(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101083607 B
(45)授权公告日 2010.12.08

(21)申请号 200610027047.2

(22)申请日 2006.05.30

(73)专利权人 倪海生
地址 201204 上海市浦东新区白杨路 199 弄 24 号 202 室
专利权人 朱琳

(72)发明人 朱琳 倪海生

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 章蔚强

(51)Int.Cl.
H04L 12/56(2006.01)
H04L 29/06(2006.01)
H04L 12/46(2006.01)

(56)对比文件
WO 01/33801 A2,2001.05.10, 全文.
CN 1571398 A,2005.01.26, 全文.
CN 1350242 A,2002.05.22, 全文.

审查员 文娟

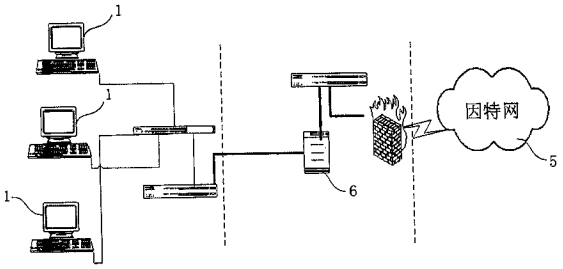
权利要求书 1 页 说明书 8 页 附图 7 页

(54)发明名称

一种用于内外网络隔离的因特网访问服务器及其处理方法

(57)摘要

一种用于内外网络隔离的因特网访问服务器及其处理方法，其中该服务器用于将用户计算机和因特网隔开，并在基于通用的计算机服务器本体上包括图形终端服务模块、图形终端网络传输模块、对内网络传输控制模块、文件传输控制模块、系统配置和用户管理模块和因特网访问传输模块。本发明是以特殊的访问方式和传输控制来实现内外网络的隔离和安全。所有有授权的内网中计算机可以通过因特网访问服务器访问因特网，因特网访问服务器包含图象终端，而通过这些方式下载下来的文件或信息，只能存放在外网的个人专用存储空间中，再从外网服务器上下载下来到内网。而无法（或严格受控）把内网中的文件上传。本发明不仅实现可以保护内网中的资料，而且可以提供对外的资料查询和联系。



CN 101083607 B

1. 一种用于内外网络隔离的因特网访问服务器，连接在由若干个用户计算机组成的内网和因特网之间，用于将用户计算机和因特网隔开，其基于通用的计算机服务器本体，其特征在于：

所述的因特网访问服务器包括：图形终端服务模块，图形终端网络传输模块，对内网络传输控制模块，文件传输控制模块，系统配置和用户管理模块，以及因特网访问传输模块，其中：

图形终端服务模块与图形终端网络传输模块相连，为客户端提供图形终端服务；

对内网络传输控制模块，连接在所述计算机服务器本体上，用于提供对网络会话的严格限制，保证网络内客户端和本因特网访问服务器之间都是合法的会话；

文件传输控制模块，连接在所述计算机服务器本体上，用于管理用户计算机本地硬盘与因特网访问服务器各用户专有存储空间之间文件资料的传输；

系统配置和用户管理模块，连接在所述计算机服务器本体上，用于增删、修改用户设置，上载部分的流程设计，以及系统参数设置；

因特网访问传输模块，连接在所述计算机服务器本体上，用于提供所述图形终端服务模块访问因特网的传输控制管理；

所述的因特网访问服务器还包括两个网络界面，一个是对用户计算机提供因特网图形终端访问服务的网络界面，另一个是连接和访问因特网的网络界面。

2. 根据权利要求 1 所述的用于内外网络隔离的因特网访问服务器，其特征在于：

所述图形终端服务模块包括 www 网页浏览器，电子邮件客户端，FTP 客户端。

3. 根据权利要求 1 所述的用于内外网络隔离的因特网访问服务器，其特征在于：

所述对内网络传输控制模块在客户端和所述的因特网访问服务器之间所控制的数据传输有三种数据会话，即：图象终端网络协议，服务器向客户的合法下载，客户机向因特网访问服务器的受控的上载。

4. 根据权利要求 1 所述的用于内外网络隔离的因特网访问服务器，其特征在于：

所述文件传输控制模块包括下载和上载两部分。

5. 根据权利要求 1 所述的用于内外网络隔离的因特网访问服务器，其特征在于：

所述的对内网络传输控制模块、图形终端服务模块、文件传输控制模块、系统配置和用户管理模块、以及因特网访问传输模块按预定的组合方式分别设置在不同的通用的计算机服务器本体上。

6. 一种在权利要求 1 所述的因特网访问服务器中进行上传控制的方法，包括下列步骤：

传输连接初始化后，认证用户通过文件上传文件，上传文件保存在所述的因特网访问服务器保密区，经判断后，若通过，则从所述的保密区传输到用户个人存储区，并告结束；若不通过，则直接记录失败结果，并告结束。

一种用于内外网络隔离的因特网访问服务器及其处理方法

技术领域

[0001] 本发明涉及计算机网络安全技术，尤其适用于在局域网络里实现网络中内外网的隔离，即内网是内网含有机密文件和资料的网络，外网是可以和 internet 连接的网络，并在隔离同时实现 internet 的便利使用，具体地说，本发明是涉及一种用于内外网络隔离的因特网访问服务器及其处理方法。

背景技术

[0002] 现有公司和机构网络架构最常用的方式就是在内部建构自己的局域网，然后自己的局域网再通过防火墙或 NAT（内部网络地址转换协议）的方式连接到外部的因特网(internet)，这样内部计算机就通过防火墙安全管理访问 internet 了，而外部到内部的连接必须经过防火墙的合法验证。

[0003] 为实现内部局域网中上 internet 的追踪和控制，一般企业还会建设一个 proxy server（代理服务器），所有的局域网中计算机只有透过 proxy server 才能上网。

[0004] 图 1 是一个典型的局域网连接广域网络的典型结构，包括由若干个计算机 1、交换机 2 和路由器 3 组成的局域网、防火墙 4 和因特网 5。

[0005] 隔离概念是在为了保护高安全度网络环境的情况下产生的；隔离产品的大量出现，也是经历了五代隔离技术不断的实践和理论相结合后得来的。

[0006] 第一代隔离技术－完全的隔离

[0007] 此方法使得网络处于信息孤岛状态，做到了完全的物理隔离，需要至少两套网络和系统，更重要的是信息交流的不便和成本的提高，这样给维护和使用带来了极大的不便。

[0008] 第二代隔离技术－硬件卡隔离

[0009] 在客户端增加一块硬件卡，客户端硬盘或其他存储设备首先连接到该卡，然后再转接到主板上，通过该卡能控制客户端硬盘或其他存储设备。而在选择不同的硬盘时，同时选择了该卡上不同的网络接口，连接到不同的网络。但是，这种隔离产品有的仍然需要网络布线为双网线结构，产品存在着较大的安全隐患。

[0010] 第三代隔离技术－数据转播隔离

[0011] 利用转播系统分时复制文件的途径来实现隔离，切换时间非常之久，甚至需要手工完成，不仅明显地减缓了访问速度，更不支持常见的网络应用，失去了网络存在的意义。

[0012] 第四代隔离技术－空气开关隔离

[0013] 它是通过使用单刀双掷开关，使得内外部网络分时访问临时缓存器来完成数据交换的，但在安全和性能上存在有许多问题。

[0014] 第五代隔离技术－安全通道隔离

[0015] 此技术通过专用通信硬件和专有安全协议等安全机制，来实现内外部网络的隔离和数据交换，不仅解决了以前隔离技术存在的问题，并有效地把内外部网络隔离开来，而且高效地实现了内外网数据的安全交换，透明支持多种网络应用，成为当前隔离技术的发展方向。

[0016] 但是，在第五代隔离技术中如何做到安全和使用便利是难点所在。

[0017] 最常用的访问 internet 的访问方式有 web，mail，FTP 等方式，这些方式都是灵活而强大的，而 internet 中这些的内容资源丰富巨大，为工作与外部世界的交互提供非常多的方便和帮助。

[0018] 而与 internet 的交互中包括从 internet 中拿取资料和把自己的资料分享或传递到 internet 和别人分享。关键就在于这个把自己资料分享或传递出去，internet 技术为我们提供成百上千种方法，这些方法在为大家提供便利的同时，也为组织和机构的资料外泄带来巨大的风险。

[0019] 为防范这些风险，从技术上来讲，有些组织和机构通常采用的有两种办法，一就是对所有机密的文件采用加密的方法，二是用隔离的办法把有机密资料的网络与 internet 隔离开。

[0020] 然而第一种方法，即对所有机密文件加密的方式，用密码控制文件的访问和文件用密码又为用户带来的不方便性，所以就出现了对文件进行文件密钥集中控制的方法，但这又有另外的问题，各种机密文件有各种格式，所有的文件的阅读都必须在特殊的文件阅读器中去阅读。这个又为密码控制带来不方便性。

[0021] 第二种方法也被广泛采用，许多网络从物理上被分为两个网络，两台计算机分别被连接到不同网络。而且也因此出现了很多在这方面的技术，比如物理隔离卡，网闸。物理隔离卡需要对一台计算机做改装来实现一台计算机里的两块硬盘的物理隔离，而且能在两个网络中切换。网闸是用来隔离两个内外网，并允许两个网络中必要的传输。

[0022] 但上述的两种方法都为用户的使用带来许多的额外的使用成本和不方便。而采用逻辑的方式有着 internet 连接的多样性，彻底的逻辑隔离是很难做到的。而本发明就是针对解决上述问题提出的。

发明内容

[0023] 本发明的目的在于提供一种用于内外网络隔离的因特网访问服务器及其处理方法，通过该因特网访问服务器，既能使用户能方便地从 internet 上获得信息和资料，又能使组织和机构内的文件发送得到有序的控制，实现方便合理的分隔企业内部网络和外部 internet 网络。

[0024] 本发明所提供的一种用于内外网络隔离的因特网访问服务器，连接在由若干个用户计算机组成的内网和因特网之间，用于将用户计算机和因特网隔开，其基于通用的计算机服务器本体，其特点是：

[0025] 所述的因特网访问服务器包括：图形终端服务模块，图形终端网络传输模块，对内网络传输控制模块，文件传输控制模块，系统配置和用户管理模块，以及因特网访问传输模块，其中：

[0026] 图形终端服务模块与图形终端网络传输模块相连，为客户端提供图形终端服务；

[0027] 对内网络传输控制模块，连接在所述计算机服务器本体上，用于提供对网络会话的严格限制，保证网络内客户端和本因特网访问服务器之间都是合法的会话；

[0028] 文件传输控制模块，连接在所述计算机服务器本体上，用于管理用户计算机本地硬盘与因特网访问服务器各用户专有存储空间之间文件资料的传输；

[0029] 系统配置和用户管理模块，连接在所述计算机服务器本体上，用于增删、修改用户设置，上载部分流程设计，以及系统参数设置；

[0030] 因特网访问传输模块，连接在所述计算机服务器本体上，用于提供所述图形终端服务模块访问 internet 的传输控制管理。

[0031] 在上述的用于内外网络隔离的因特网访问服务器中，它还包括两个网络界面，一个是对用户计算机提供因特网图形终端访问服务的网络界面，另一个是连接和访问因特网的网络界面。

[0032] 在上述的用于内外网络隔离的因特网访问服务器中，所述图形终端服务模块包括 www 网页浏览器，电子邮件客户端，FTP 客户端。

[0033] 在上述的用于内外网络隔离的因特网访问服务器中，所述对内网络传输控制模块在客户端和 internet 服务器之间所控制的数据传输有三种数据会话，即：图象终端网络协议，服务器向客户的合法下载，客户机向因特网访问服务器的受控的上载。

[0034] 在上述的用于内外网络隔离的因特网访问服务器中，所述文件传输控制模块包括下载和上载两部分。

[0035] 本发明还提供了一种上述的因特网访问服务器中进行客户端登记的方法，包括下列步骤：

[0036] 客户端程序初始化，得到数据标识号和用户授权信息，向因特网访问服务器登记数据标识号和授权过程；

[0037] 对于因特网访问服务器确认授权的，则因特网访问服务器记录登记，并告登记结束；否则直接告登记结束。

[0038] 本发明又提供了一种在上述的因特网访问服务器中进行数据包过滤的方法，包括下列步骤：

[0039] 收到传输数据包，判断是否有正确数据标识号：

[0040] 对于有正确数据标识号的，从数据包中得到 K 客户端和服务器地址，并判断是否拥有授权登记并且数据类型的合法性：

[0041] 若是，则传输数据包到正确地址，并告结束；

[0042] 若否，丢弃数据包；

[0043] 对于没有正确数据标识号的，则直接丢弃数据包，并告结束。

[0044] 本发明还提供了一种在因特网访问服务器中用户从 internet 上下载到用户客户端的方法，包括下列步骤：

[0045] 在用户使用图形终端中的 www 网页浏览器，或电子邮件客户端，或 FTP 客户端把文件下载到用户私有存储空间后，文件传输模块在下载连接初始化后可根据服务器用户私有存储空间的文件清单对客户端列出所有文件信息，用户可选择的下载；

[0046] 在读取用户定义好的目标目录后，传输模块通过受认证的数据传输通道，传输到用户自己的内网机器上的预先定义好的本地文件目录中。

[0047] 本发明再提供了一种在上述的因特网访问服务器中进行上传控制的方法，包括下列步骤：

[0048] 传输连接初始化后，认证用户通过文件上传文件，上传文件保存所述的因特网访问服务器保密区，经判断后，若通过，则从所述的保密区传输到用户个人存储区，并告结束；

若不通过，则直接记录失败结果，并告结束。

[0049] 本发明最后提供了一种如上的用于内外网络隔离的因特网访问服务器，其特征在于：所述的对内网络传输控制模块、图形终端服务模块、文件传输控制模块、系统配置和用户管理模块、以及因特网访问传输模块按预定的组合方式分别设置在不同的计算机服务器本体上。

[0050] 本发明是以特殊的访问方式和传输控制来实现内外网络的隔离和安全。所有有授权的内网中计算机可以通过因特网访问服务器访问因特网，因特网访问服务器可以包含图象终端中的 internet 常用客户端工具（如：www，email，ftp 等）。而通过这些方式下载下来的文件或信息，它们只能存放在外网的个人专用存储空间中，再从外网服务器上下载下来到内网。而无法（或严格受控）把内网中的文件上传。通过本发明不仅可以实现隔离保护内网中的资料，而且可以提供对外的资料查询和联系。

附图说明

[0051] 通过以下对本发明的一实施例结合其附图的描述，可以进一步理解本发明的目的、具体结构特征和优点。其中，附图为：

[0052] 图 1 是现有典型的网络架构示意图；

[0053] 图 2 是本发明因特网访问服务器置于图 1 所示网络架构中的示意图；

[0054] 图 3 是本发明因特网访问服务器的功能模块框图；

[0055] 图 4 是本发明中客户端登记流程示意图；

[0056] 图 5 是本发明中对内数据控制模块数据包过滤过程示意图；

[0057] 图 6 是本发明中文件传输控制模块具体上传的控制流程示意图；

[0058] 图 7 是本发明中图形终端服务模块建立一个 internet 访问连接的流程示意图；

[0059] 图 8 本发明中文件传输控制模块具体下载的控制流程示意图。

具体实施方式

[0060] 本发明的基本思想是：实现在机构内既能便利地访问 internet，又通过隔离和特殊的传输方法充分保障机构内的网络安全。

[0061] 本发明首先需要对网络结构进行改造，以图 1 所示的现有典型网络结构看，本发明把由若干个用户计算机（客户端）组成的内网和因特网（internet）隔开，使的客户端无法直接或间接（透过 proxy 等方法）访问 internet 资源。

[0062] 如图 2 所示，本发明在因特网（internet）5 和用户计算机 1 之间架设了因特网访问服务器 6。客户端与 internet 是隔开的，只有因特网访问服务器才能真正透过路由器和防火墙来访问 internet，客户端只能通过因特网访问服务器图形终端来访问 internet。

[0063] 1）因特网访问服务器

[0064] 硬件平台的实现

[0065] 因特网访问服务器硬件本是采用通用的计算机服务器，包含服务器的主板、CPU、内存、显示适配卡和网卡。在本服务器中需要对网络布件做特殊改变。需要两块网卡，一块是对客户机器提供 internet 图形终端访问服务的，它的 IP 是网络内部计算机能直接连接的。一块是连接和访问 internet 的，它的 IP 是能和网络中 internet 路由器直接通信的。

当然另一种变通的做法它也可以采用一块网卡，在操作系统中绑定两套网络配置设置到一块网卡中。这两套网络配置的作用分别与前面相同。总之该服务器有两个网络界面，一个是对客户机器提供 internet 图形终端访问服务的，一个是连接和访问 internet 的。

[0066] 另外在服务器的操作系统中这两个网络界面不提供路由或数据包转发功能。

[0067] 软件部分设计和实现

[0068] 如图 3 所示，因特网访问服务器包括：图形终端服务模块 61，图形终端网络传输模块 62，对内网络传输控制模块 63，文件传输控制模块 64，系统配置和用户管理模块 65，因特网访问传输模块 66。

[0069] 图形终端服务模块与图形终端网络传输模块相结合，为客户端提供图形终端服务。

[0070] 对内网络传输控制模块，用于提供对网络会话的严格限制，保证网络内客户端和本服务器系统之间都是合法的会话。

[0071] 文件传输控制模块，用于管理用户计算机本地硬盘与因特网访问服务器各用户专有存储空间之间文件资料的传输。

[0072] 系统配置和用户管理模块，用于增删、修改用户设置，上载部分流程设计，以及系统参数设置。

[0073] 因特网访问传输模块，用于提供所述图形终端服务模块访问 internet 的传输控制管理。

[0074] 本服务器可以实现在 Linux，Microsoft Window 服务器和 Unix 中的任一种操作系统上。

[0075] 下面就各个功能模块分别进行详细描述。

[0076] 1) 图形终端服务模块与图形终端网络传输模块

[0077] 图形终端服务模块包括基本的 www 网页浏览器，电子邮件，FTP 客户端。图形终端服务模块能启动 / 调用 www 网页浏览器，电子邮件，FTP 作为客户访问 internet 的工具。但随着 internet 技术的发展，这些常用工具是可以灵活扩充的。

[0078] 图形终端服务模块的客户 / 服务器模型不是建立在特定的软、硬件资源之上，而是建立在图形终端协议之上。图形终端协议是一个抽象的应用服务协议，包括了终端的输入请求和对服务器服务程序发出的屏幕 / 媒体输出命令，不包括对底层硬件的访问和控制。图形终端协议是图形终端服务程序和图形终端客户程序进行通信的途径。图形终端客户程序通过它向图形终端服务程序发送请求，而图形终端服务程序通过它回送状态及一些其它的信息。真正控制终端工作的是图形终端服务程序。

[0079] 此外，图形终端协议是建立在一些常用的传输协议之上，包括 TCP/IP、IPX/SPX 和 DECnet 等网络协议。通过这些协议，客户和服务器之间就可能方便地对话。

[0080] 图形终端是一个基于网络的图形引擎，它可以在与远端机连接、在服务器机器上运行应用，使用远程服务器的 CPU，硬盘空间的同时，在客户端的图形终端上处理 I/O 操作，包括输入，显示，声音。使用 internet 访问图形终端访问 internet 与普通客户端直接访问 internet 最大的不同就在于你的网页浏览器，邮件客户端实际上是在服务器上运行的，你能直接使用的硬盘空间是服务器上您被授权能使用的硬盘空间。本发明不局限于何种图形终端的协议。

[0081] 服务器建立一个 internet 访问连接的流程见图 7。首先检查服务器是否正常，正常再读取连接用户的个性化配置和数据，以便对 www 浏览器，email，ftp 客户端进行初始化。在初始化一个 internet 连接中包含重要的一点，每个用户都有自己的个性化设置，比如 internet 访问的 cookie（个性化参数）。这些初始化设置都单独保存在每个用户的私有存储区。在访问连接初始化过程中需要参考他们。

[0082] www 网页浏览器实现的是基于 http 网络协议的的 html（超文本标记语言）显示和浏览组件，电子邮件客户端是基于 smtp（简单邮件传输协议）的 email 管理工具，FTP 客户端是 FTP 图形化界面。它们的使用可以是采用第三方组件的方式来调用，而这类第三方组件非常繁多。这里不对这三部分的实现做详细的描述。

[0083] 而图形终端网络传输模块维护的是把图形终端服务层的对网络上机器的输出请求做压缩，使得在网络上占的频宽足够小。

[0084] 本发明中 internet 访问的实现是通过把客户端和 internet 千变万化的传输协议统一转变为客户端和 internet 访问服务器之间的基于图形终端的传输协议和后面讲的传输协议。

[0085] 2) 对内网络传输控制模块

[0086] 对内网络传输控制模块是用于控制客户端和 internet 访问服务器之间的数据安全传输，实现方式是有条件的数据包过滤。

[0087] 数据包过滤的实现是在对内的网络界面上的网络协议中绑定网络数据包的过滤程序实现的。通过对内网络界面的数据包都需要受到对内网络传输控制层的筛选。

[0088] 只有合法的数据包才允许通过。

[0089] 对内网络传输控制模块是实现在客户端和本因特网访问服务器之间的数据传输只能是三种数据会话：图象终端网络协议，服务器向客户的合法下载，客户机向 internet 访问服务器的严格受控的上载。而控制网关识别这三类会话是通过识别通信网络数据包中加密后的数据标记。没有正确数据标记的数据包一律被丢弃。

[0090] 数据包的标记可以是在网络数据每个数据包中必须包含客户端网卡的物理地址和会话开始登记时间的加密数据转化。

[0091] 在对内网络传输控制层登记的会话记录是：

[0092]

ClientMac	客户端 mac 地址
ClientIP	IP 地址
ServerMac	服务器 mac 地址
ServerIP	服务器 IP 地址
SessionMark	会话标记号
Sessionstarttime	会话开始时间

SessionLasttime	最近会话开始时间
Active	是否失效

[0093] 系统每隔两分种会自动刷新记录一次，两分钟内没有通话的会话记录会失效。再使用需要重新认证。

[0094] 具体客户端登记的流程见图 4，数据过滤的流程图见图 5。

[0095] 参见图 4，客户端程序初始化，得到数据标识号和用户授权信息，向因特网访问服务器登记数据标识号和授权过程，对于因特网访问服务器确认授权的，则因特网访问服务器记录登记，并告登记结束；否则直接告登记结束。

[0096] 参见图 5，收到传输数据包，判断是否有正确数据标识号：

[0097] 对于有正确数据标识号的，从数据包中得到客户端和服务器地址，并判断是否拥有授权登记并且数据类型的合法性，若是，则传输数据包到正确地址，并告结束；若否，丢弃数据包；

[0098] 对于没有正确数据标识号的，则直接丢弃数据包，并告结束。

[0099] 因此，客户端要访问因特网访问服务器必须先向对内网络传输控制模块登记并得到服务器用户认证，才允许数据包通过，而客户端关闭或长时间没有活动，在访问控制网关这个客户端的登记蒋被注销。新使用时需要重新登记。

[0100] 没有登记的访问不会被通过，不管是从客户端到服务器端还是服务端到客户端。所以会话登记和数据包的加密数据标记是数据包通过的两个关键条件。

[0101] 3) 文件传输控制模块

[0102] 除了图形终端协议，在 internet 访问服务器和 internet 访问的客户端还允许存在文件传输加密的数据传输通道，在这里面包含下载和上载两部分。

[0103] 具体下载的控制流程如图 8 所示，在用户使用图形终端中的 www 网页浏览器，或电子邮件客户端，或 FTP 客户端把文件下载到用户私有存储空间后，文件传输模块在下载连接初始化后可根据服务器用户私有存储空间的文件清单对客户端列出所有文件信息，用户可选择的下载；

[0104] 在读取用户定义好的目标目录后，传输模块通过受认证的数据传输通道，传输到用户自己的内网机器上的预先定义好的本地文件目录中。

[0105] 用户从 internet 中下载文件方法是先把 internet 中文件下载到本因特网访问服务器中私有的存储空间中。然后文件传输模块中可根据存储空间的文件对客户端列出所有文件信息，用户可选择的下载。通过受认证的数据传输通道，传输到用户自己的内网机器上的预先定义好的本地文件目录中。

[0106] 高级用户则允许可控的文件上传。

[0107] 具体上传的控制流程如图 6 所示，即：上传中高级用户通过受认证的加密的数据传输通道上传后，上传后文件被放在服务器的保密存储区，然后文件会受到相关的审查，只有通过后文件才会出现在服务器中的用户的专用存储区。用户则可以再通过图形终端服务对 internet 访问时做真正的文件外传。在下载和上传中 internet 服务器上为用户分配的个人存储区在个人用户的内网络机器和外部 internet 之间起到了存储过渡作用。

[0108] 4) 系统配置和用户管理模块

[0109] 该模块关键在用户管理部分，用户管理部分是对可访问 internet 的用户的管理，对用户的增删，修改，用户使用存储区空间和空间大小的指定。

[0110] 具体核心用户数据记录是：

[0111]

Username	用户名
Password	用户密码
SpacePath	私有存储路径
SpaceSize	私有存储空间大小
DownloadEnable	能否下载
UploadEnable	能否上载
Disable	用户是否失效

[0112] 5) 因特网访问传输模块

[0113] 在本系统 internet 访问传输实现的是为图形终端服务提供 internet 访问传输。它的实现不在保护范围之内。故不再详述。

[0114] 本发明对内网络传输控制模块和图形终端服务模块等各子模块可以分开实施在不同的服务器中。如对内传输控制模块的实施在服务器 A 上，图形终端服务实施在 B 上，那么客户端的数据访问必须访问 A，然后经过 A 验证之后再由 A 把数据包转发给 B。实现方法和效果相同。它们的分开实施在不同服务器上是本服务系统的一种变型。

[0115] 该发明的实施效果：

[0116] 在企业或机构里实施本结构的系统后，用户可以很方便的使用专用的客户端连接到远程的因特网访问服务器，用户的客户端是对服务器的远程图像终端。在这个客户端里使 internet，，每个用户在服务器上有个自己私有的下载存储区，用户可以很方便的把自己的下载存储区中的文件再传递到用户自己的办公电脑上去。而文件的上载是严格受控的。

[0117] 本发明使用后，大部分需要物理区分内外网络的机构，都可以在享用 internet 便利性的同时又保证了信息的安全，可反防止失误的性的信息外泄，同时对防止病毒和木马都是一个有效的措施。

[0118] 虽然本发明已参照当前的具体实例进行了描述，但是本技术领域的普通技术人员应该认识到，以上的实例仅是用来说明本发明，在没有脱离本发明精神的情况下还可做出各种等效的变化和修改。因此，只要在本发明的实质精神范围内对上述实例的变化，变型都将落在本发明的权利要求书的范围内。

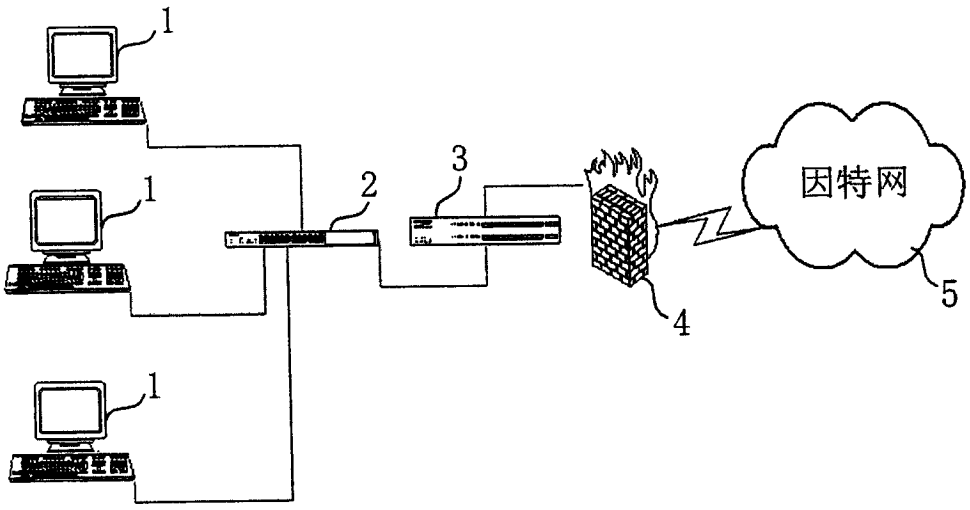


图 1

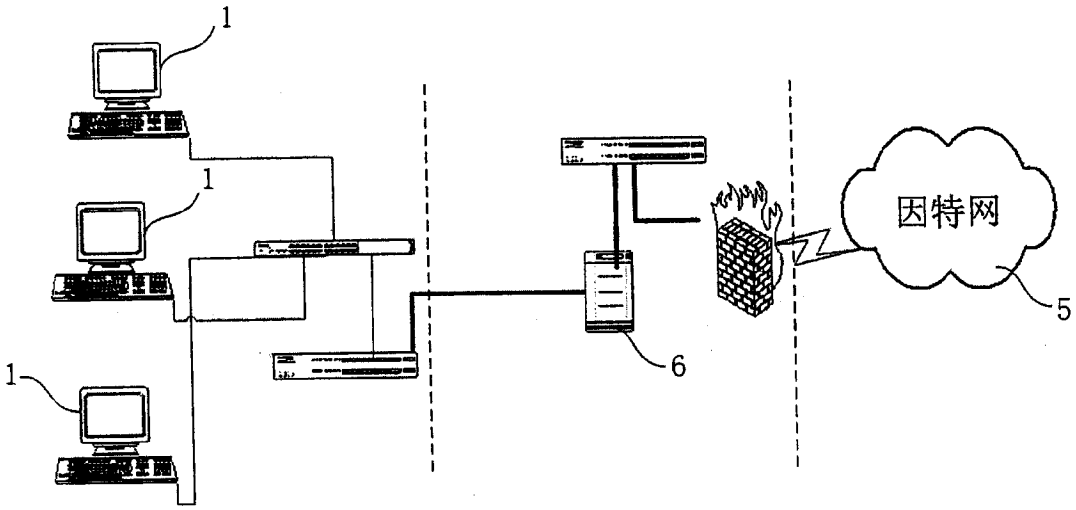


图 2

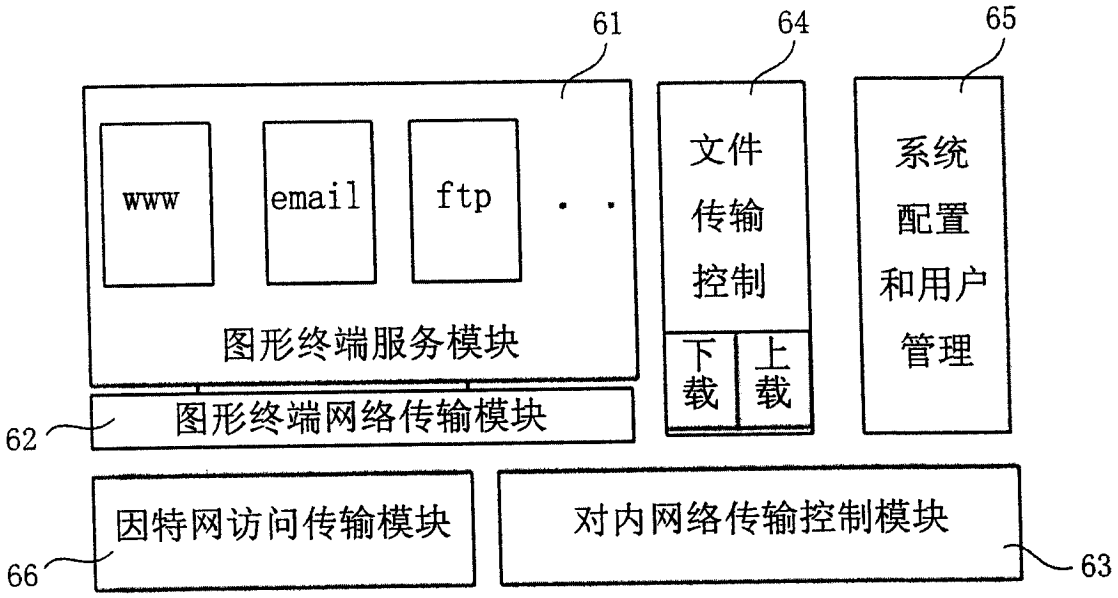

61
64
65
www
email
ftp
. .
图形终端服务模块
文件
传输
控制
下载
上载
系统
配置
和用户
管理
62
图形终端网络传输模块
因特网访问传输模块
对内网络传输控制模块
66
63

图 3

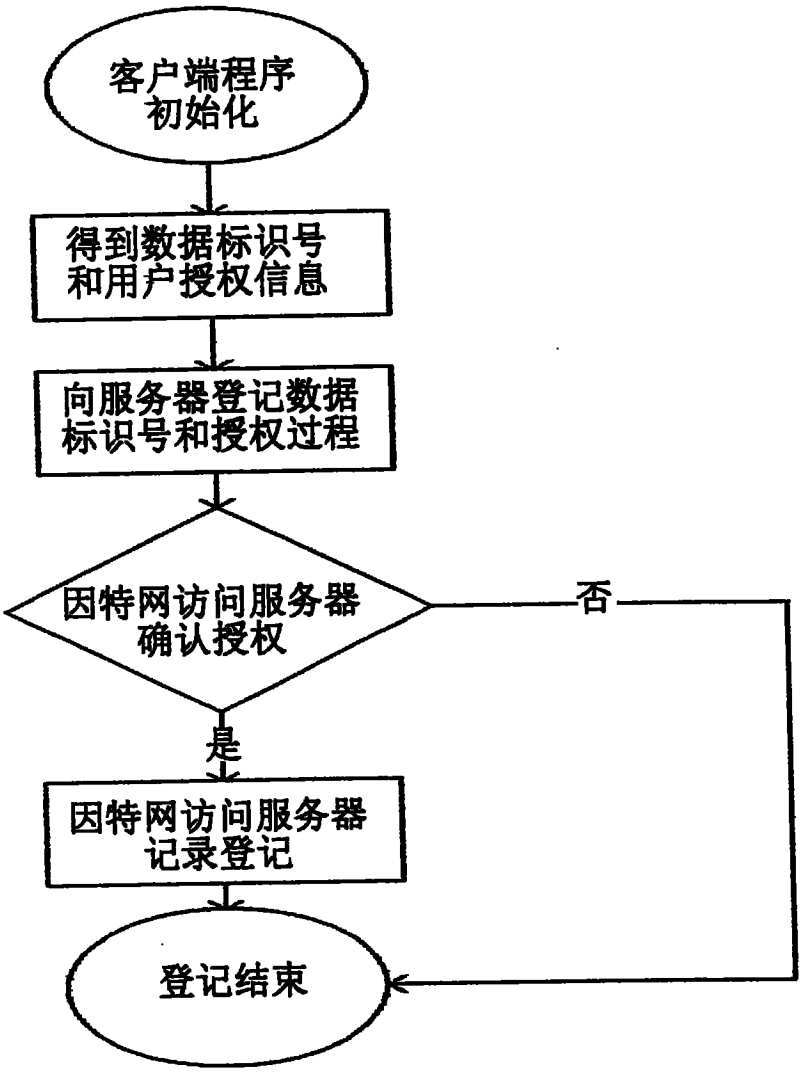

客户端程序
初始化
得到数据标识号
和用户授权信息
向服务器登记数据
标识号和授权过程
因特网访问服务器
确认授权
否
是
因特网访问服务器
记录登记
登记结束

图 4

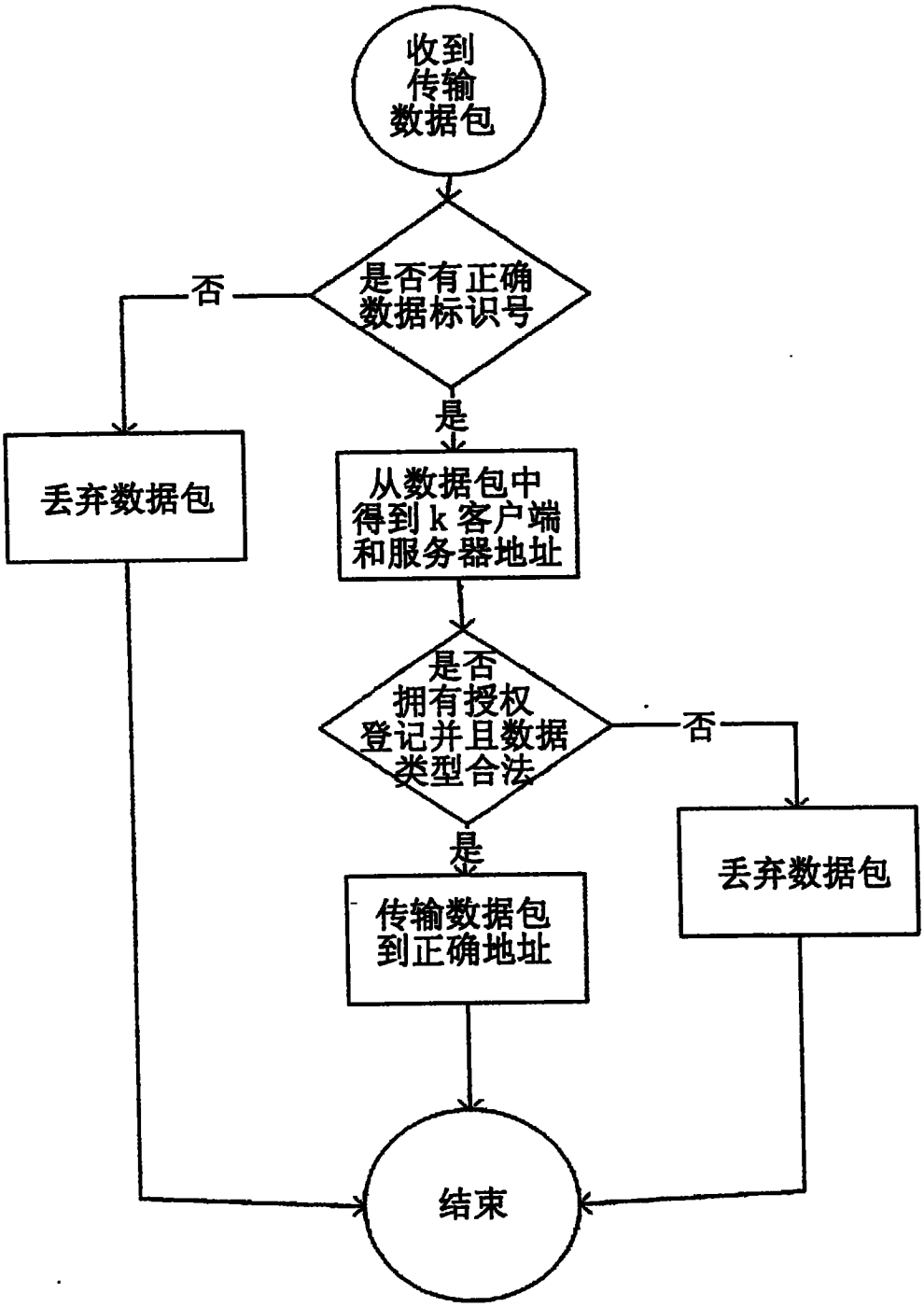

收到
传输
数据包
是否有正确
数据标识号
否
是
丢弃数据包
从数据包中
得到 k 客户端
和服务器地址
是否
拥有授权
登记并且数据
类型合法
否
是
丢弃数据包
传输数据包
到正确地址
结束

图 5

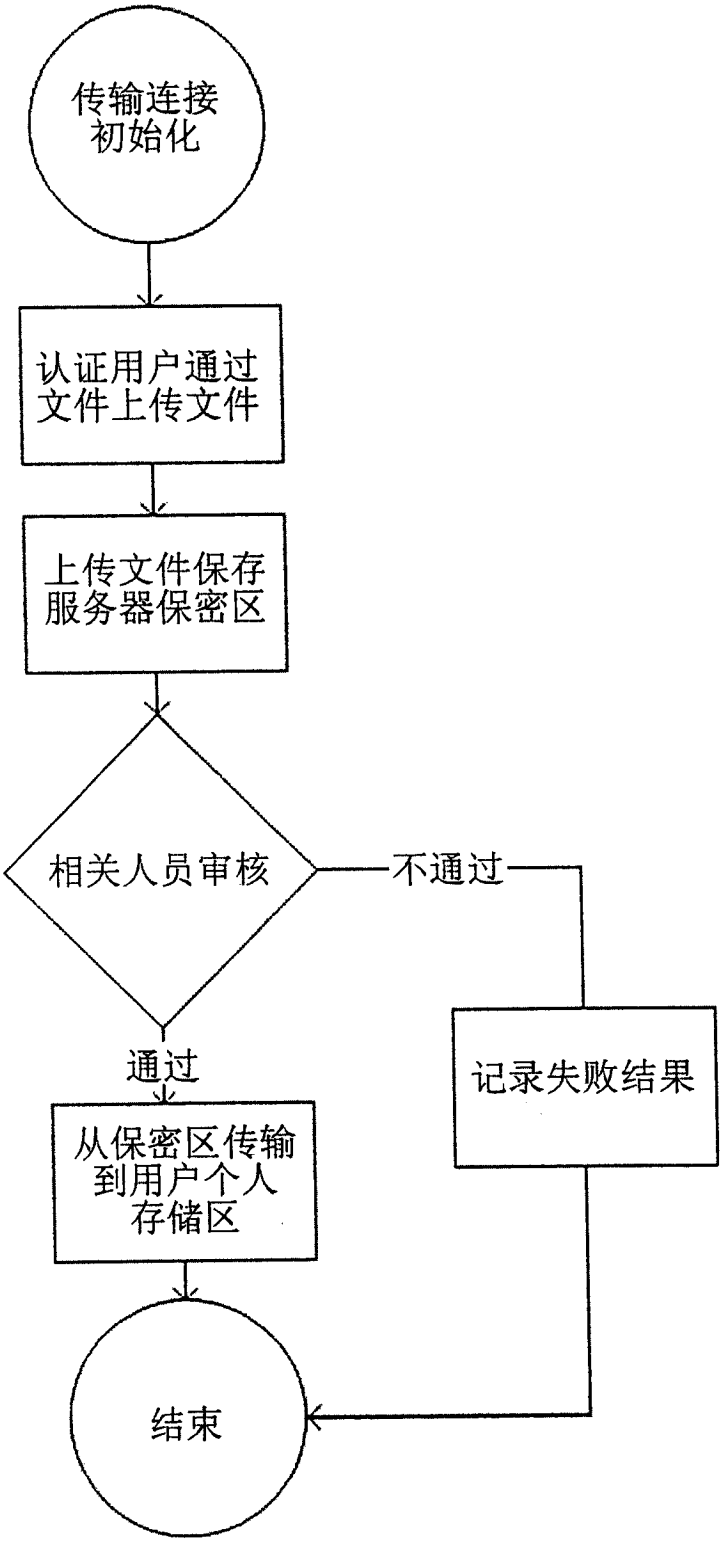

传输连接初始化
认证用户通过文件上传文件
上传文件保存服务器保密区
相关人员审核
不通过
通过
记录失败结果
从保密区传输到用户个人存储区
结束

图 6

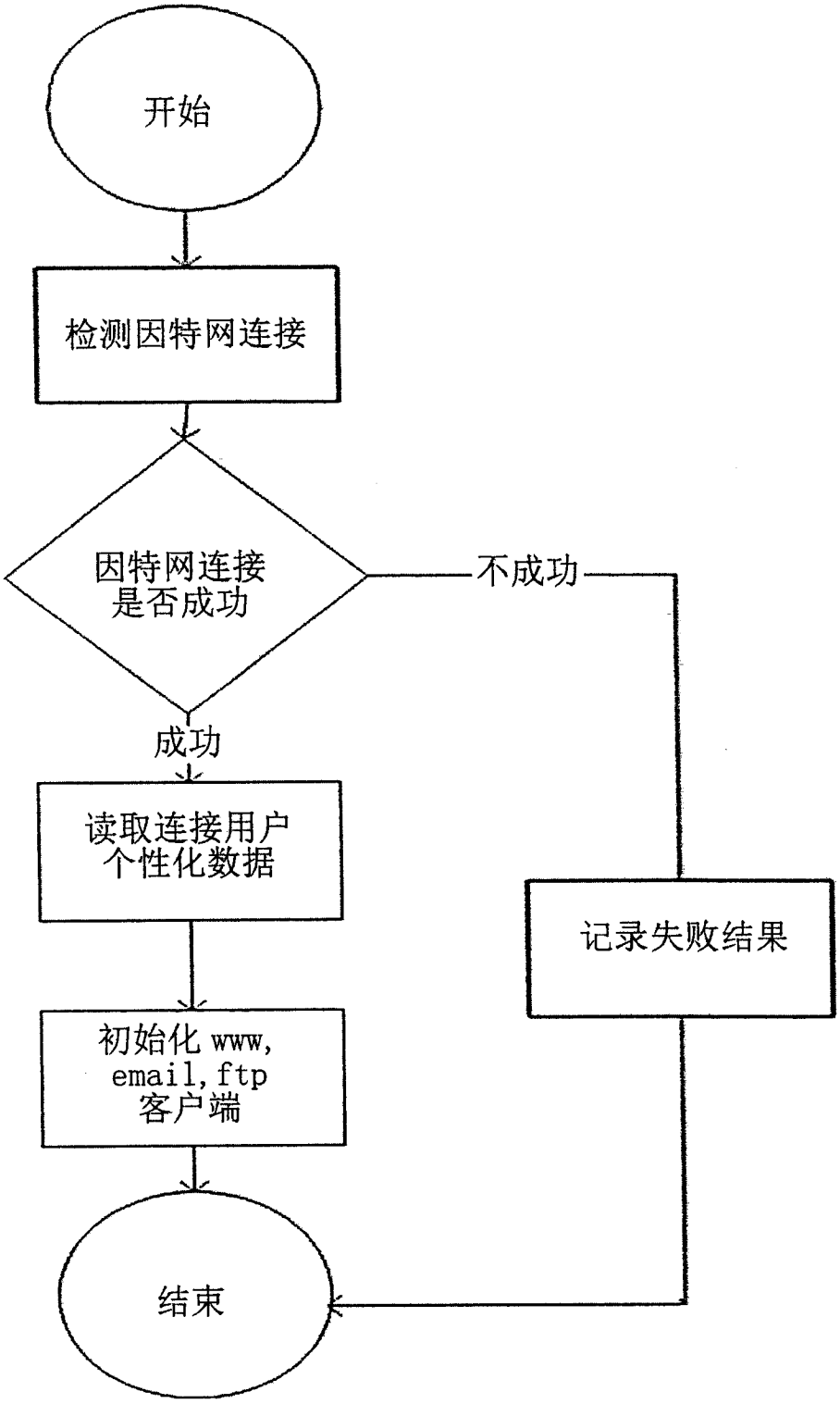

开始
检测因特网连接
因特网连接
是否成功
不成功
成功
读取连接用户
个性化数据
记录失败结果
初始化 www,
email, ftp
客户端
结束

图 7

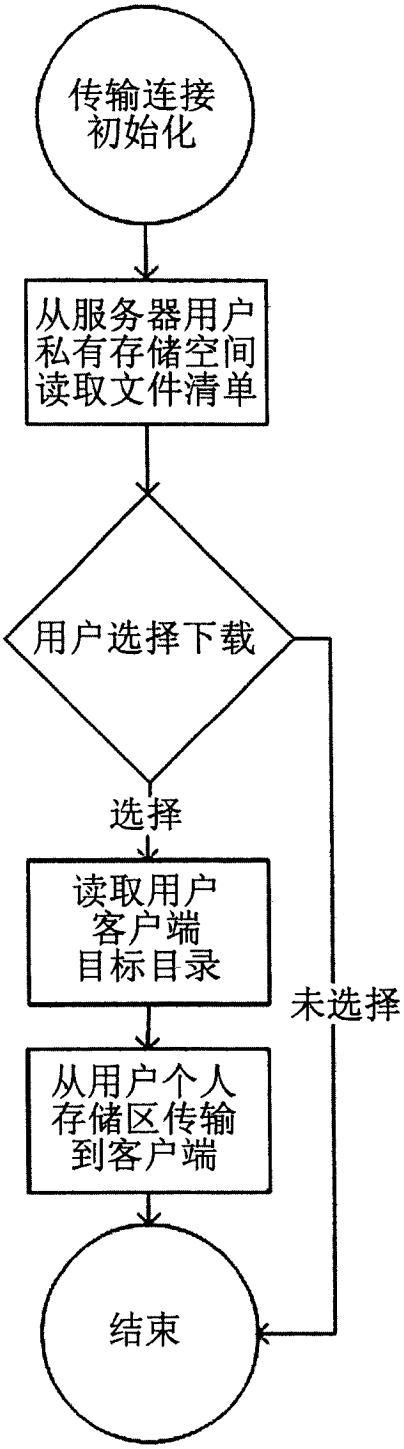

传输连接
初始化
从服务器用户
私有存储空间
读取文件清单
用户选择下载
选择
读取用户
客户端
目标目录
从用户个人
存储区传输
到客户端
结束
未选择

图 8