(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 1846421 B
(45)授权公告日 2012.10.03

(21)申请号 200480024922.0

(22)申请日 2004.06.29

(30)优先权数据
0320057.3 2003.08.28 GB

(85)PCT申请进入国家阶段日
2006.02.28

(86)PCT申请的申请数据
PCT/EP2004/051290 2004.06.29

(87)PCT申请的公布数据
WO2005/022860 EN 2005.03.10

(73)专利权人 摩托罗拉解决方案公司
地址 美国伊利诺伊州

(72)发明人 延斯-克里斯蒂安·约尔根森

(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
代理人 穆德骏 陆锦华

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/26(2006.01)

(56)对比文件
US 6339830 B1,2002.01.15, 全文.
EP 0762707 A2,1997.03.12, 说明书第1栏第34行-第3栏第50行,附图1,摘要.
WO 03/044676 A1,2003.05.30, 全文.
MALKIN G S.Dial-in Virtual Private Networks Using Layer 3 Tunneling.LOCAL COMPUTER NETWORKS,1997. PROCEEDINGS., 22ND ANNUAL CONFERENCE ON MINNEAPOLIS.1997, 第1-3段, 图1-2, 摘要.

审查员 于志辉

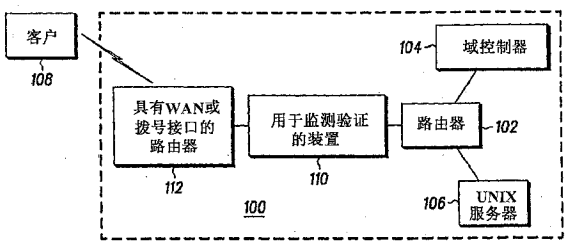
权利要求书 2 页 说明书 3 页 附图 3 页

(54)发明名称

计算机网络安全系统及用于防止计算机网络资源的未授权访问的方法

(57)摘要

一种计算机网络安全系统(100),包括操作地连接以形成计算机网络的网络传输设备(102)、域控制器(104)、至少一个网络资源(106)以及至少一个客户(108),其中,在所述网络传输设备(102)和所述客户(108)之间连接的一种用于对所述域控制器(104)监测所述客户的验证的装置(110)。



CN 1846421 B

1. 一种计算机网络安全系统，包括操作地连接以形成计算机网络的网络传输设备、至少一个网络资源、和控制对于所述至少一个网络资源的访问的域控制器、至少一个客户、以及用于监测所述客户的验证以具有对于所述至少一个网络资源的访问的装置，所述用于监测验证的装置可操作用于将所述客户的请求路由至所述域控制器以由所述域控制器进行验证；并且，如果所述客户的请求被所述域控制器验证，则从所述域控制器接收所述客户的接受，并且经由所述用于监测验证的装置对所述客户开启连接；特征在于：所述域控制器是操作用于控制对于网络域的访问的域控制器，所述网络域包括该域中在不同操作系统控制下操作的网络资源，所述操作系统包括与所述域控制器的操作系统不同的操作系统，并且所述用于监测验证的装置连接在所述网络传输设备和所述客户之间，并且操作用于仅使用在所述用于监测验证的装置和所述客户之间路径上进行的验证机制，并且当所述客户请求访问所述域时，校验由所述客户指示的 IP 目的地地址，并且如果所述 IP 目的地地址是所述域控制器的 IP 目的地地址，则将所述客户的请求路由到所述域控制器以由所述域控制器进行验证。

2. 如权利要求 1 所述的计算机网络安全系统，其中所述用于监测验证的装置包括用于如果所述验证失败、或者在预设时间周期内没有执行所述验证、或者如果所述客户试图连接至所述域中所述客户没有被授权连接的网络资源，则断开所述客户的装置。

3. 如权利要求 2 所述的计算机网络安全系统，其中装备有 WAN 或拨号接口的第二网络传输设备连接在所述客户和所述用于监测验证的装置之间。

4. 如权利要求 3 所述的计算机网络安全系统，其中所述网络传输设备是路由器或者转换器。

5. 如权利要求 4 所述的计算机网络安全系统，其中所述至少一个客户对于所述域远程设置，并且所述系统包括用于监测至少一个其他客户的验证，以具有对于所述域的至少一个资源的访问的第二装置，所述至少一个其他客户本地设置在所述域内。

6. 一种用于防止以上任何一个权利要求所述的网络系统中至少一个网络资源的未授权访问的方法，该方法包括仅使用在所述用于监测验证的装置和所述客户之间路径上的验证机制进行监测的装置，并且当所述客户请求访问所述域时，校验所述客户指示的 IP 目的地地址，如果所述 IP 目的地地址是所述域控制器的 IP 目的地地址，则所述用于监测验证的装置将所述客户的请求路由到所述域控制器以由所述域控制器进行验证；并且，如果所述域控制器验证了所述客户的请求，则所述域控制器将接受数据分组经由所述用于监测验证的装置发送到所述客户；以及，响应于接收到所述接收数据分组，所述用于监测验证的装置对所述客户开启到包括至少一个资源的网络资源的连接，所述资源具有与所述域控制器的操作系统不同的操作系统。

7. 如权利要求 6 所述的方法，还包括所述用于监测验证的装置将关于由所述客户接触的所述网络资源的信息发送到所述域控制器；所述域控制器将关于允许或拒绝访问所述网络资源的信息发送到所述用于监测验证的装置；以及，所述用于监测验证的装置将所述关于允许或拒绝访问的信息转换为动态 IP 分组过滤器。

8. 如权利要求 7 所述的方法，其中，在所述域控制器进行验证之前，所述用于监测验证的装置仅允许到所述域控制器 IP 地址的连接路由。

9. 如权利要求 8 所述的方法，其中针对由所述客户接触的所述网络资源的信息，所述

用于监测验证的装置向所述域控制器发送所述资源的 IP 地址和 UDP/TCP 端口号。

10. 如权利要求 9 所述的方法，其中如果所述验证失败、如果在预设时间周期内没有执行所述验证、或者如果所述客户试图连接到所述客户未被授权连接的网络资源，则所述用于监测验证的装置断开所述客户。

11. 如权利要求 10 所述的方法，其中在所述客户和所述用于监测验证的装置或者在局域网上的接入点之间建立虚拟个人网络通道。

计算机网络安全系统及用于防止计算机网络资源的未授权访问的方法

技术领域

[0001] 本发明通常涉及数据安全系统，具体涉及用于防止网络资源的未授权访问的系统和方法。

背景技术

[0002] 随着计算机网络特别是因特网的到来，连接到这些网络上的计算机客户访问各种资源。这些资源是文档、文件、技术和经济数据以及其它电子内容。从一方面来说，这种对资源的远程或本地访问给了独立于它们的位置而使用这些资源的可能性。从另一方面来说，由于对它们的特性来说，这些资源在大多数情况下是至关重要的，当被未授权的客户访问时，这带来了危险。

[0003] 从技术的角度来看，由在操作系统的控制下的网络服务其提供这些资源。需要访问资源的远程或本地客户向服务器发送请求，作为响应，服务器将资源发送给（给予访问）远程或本地客户。由于大多数资源是有价值的和重要的，仅由授权的远程或本地客户可以访问它们。远程或本地客户的一种验证方法是要求正确输入用户名和密码。只有那些通过了验证的远程或本地客户可以访问资源。用户名－密码方案是使得服务器对特定客户（用户）限制访问的验证机制。

[0004] 然而，经常发生在一个计算机网络中，不同的网络资源在不同的操作系统的控制下工作。在这种情况下问题在于连接到域控制器的远程或本地客户，当他们登陆到由域控制器控制的域上时，如果可户安装不是授权的视窗 (RTM)NT/2000 客户安装，能够旁路域控制器。

[0005] 这将使得未授权的远程或本地客户没有在会话启动时登陆到域控制器而访问网络资源，例如 UNIX(RTM) 服务器，该网络资源没有由视窗 (RTM)NT/2000 域控制器控制验证。

[0006] 本领域中执行远程客户的验证的一个解决方案，即被称为远程访问服务器 (RAS)，可以被安置到远程客户和域控制器之间的通路上。验证阶段之后的 RAS 给予对网络的访问，而不仅仅是域控制器。这意味着在 RAS 已经验证远程客户之后，可以旁路域控制器。然而，从网络安全的角度看，域控制器应验证并授权所有由远程或本地客户启动的会话，以将所有验证过程放置在一个服务器上。

发明内容

[0007] 有对用于防止网络资源的未授权访问的计算计网络安全系统和方法的需求，其避免或克服现有技术中的缺点。

[0008] 根据本发明的第一方面，提供了如权利要求 1 所要求的计算机网络安全系统。

[0009] 根据本发明的第二方面，提供了如权利要求 11 所要求的用于防止计算机网络资源的未验证访问的方法。

[0010] 本发明有利地允许：

[0011] 1. 减小客户和遍历 (traverse) 域控制器的服务器之间的网络业务。

[0012] 2. 应由域控制器验证的连接到域控制器位置的远程或本地客户，与域控制器位置相比，可以位于任何位置。

附图说明

[0013] 从下面结合附图对试实例的详细说明中，可以更加完全地理解和评价本发明，其中：

[0014] 图 1 是在本发明的一个实施例中的计算机网络安全系统的框图，

[0015] 图 2 是在本发明的第二实施例中的计算机网络安全系统的框图，

[0016] 图 3 是在本发明的第三实施例中的计算机网络安全系统的框图，

[0017] 图 4 是说明在本发明的一个实施例中的用于防止计算机网络资源的未授权访问的方法的流程图。

具体实施方式

[0018] 参照图 1，说明了根据发明的计算机网络安全系统 100 的一个实施例。计算机网络系统 100 包括网络传输设备 102，其负责将数据分组指引到它们的目的地 IP 地址。在一个实施例中，所述网络传输设备 102 可以是路由器，在另一个实施例中它可以是转换器。所述网络传输设备连接到域控制器 (也称为 DC) 104 以及连接到 UNIX(RTM) 服务器 106。客户 108 操作地连接到用于监测验证 (authentication) 的装置 110，该用于监测验证的装置 110 连接到所述网络传输设备 102。如果所述客户 108 位于远离由所述域控制器 104 控制的域，则所述客户 1 经由具有 WAN 或拨号接口的路由器连接到用于监测验证的装置 110。

[0019] 参照图 2 和 3，说明了所述计算机网络安全系统的另一个实施例。如果至少一个客户位于由所述域控制器控制的域内 (本地客户 218)，以及至少一个用户位于远程 (远程客户 202)，所述本地客户 218 经由转换器或集线器 220 连接到用于监测验证的第二装置 216，以及所述远程客户经由具有 WAN 或拨号接口 112 的路由器连接到用于监测验证的第一装置 206。或者，如果在域中共享仅一个用于监测验证的装置，具有 WAN 或拨号接口 112 的所述路由器连接到转换器或所述集线器 220。

[0020] 如果所述域控制器 104 和所述 UNIX(RTM) 服务器 106 在不同的操作系统的控制下工作，那么所述域控制器 104 不对所述 UNIX(RTM) 服务器 106 的访问进行验证控制。当客户 108 在域控制器 104 的控制下，对在域中的服务器 108 或主机开始会话时，基于目的地 IP 地址，由用于监测验证的装置将所述客户 108 定向到所述域控制器 104。在对所述域中的网络资源的访问被允许或拒绝之前，所述域控制器 104 验证所述客户 108。在验证之前，用于监测验证的所述装置 110 仅允许与所述域控制器 104 连接。

[0021] 参照图 4，在一个实施例中示出了用于防止计算机网络资源的未授权访问的方法。在图 4 中，将用于监测验证的所述装置指代为“AM”。在会话开始时，所述客户 108 向由所述域控制器 104 控制的所述域请求验证 402。

[0022] 所述用于监测验证的装置 110 校验所述客户 108 的 IP 目的地地址 404，以防止访问没有验证控制的网络资源。只有那些 IP 目的地地址是所述域控制器 406 的 IP 目的地地址的客户被路由到所述域控制器 104 来验证。如果在验证之前所述客户 108 的目的地 IP

地址不是所述域控制器 104 的目的地 IP 地址，所述用于监测验证的装置 110 改变所述目的地 IP 地址并仅允许路由到所述域控制器 104。

[0023] 验证过程可以基于所述客户 108 和所述域控制器 104 之间达成的加密机制。如果所述客户被验证 410，将接受 (acceptance) 分组从所述域控制器 104 经由所述用于监测验证的装置 110 发送到所述客户 108。基于该信息，所述用于监测验证的装置 110 对所述客户开启 414 到所述域内的网络资源的连接。结果，所述会话的通路不限于域控制器 104 和客户 108 之间的通路，而且在所述会话期间所述客户 108 可以接触其他服务器 106 和 214。所述用于监测验证的装置 110 基于该会话的加密算法和密钥来记录会话。基于加密并由所述用于监测验证的装置 110 所使用的验证机制仅在所述用于监测验证的装置 110 和所述客户 108 之间的通路上出现。这是因为客户 108 访问的例如 UNIX(RTM) 服务器和其它网络设备在适当的地方可能不具有加密机制。

[0024] 如果所述验证失败或者在预设时间周期内没有被执行，所述用于监测验证的装置 110 断开 422 所述客户 108。

[0025] 为了保持对连接到域的客户进行控制，所述用于监测验证的装置 110 将关于由所述客户接触的所述网络资源的信息发送 416 到所述域控制器 104。所述用于监测验证的装置 110 收集由所述客户 108 接触的 IP 地址和 UDP/TCP 端口号，并将该信息发送 416 到所述域控制器 104。作为响应，所述域控制器 104 将关于允许或拒绝访问所述网络资源的信息发送 418 到所述用于监测验证的装置 110。所述用于监测验证的装置将所述关于允许或拒绝访问的信息转换为动态 IP 分组过滤器。如果所述用户试图连接到所述客户未被授权的网络资源，所述用于监测验证的装置 110 断开所述用户 108。

[0026] 只要在验证期间开始的会话是有效的，保持对所述网络资源 214 的访问。所述用于监测验证的装置 110 基于所述客户 108 的源 IP 地址和加密机制来确定该会话是否属于所述客户 108。

[0027] 为提供计算机网络的安全，由在所述域控制器 104 和客户中已经实现的特性来执行在验证期间所使用的客户 108 的密码的标准加密。在域控制器在视窗 (RTM)NT/2000 下运行的情况下，在客户和域控制器之间发生加密机制，使得运行过程可信。即，为不是正确客户的客户复制该过程是非常困难的。

[0028] 为加密在所述客户 108 和所述网络资源之间的会话，其不被所述域控制器 104 控制，使用虚拟个人网络通道。在所述客户 108 和所述用于监测验证的装置 110 或者例如具有 WAN 接口 112 的路由器的局域网上的接入点之间建立所述虚拟个人网络通道。

[0029] 在一个实施例中，以可以在所述网络传输设备 102(例如，路由器) 上执行的软件来实现所述用于监测验证的装置 110。软件实现相对低成本并允许简单的重新配置。然而硬件实现也是可以的。然而，应理解本发明可以被实现为硬件或软件并用于计算机网络中。

[0030] 值得强调，本发明的实施例允许试图访问在一个域中在不同操作系统下控制的网络资源的客户的验证。此外，所有验证过程和所有关于由所述客户接触的网络资源的信息放置在一个服务器上。

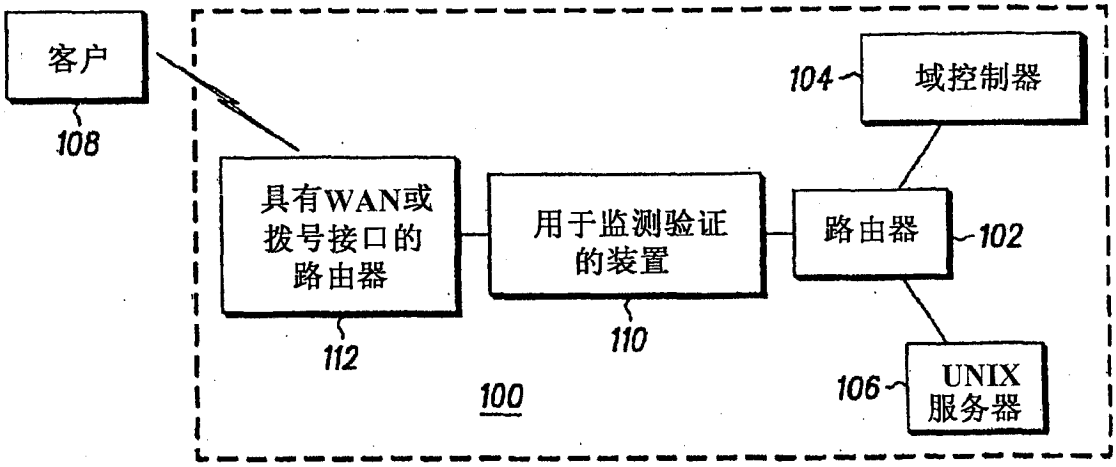

客户
108
104
域控制器
具有WAN或
拨号接口的
路由器
112
用于监测验证
的装置
110
路由器
102
100
106
UNIX
服务器

图 1

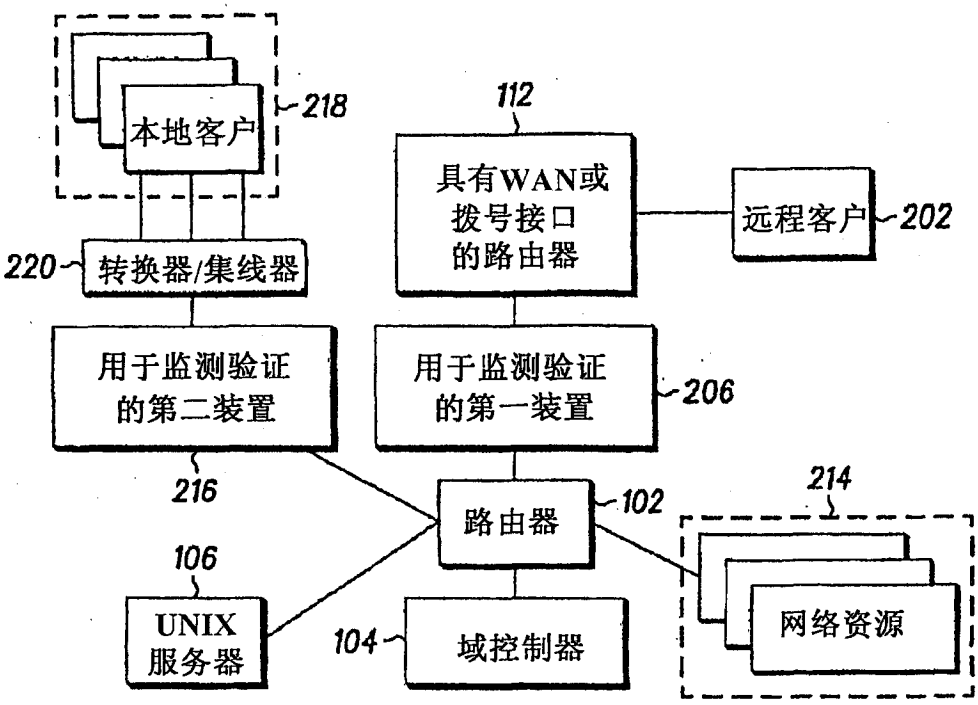

218
本地客户
112
具有WAN或
拨号接口
的路由器
远程客户
202
220
转换器/集线器
用于监测验证
的第二装置
用于监测验证
的第一装置
206
216
路由器
102
214
106
UNIX
服务器
104
域控制器
网络资源

图 2

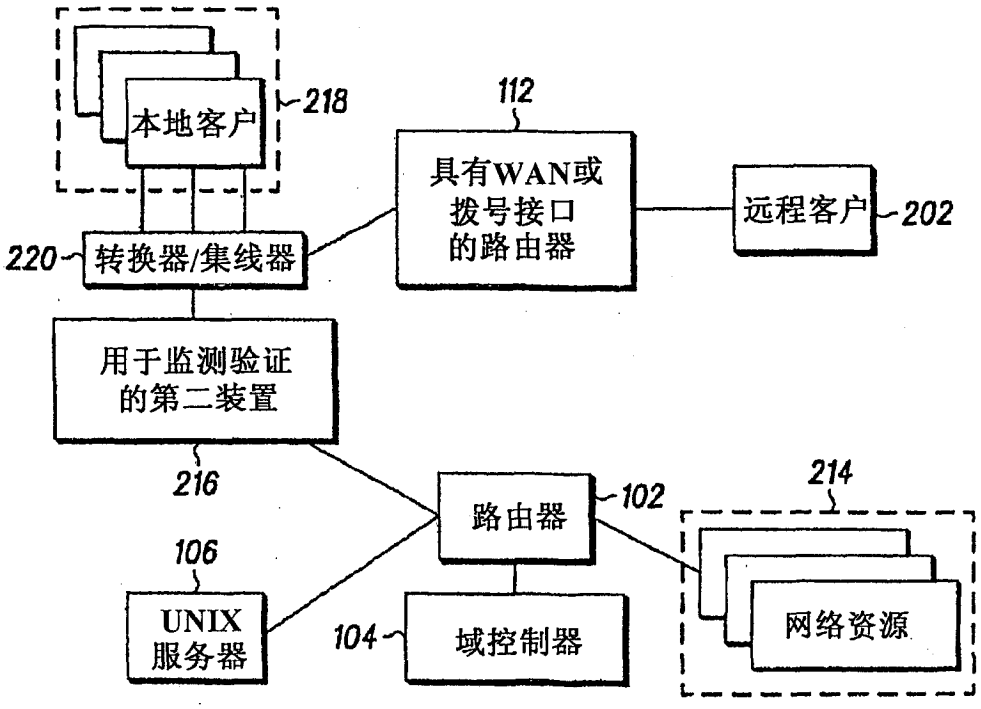

本地客户
218
112
具有WAN或
拨号接口
的路由器
远程客户
202
220
转换器/集线器
用于监测验证
的第二装置
216
路由器
102
214
106
UNIX
服务器
104
域控制器
网络资源

图 3

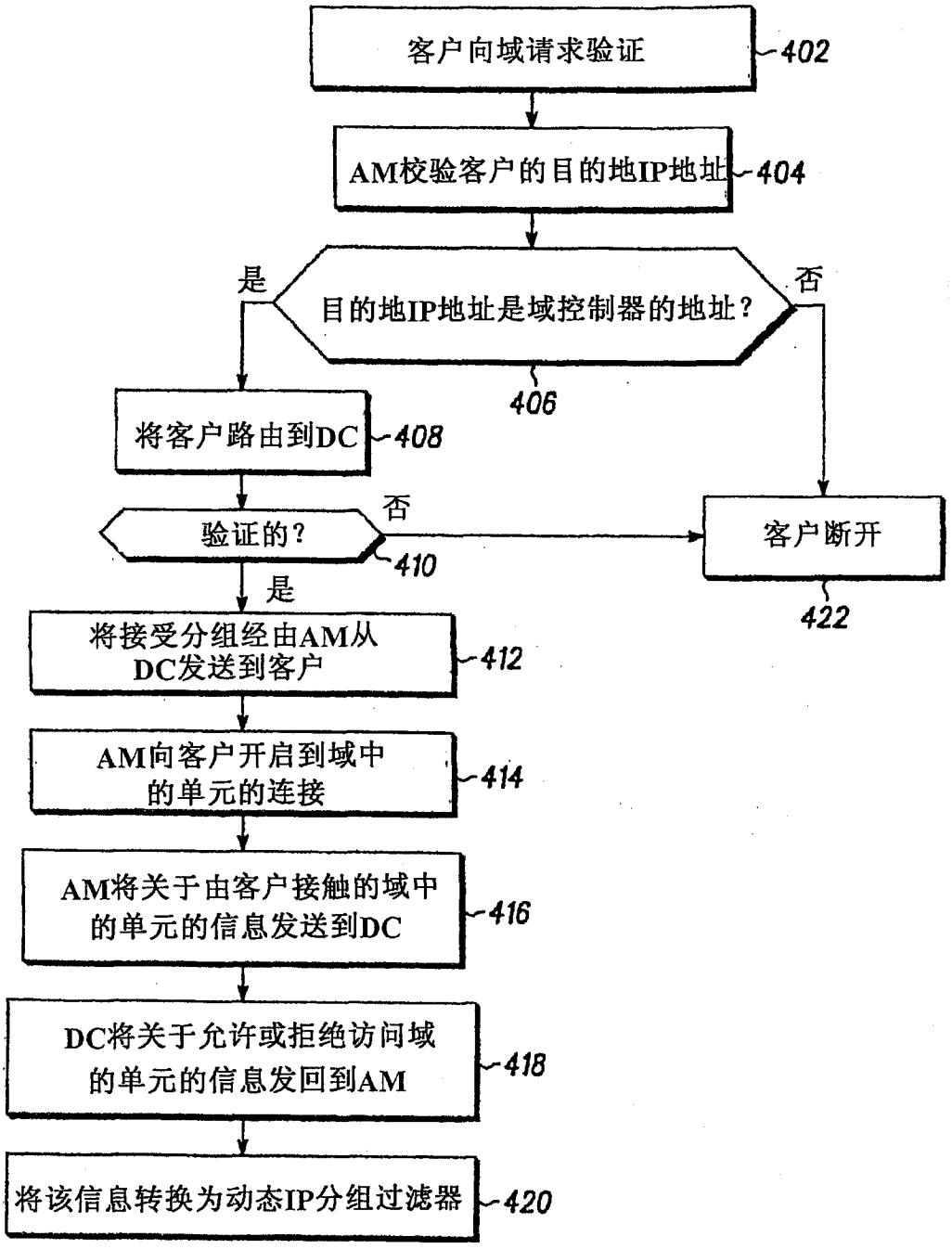

客户向域请求验证
402
AM校验客户的目的地IP地址
404
是
目的地IP地址是域控制器的地址？
否
406
将客户路由到DC
408
验证的？
否
410
客户断开
422
是
将接受分组经由AM从DC发送到客户
412
AM向客户开启到域中的单元的连接
414
AM将关于由客户接触的域中的单元的信息发送到DC
416
DC将关于允许或拒绝访问域的单元的信息发回到AM
418
将该信息转换为动态IP分组过滤器
420

图 4