虚拟专用网设备，第一虚拟专用网设备根据建立虚拟专用网的信息与第二虚拟专用网设备建立虚拟专用网通道。这样，在建立虚拟专用网通道的过程中，不需要对第一虚拟专用网设备进行配置，当第一虚拟专用网设备接入网络时，即可自动建立虚拟专用网通道，使得建立虚拟专用网通道更加简单、高效。

附图说明

- [0034] 图1为一个实施例中虚拟专用网设备注册系统的应用环境图；
- [0035] 图2为一个实施例中建立虚拟专用网通道的方法的流程示意图；
- [0036] 图3为一个实施例中虚拟专用网设备证书验证的步骤的流程示意图；
- [0037] 图4为一个实施例中重新建立虚拟专用网通道的步骤的流程示意图；
- [0038] 图5为一个实施例中建立虚拟专用网通道的装置的结构框图；
- [0039] 图6为另一个实施例中建立虚拟专用网通道的装置的结构框图；
- [0040] 图7为再一个实施例中建立虚拟专用网通道的装置的结构框图。

具体实施方式

[0041] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0042] 图1为一个实施例中建立虚拟专用网通道系统的应用环境图。虚拟专用网设备注册系统包括注册服务器102、第一网络连接设备104、第二网络连接设备106、第一虚拟专用网设备108、第二虚拟专用网设备110、第一终端112和第二终端114。其中注册服务器102连接到互联网，第一虚拟专用网设备108通过第一网络连接设备104连接到互联网，第二虚拟专用网设备110通过第二专用网设备106连接到互联网，第一网络连接设备104和第二网络连接设备106支持动态分配网络地址，具体可以是交换机或路由器。第一虚拟专用网设备108和第二虚拟专用网设备110在不同的网段。第一终端112是第一虚拟专用网设备108所在网段中的终端，通过网络与第一虚拟专用网设备108连接。第二终端114是第二虚拟专用网设备110所在网段中的终端，通过网络与第二虚拟专用网设备110连接。

[0043] 如图2所示，在一个实施例中，提供一种建立虚拟专用网通道的方法，本实施例以该方法应用于图1中的虚拟专用网设备注册系统中的第一虚拟专用网设备108上来举例说明。该方法具体包括如下步骤：

[0044] 步骤202，将携带有第一虚拟专用网设备物理标识的虚拟专用网设备注册请求发送给注册服务器。

[0045] 具体地,第一虚拟专用网设备108在通过第一网络连接设备104连接到互联网时,第一虚拟专用网设备108从第一网络连接设备104的地址池中获取网络地址和网段号。网段号是用于区别网段的唯一标识,网段号具体可以通过网络地址和子网掩码来确定。第一虚拟专用网设备108在获取到网络地址和网段号之后,向注册服务器102发送虚拟专用网设备注册请求。虚拟专用网设备注册请求中包括第一虚拟专用网设备物理标识、网络地址以及网段号。第一虚拟专用网设备物理标识是第一虚拟专用网设备108的唯一标识,具体可以是物理地址或出厂编号等。第二虚拟专用网设备110在通过第二网络连接设备106连接到互联网时,第二虚拟专用网设备110也会从第二网络连接设备106的地址池中获取网络地址和网段号,并向注册服务器102发送虚拟专用网设备注册请求。注册服务器102接收到虚拟专用网设备注册请求后,提取虚拟专用网设备注册请求中的信息,并将提取到的信息与第一虚拟专用网设备物理标识或第二虚拟专用网设备物理标识对应存储。

[0046] 在一个实施例中,注册服务器102中会预先获取虚拟专用网设备物理标识并存储在注册服务器102中,注册服务器102在接收到第一虚拟专用网设备108的虚拟专用网设备注册请求时,提取第一虚拟专用网设备物理标识,查找是否已经存储有第一虚拟专用网设备物理标识,若查找到,则提取与第一虚拟专用网设备物理标识对应的密钥和第二虚拟专用网设备的地址并发送给第一虚拟专用网设备108;若未查找到,则可向第一虚拟专用网设备108返回注册失败的信息。

[0047] 步骤204,接收注册服务器根据虚拟专用网设备注册请求返回的与第一虚拟专用网设备物理标识对应的密钥和第二虚拟专用网设备的地址。

[0048] 具体地,在注册服务器102中预设有与第一虚拟专用网设备物理标识或第二虚拟专用网设备物理标识对应的密钥,以及与第一虚拟专用网设备物理标识对应的第二虚拟专用网设备物理标识,第二虚拟专用网设备110是用于与第一虚拟专用网设备108建立虚拟专用网的虚拟专用网设备。

[0049] 注册服务器102接收到第一虚拟专用网设备108发送的虚拟专用网设备注册请求之后,将虚拟专用网设备注册请求中的信息存储,并提取第一虚拟专用网设备物理标识查找对应的密钥和第二虚拟专用网设备物理标识,并提取与第二虚拟专用网设备物理标识对应的第二虚拟专用网设备110的网络地址以及网段号,注册服务器102将查找到的密钥、第二虚拟专用网设备110的网络地址以及网段号发送给第一虚拟专用网设备108。注册服务器102在接收到第二虚拟专用网设备110发送的虚拟专用网设备注册请求后,将与第二虚拟专用网设备物理标识对应的密钥和第一虚拟专用网设备106的网络地址及网段号发送给第二虚拟专用网设备110。

[0050] 步骤206,根据密钥对建立虚拟专用网通道所需的信息进行加密获得加密信息,并根据第二虚拟专用网设备的地址将加密信息发送给第二虚拟专用网设备,使第二虚拟专用网设备利用从注册服务器获取到的密钥对加密信息解密以建立虚拟专用网通道。

[0051] 具体地,第一虚拟专用网设备108接收到注册服务器102返回的密钥和第二虚拟专用网设备110的网络地址后,利用返回的密钥对建立虚拟专用通道所需的信息进行加密,建立虚拟专用通道所需的信息具体可以包括建立通道使用的加密算法、随机数和协议版本号中至少一种。协议版本号具体可以是SSL(Secure Sockets Layer,安全套接层)协议的版本号。第一虚拟专用网设备108通过对建立虚拟通道所需信息进行加密生成加密信息,根据第

二虚拟专用网设备110的网络地址将加密信息发送给第二虚拟专用网设备110。第二虚拟专用网设备110利用从注册服务器102获取到的密钥对加密信息进行解密,提取其中用于建立虚拟专用网通道的加密算法来与第一虚拟专用网设备108建立加密的虚拟专用网通道。虚拟专用网通道可以是基于SSL(Secure Sockets Layer,安全套接层)协议建立的加密通道,加密算法具体可以是3DES算法或AES256算法。

[0052] 在一个实施例中,在建立了第一虚拟专用网设备108所在网段和第二虚拟专用网设备110所在网段建立了虚拟专用网络通道后,第一虚拟专用网设备108所在网段中的第一终端112可以直接通过虚拟专用网通道与第二虚拟专用网设备110所在网段中的第二终端114进行通信。

[0053] 本实施例中,在建立虚拟专用网通道的过程中,不需要对第一虚拟专用网设备进行配置,当第一虚拟专用网设备接入网络时,即可自动建立虚拟专用网通道,使得建立虚拟专用网通道更加简单、高效。

[0054] 在一个实施例中,该建立虚拟专用网的方法还包括:注册服务器提取第一虚拟专用网设备物理标识,并在加密库中查找与第一虚拟专用网设备物理标识对应的算法标识,根据查找到的算法标识所对应的密钥生成算法生成密钥。

[0055] 具体地,注册服务器102中预设有加密库,加密库中设置有多种用于建立隧道的加密算法,具体可以是3DES(Data Encryption Standard-3,第三代数据加密标准)算法、AES256(Advanced Encryption Standard-256,使用256位密钥的高级加密标准)算法和SHA(Secure Hash Algorithm,安全哈希算法)算法等,每种算法有唯一的算法标识,并设置了虚拟专用网设备物理标识与算法标识的对应关系。当注册服务器102接收到携带有第一虚拟专用网设备物理标识的虚拟专用网设备注册请求时,查找与第一虚拟专用网设备物理标识对应的算法标识,并在加密库中提取算法标识对应的加密算法,并根据提取的加密算法生成相应的密钥。

[0056] 本实施例中,通过在注册服务器102中设置加密库,可以根据不同的虚拟专用网设备物理标识在加密库中查找相应的密钥生成算法,并根据加密库中的不同的密钥生成算法生成不同的密钥,并建立不同的虚拟专用网加密通道,使虚拟专用网加密通道更加安全。

[0057] 如图3所示,在一个实施例中,提供一种建立虚拟专用网通道的方法,该方法具体包括虚拟专用网设备证书验证的步骤,该步骤具体步骤如下:

[0058] 步骤302,根据第二虚拟专用网设备的地址向第二虚拟专用网设备发送第一虚拟专用网设备的数字证书。

[0059] 具体地,第一虚拟专用网设备108向第二虚拟专用网设备110发送第一虚拟专用网设备108的数字证书。数字证书中具体包括第一虚拟专用网设备108的身份信息,证书签名和数字证书的有效期限中的至少一种。

[0060] 步骤304,接收第二虚拟专用网设备在对数字证书的验证通过后发送的反馈信息。

[0061] 具体地,第二虚拟专用网设备110接收到第一虚拟专用网设备108发送的数字证书,提取数字证书中的身份信息和证书签名对第一虚拟专用网设备108的身份进行验证,当验证通过后向第一虚拟专用网设备108发送验证通过的信息;如果验证未通过,则向第一虚拟专用网设备108发送验证失败信息。

[0062] 步骤306,响应于反馈信息,根据密钥对建立虚拟专用网通道所需的信息进行加密

获得加密信息。

[0063] 具体地,第一虚拟专用网设备108接收到第二虚拟专用网设备110的验证通过信息后,第一虚拟专用网设备108可以利用密钥对建立虚拟专用网通道所需的信息进行加密生成加密信息,并将加密信息发送给第二虚拟专用网设备110。

[0064] 本实施例中,通过第二虚拟专用网设备110对第一虚拟专用网设备108的数字证书进行验证,增加了在建立虚拟专用网通道之前的安全验证步骤,在验证通过后才能进一步建立虚拟专用网通道,提高了虚拟专用网通道的安全性。

[0065] 如图4所示,在一个实施例中,提供一种建立虚拟专用网通道的方法,该方法具体还包括重新建立虚拟专用网通道的步骤,该步骤具体如下:

[0066] 步骤402,当检测到虚拟专用网通道中断时,则重新发送用于建立虚拟专用网通道的加密信息以重新建立虚拟专用网络通道。

[0067] 具体的,第一虚拟专用网设备108在检测到已经建立的虚拟专用网通道中断时,则会提取加密信息,并将加密信息再次发送给第二虚拟专用网设备110使第二虚拟专利网设备110对加密信息再次解密以重新建立虚拟专用网通道。

[0068] 在一个实施例中,第一虚拟专用网设备108在发出加密信息时开始计时,所计时间达到预设时间,虚拟专用网通道仍未被建立,并记录建立通道失败次数,则再次发送加密信息。预设时间可以是3秒到10秒,或者3秒到5秒。

[0069] 步骤404,当建立虚拟专用网通道失败次数达到预设次数时,则将失败信息上传到注册服务器。

[0070] 具体地,当第一虚拟专用网设备108所计的虚拟专用网通道建立失败次数达到预设次数时,则失败信息上传到注册服务器102。失败信息可以包括第一虚拟专用网设备物理标识、第一虚拟专用网设备108的网络地址、第二虚拟专用网设备物理标识和第二虚拟专用网设备110的网络地址中的至少一种。

[0071] 本实施例中,当第一虚拟专用网设备108检测到虚拟专用网通道中断时,重新建立虚拟专用网通道,以保证虚拟专用网通道的畅通,提高了虚拟专用网通道的安全可靠性。

[0072] 如图5所示,在一个实施例中,提供一种建立虚拟专用网通道的装置500,该装置包括:请求发送模块502、建立信息接收模块504和通道建立模块506。

[0073] 请求发送模块502,用于将携带有第一虚拟专用网设备物理标识的虚拟专用网设备注册请求发送给注册服务器。

[0074] 建立信息接收模块504,用于接收注册服务器根据虚拟专用网设备注册请求返回的与第一虚拟专用网设备物理标识对应的密钥和第二虚拟专用网设备的地址。

[0075] 通道建立模块506,用于根据密钥对建立虚拟专用网通道所需的信息进行加密获得加密信息,并根据第二虚拟专用网设备的地址将加密信息发送给第二虚拟专用网设备,使第二虚拟专用网设备利用从注册服务器获取到的密钥对加密信息解密以建立虚拟专用网通道。

[0076] 本实施例中,在建立虚拟专用网通道的过程中,不需要对第一虚拟专用网设备进行配置,当第一虚拟专用网设备接入网络时,即可自动建立虚拟专用网通道,使得建立虚拟专用网通道更加简单、高效。

[0077] 在一个实施例中,注册服务器用于从接收到的虚拟专用网设备注册请求中提取第

一虚拟专用网设备物理标识,从注册服务器查找是否记录有第一虚拟专用网设备物理标识,若是则提取与第一虚拟专用网设备物理标识对应的密钥和第二虚拟专用网设备的地址并发送给第一虚拟专用网设备。

[0078] 本实施例中,注册服务器106从注册请求中提取虚拟专用网设备物理标识,以验证虚拟专用网设备的身份,在验证通过后,返回建立虚拟专用网通道的信息,保证建立虚拟专用网通道的信息安全。

[0079] 在一个实施例中,注册服务器用于提取第一虚拟专用网设备物理标识,并在加密库中查找与第一虚拟专用网设备物理标识对应的算法标识,根据查找到的算法标识所对应的密钥生成算法生成密钥。

[0080] 本实施例中,通过在注册服务器102中设置加密库,可以根据不同的虚拟专用网设备物理标识在加密库中查找相应的密钥生成算法,并根据加密库中的不同的密钥生成算法生成不同的密钥,并建立不同的虚拟专用网加密通道,使虚拟专用网加密通道更加安全。

[0081] 如图6所示,在一个实施例中,建立虚拟专用网通道装置500还包括:证书发送模块508和反馈信息接收模块510。

[0082] 证书发送模块508,用于根据第二虚拟专用网设备的地址向第二虚拟专用网设备发送第一虚拟专用网设备的数字证书。

[0083] 反馈信息接收模块510,用于接收第二虚拟专用网设备在对数字证书的验证通过后发送的反馈信息。

[0084] 通道建立模块508还用于响应于反馈信息,根据密钥对建立虚拟专用网通道所需的信息进行加密获得加密信息。

[0085] 本实施例中,通过第二虚拟专用网设备110对第一虚拟专用网设备108的数字证书进行验证,增加了在建立虚拟专用网通道之前的安全验证步骤,在验证通过后才能进一步建立虚拟专用网通道,提高了虚拟专用网通道的安全性。

[0086] 如图7所示,在一个实施例中,建立虚拟专用网通道的装置500还包括:通道重新建立模块512和失败信息上传模块514。

[0087] 通道重新建立模块512,用于当检测到虚拟专用网通道中断时,则重新发送用于建立虚拟专用网通道的加密信息以重新建立虚拟专用网络通道。

[0088] 失败信息上传模块514,用于当建立虚拟专用网通道失败次数达到预设次数时,则将失败信息上传到注册服务器。

[0089] 本实施例中,当第一虚拟专用网设备108检测到虚拟专用网通道中断时,重新建立虚拟专用网通道,以保证虚拟专用网通道的畅通,提高了虚拟专用网通道的安全可靠性,且将失败信息上传到注册服务器102,调试人员可以根据失败信息来排除故障。

[0090] 以上所述实施例的各技术特征可以进行任意的组合,为使描述简洁,未对上述实施例中的各个技术特征所有可能的组合都进行描述,然而,只要这些技术特征的组合不存在矛盾,都应当认为是本说明书记载的范围。

[0091] 以上所述实施例仅表达了本发明的几种实施方式,其描述较为具体和详细,但并不能因此而理解为对发明专利范围的限制。应当指出的是,对于本领域的普通技术人员来说,在不脱离本发明构思的前提下,还可以做出若干变形和改进,这些都属于本发明的保护范围。因此,本发明专利的保护范围应以所附权利要求为准。

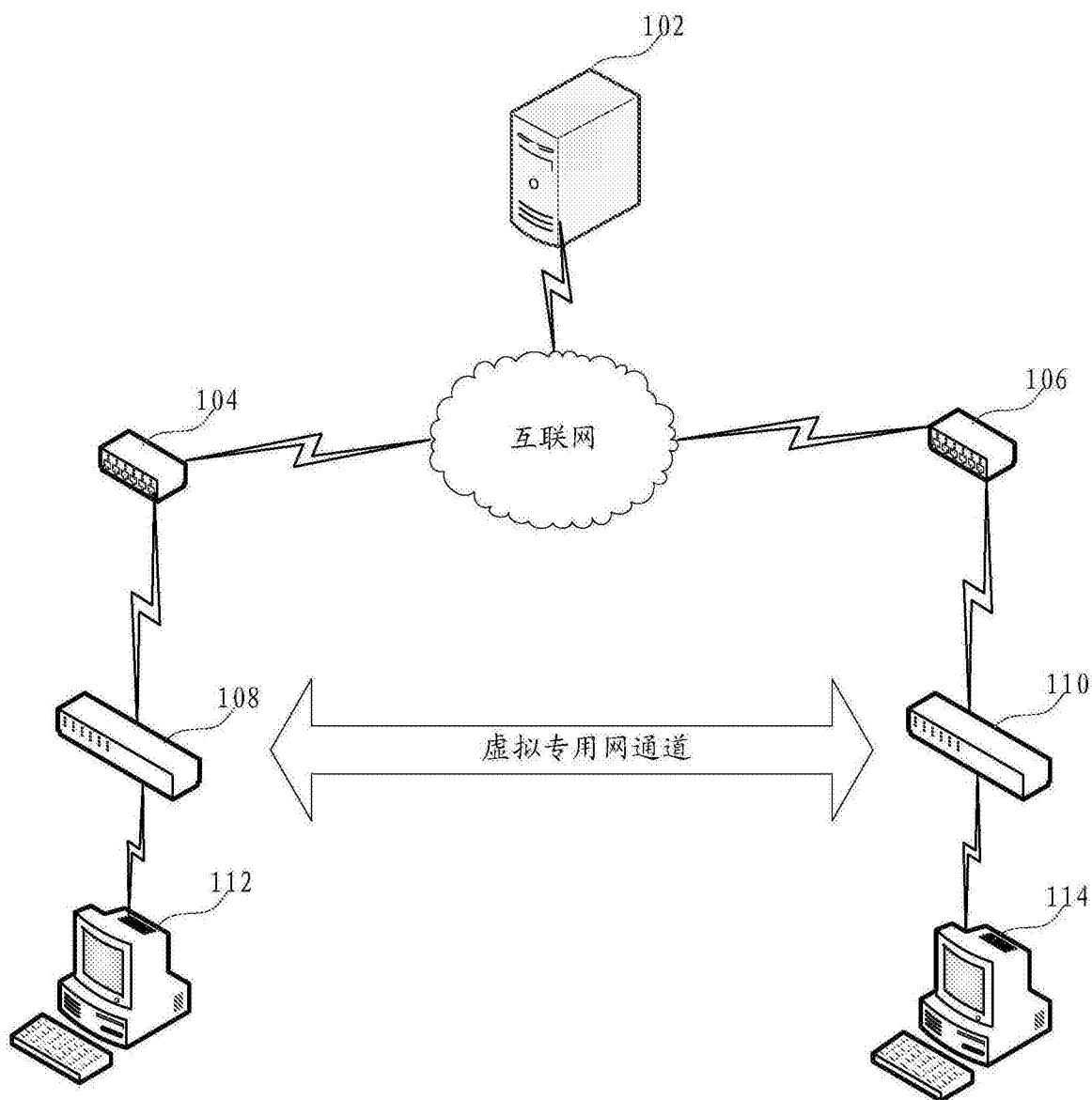


图1

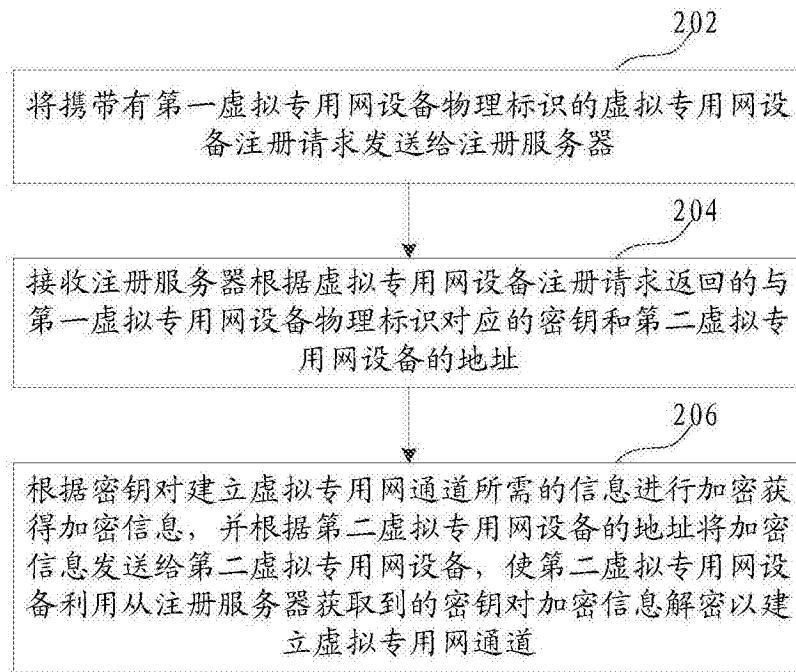


图2

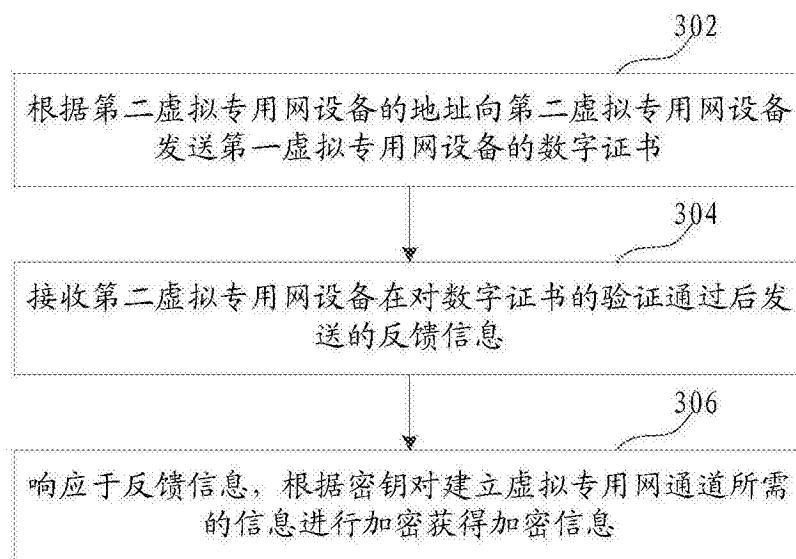


图3

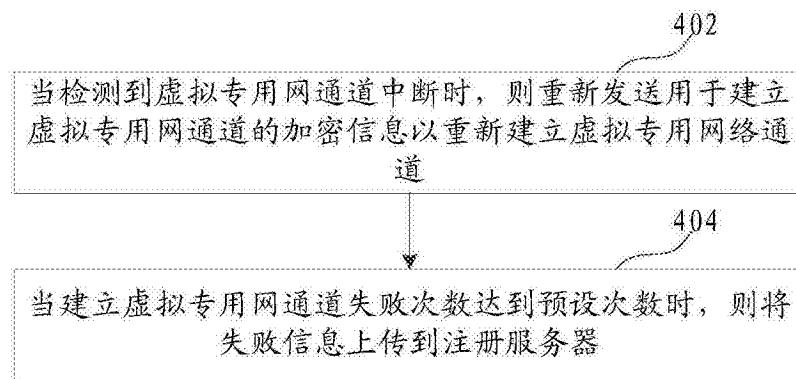


图4

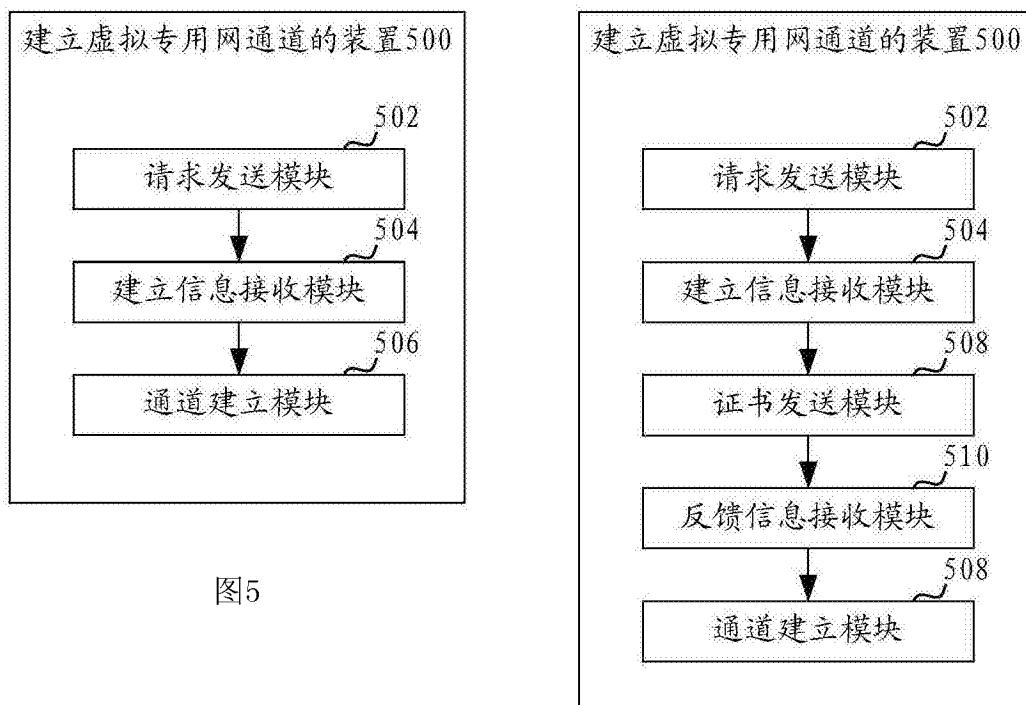


图5

图6

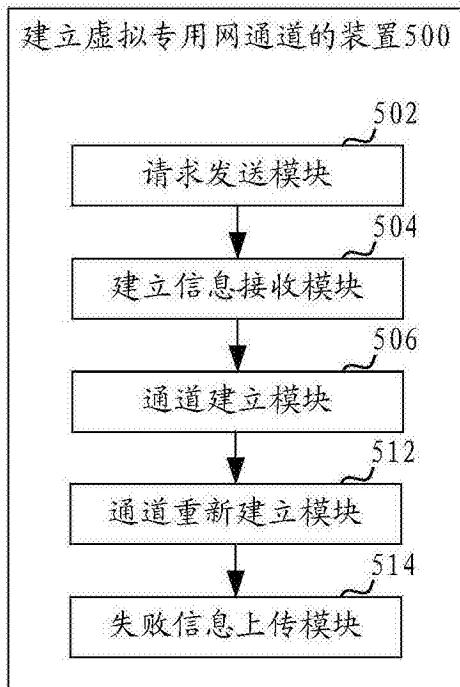


图7