[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/32

[12] 发明专利申请公开说明书

[21] 申请号 200410063244.0

[43] 公开日 2005 年 2 月 9 日

[11] 公开号 CN 1578218A

[22] 申请日 2004.6.30
[21] 申请号 200410063244.0
[30] 优先权
[32] 2003.6.30 [33] US [31] 10/611,832
[71] 申请人 微软公司
地址 美国华盛顿州
[72] 发明人 A·谢勒斯特 C·惠特马

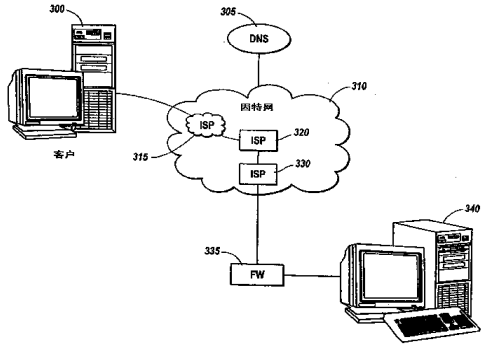
[74] 专利代理机构 上海专利商标事务所
代理人 谢喜堂

权利要求书 7 页 说明书 14 页 附图 5 页

[54] 发明名称 用透明虚拟专用网络减少网络配置复杂性

[57] 摘要

防火墙通过启动未经请求的要客户提供认证凭证的要求而起到专用网络内的服务器的透明网关的作用。 在接收到客户凭证后，防火墙会验证认证凭证并为访问服务器建立安全通道。 可以利用安全通道把从客户发往服务器的数据通过防火墙转发。 防火墙可签署或以其它方式表明：转发到服务器的数据是来自防火墙已认证的客户。 防火墙也可以向客户提供一定级别的认证。 当与服务器连接时，客户可以访问专用网络外部的其它服务器，而不会有与其它服务器相关的数据穿过专用网络。 防火墙减少了客户为访问各种专用网络服务器而必须保持的配置信息。



ISSN1008-4274

1．在包括资源与防火墙的专用网络中，该防火墙通过控制客户对专用网络资源的期望访问而起到网关的作用，一种与专用网络资源建立连接而同时平衡客户与防火墙之间的认证处理要求以共同防卫拒绝服务攻击的方法，其特征在于，拒绝服务，所述方法包括以下动作：

由防火墙接收来自客户的要访问专用网络资源的请求，其中来自客户的所述请求是向专用网络资源作出而对防火墙无任何了解；

由防火墙请求客户提供一个或多个客户凭证以认证客户；

由防火墙发送一个或多个防火墙凭证以认证防火墙，其中产生所述一个或多个防火墙凭证会消耗一定水平的有限的防火墙处理资源；

在防火墙处接收一个或多个客户凭证，其中产生所述一个或多个客户凭证会消耗在数量上与有限的防火墙处理资源的消耗类似的一定水平的有限的客户处理资源；

由防火墙验证所述一个或更多客户凭证；

建立用于访问所述专用网络资源的安全通道，以响应对所述一个或多个客户凭证的验证；以及

利用所述安全通道，经由所述防火墙转发来自客户去往专用网络资源的数据。

2．如权利要求 1 所述的方法，其特征在于，所述验证步骤包括以下动作：

在客户与防火墙之间继续交换凭证，以递增客户与防火墙之间的信任级别，直到达到预定的信任限度。

3．如权利要求 1 所述的方法，其特征在于，所述专用网络资源为主机、网关或服务器之一。

4．如权利要求 1 所述的方法，其特征在于，从客户穿过防火墙的唯一数据是发往专用网络资源的数据包。

5．如权利要求 1 所述的方法，其特征在于，还包括以下动作：

在维持所述专用网络的安全通道的同时，建立与另外的专用网络的资源的连接。

6. 如权利要求 1 所述的方法，其特征在于，还包括以下动作：

在维持与所述专用网络的资源的安全通道的同时，建立与另一专用网络资源的连接。

7. 如权利要求 1 所述的方法，其特征在于，向专用网络资源转发来自客户的数据的动作是通过使用已认证通道来完成，所述方法还包括以下动作：

由防火墙签署从客户发往专用网络资源的数据包，其中所述签署表明客户已经通过在防火墙中执行的一个或多个安全检查。

8. 如权利要求 7 所述的方法，其特征在于，还包括以下行为：

丢弃由受保护的专用网络资源接收到的未经签署的数据包。

9. 如权利要求 1 所述的方法，其特征在于，所接收的一个或多个客户凭证是选自以下项的至少一项：用户名称、客户 IP 地址、密码、通行证、智能卡或信用卡号。

10. 如权利要求 1 所述的方法，其特征在于，防火墙让客户提供一个或多个客户凭证的请求为一问题，并且其中，所接收的一个或多个客户凭证为所述问题的答案。

11. 如权利要求 1 所述的方法，其特征在于，客户为第二防火墙。

12. 在包括资源与防火墙的专用网络中，防火墙通过控制客户对专用网络资源的期望访问而起到网关的作用，一种与专用网络资源建立连接而同时平衡客户与防火墙之间的认证处理要求以共同防卫拒绝服务攻击的方法，其特征在于，拒绝服务所述方法包括以下步骤：

开始一系列设计用于在请求访问专用网络资源的客户上和作为所述专用网络网关来操作的防火墙上施加相称的处理负担的认证事务，其中客户最初并不知道防火墙是作为所述专用网络的网关在操作，并且每一认证事务会递增客户与防火墙之间的信任级别，直到客户与防火墙的认证得到充分验证；

对于所述系列认证事务的每一认证事务：

根据所述系列认证事务之一向客户认证；以及

要求客户以要求类似处理负担的一种方式来认证；以及

在所述系列认证事务结束后，准许客户通过防火墙来访问所述专用网络资源。

13. 如权利要求 12 所述的方法，其特征在于，要求客户进行认证的步骤包括以下动作：

由防火墙请求客户提供一个或多个客户凭证；

在防火墙处接收一个或多个客户凭证；以及

由防火墙验证所述一个或多个客户凭证。

14. 如权利要求 13 所述的方法，其特征在于，所认证的一个或多个凭证是以下项中至少一项：用户名称、客户 IP 地址、密码、通行证、智能卡或信用卡号。

15. 如权利要求 13 所述的方法，其特征在于，防火墙让客户提供一个或多个客户凭证的请求为一问题，并且其中，所接收的一个或多个客户凭证为所述问题的答案。

16. 如权利要求 12 所述的方法，其特征在于，一旦客户被准许访问所述专用网络资源，则来自客户而穿过防火墙的唯一数据是发往专用网络资源的数据包。

17. 如权利要求 12 所述的方法，其特征在于，所述准许步骤包括以下动作：

在防火墙与专用网络资源之间建立已认证通道，其中所述已认证通道是通过签署来自防火墙的数据而建立。

18. 如权利要求 17 所述的方法，其特征在于，还包括以下动作：

丢弃由专用网络资源所接收的任何未经签署的数据包。

19. 如权利要求 12 所述的方法，其特征在于，所述专用网络资源为主机、网关或服务器之一。

20. 如权利要求 12 所述的方法，其特征在于，所述客户为第二防火墙。

21. 如权利要求 12 所述的方法，其特征在于，还包括以下动作：

在维持防火墙与客户之间的安全通道的同时，建立与一单独专用网络的另一资源的连接。

22. 如权利要求 12 所述的方法，其特征在于，还包括以下动作：

在维持防火墙与客户之间的安全通道的同时，建立与另一专用网络资源的连接。

23. 在包括资源与防火墙的专用网络中，其中防火墙通过控制客户对专用网络资源的期望访问而起到网关的作用，一种含有计算机可执行指令的计算机可读媒质，其特征在于，拒绝服务所述指令可执行与专用网络资源建立连接而同

时平衡客户与防火墙之间的认证处理要求以共同防卫拒绝服务攻击的方法，所述方法包括以下动作：

由防火墙接收来自客户的访问专用网络资源的请求，其中来自客户的请求是向专用网络资源作出而对防火墙无有任何了解；

由防火墙请求客户提供一个或多个客户凭证以认证客户；

由防火墙发送一个或多个防火墙凭证以认证防火墙，其中产生一个或个多防火墙凭证会消耗一定水平的有限的防火墙处理资源；

在防火墙处接收一个或多个客户凭证，其中产生一个或多个客户凭证会消耗在数量上与有限的防火墙处理资源的消耗类似的一定水平的有限的客户处理资源；

由防火墙验证所述一个或多个客户凭证；

响应对所述一个或多个客户凭证的验证，建立用于访问所述专用网络资源的安全通道；以及

利用所述安全通道，经由防火墙转发来自客户去往专用网络资源的数据。

24. 如权利要求 23 所述的方法，其特征在于，所述验证步骤包括以下动作：

在客户与防火墙之间继续交换凭证，以递增客户与防火墙之间的信任级别，直到达到预定的信任限度。

25. 如权利要求 23 所述的方法，其特征在于，所述专用网络资源为主机、网关或服务器之一。

26. 如权利要求 23 所述的方法，其特征在于，来自客户而穿过防火墙的唯一数据为发往专用网络资源的数据包。

27. 如权利要求 23 所述的方法，其特征在于，还包括以下动作：

在维持所述专用网络的安全通道的同时，建立与单独专用网络的资源的连接。

28. 如权利要求 23 所述的方法，其特征在于，还包括以下动作：

在维持所述专用网络的安全通道的同时，建立与另一专用网络资源的连接。

29. 如权利要求 23 所述的方法，其特征在于，向专用网络资源转发来自客户的数据的动作是通过使用已认证通道来完成，所述方法还包括以下动作：

由防火墙签署从客户发往专用网络资源的数据包，其中所述签署表明客户已经通过在防火墙中执行的一个或多个安全检查。

30. 如权利要求 29 所述的方法，其特征在于，还包括以下行为：

丢弃由受保护的专用网络资源接收到的未经签署的数据包。

31. 如权利要求 23 所述的方法，其特征在于，所接收的一个或多个客户凭证选自以下项中至少一项：用户名称、客户 IP 地址、密码、通行证、智能卡或信用卡号。

32. 如权利要求 23 所述的方法，其特征在于，所述防火墙让客户提供一个或个多客户凭证的请求为一问题，并且其中，所接收的一个或多个客户凭证为所述问题的答案。

33. 如权利要求 23 所述的方法，其特征在于，所述客户为第二防火墙。

34. 在包括资源与防火墙的专用网络中，其中防火墙通过控制客户对专用网络资源的期望访问而起到网关的作用，一种含有计算机可执行指令的计算机可读媒质，其特征在于，拒绝服务所述指令可执行与专用网络资源建立连接而同时平衡客户与防火墙之间的认证处理要求以共同防卫拒绝服务攻击的方法，所述方法包括以下步骤：

开始一系列设计用于在请求访问专用网络资源的客户上和作为所述专用网络网关来操作的防火墙上施加相称的处理负担的认证事务，其中客户最初并不知道防火墙是作为所述专用网络的网关在操作，并且每一认证事务会逐渐增加客户与防火墙之间的信任级别，直到客户与防火墙的认证得到充分验证；

对于所述系列认证事务的每一认证事务：

根据所述系列认证事务之一向客户认证；以及

要求客户以要求类似处理负担的一种方式来认证；以及

在所述系列认证事务结束后，准许客户通过防火墙来访问专用网络资源。

35. 如权利要求 34 所述的方法，其特征在于，要求客户进行认证的步骤包括以下动作：

由防火墙请求客户提供一个或多个客户凭证；

在防火墙处接收所述一个或多个客户凭证；以及

由防火墙验证所述一个或多个客户凭证。

36. 如权利要求 35 所述的方法，其特征在于，所认证的一个或多个凭证为以下项中的至少一项：用户名称、客户 IP 地址、密码、通行证、智能卡或信用卡号。

37. 如权利要求 35 所述的方法，其特征在于，所述防火墙让客户提供一个或多个客户凭证的请求为一问题，并且其中，所接收的一个或多个客户凭证为所述问题的答案。

38. 如权利要求 35 所述的方法，其特征在于，一旦客户被准许访问所述专用网络资源，则来自客户而穿过防火墙的唯一数据为发往专用网络资源的数据包。

39. 如权利要求 34 所述的方法，其特征在于，所述准许步骤包括以下动作：

在防火墙与专用网络资源之间建立已认证通道，其中所述已认证通道是通过签署来自防火墙的数据而建立。

40. 如权利要求 39 所述的方法，其特征在于，还包括以下动作：

丢弃由专用网络资源接收到的任何未经签署的数据包。

41. 如权利要求 34 所述的方法，其特征在于，所述专用网络资源为主机、网关或服务器之一。

42. 如权利要求 34 所述的方法，其特征在于，所述客户为第二防火墙。

43. 如权利要求 34 所述的方法，其特征在于，还包括以下动作：

在维持所述防火墙与所述客户之间的安全通道的同时，建立与一单独专用网络的另一资源的连接。

44. 如权利要求 34 所述的方法，其特征在于，还包括以下动作：

在维持所述防火墙与所述客户之间的安全通道的同时，建立与另一专用网络资源的连接。

45. 在包括服务器与防火墙的专用网络中，其中防火墙通过控制对服务器的访问而起到网关的作用，一种提供穿过防火墙访问服务器而客户无需了解防火墙的方法，其特征在于，，所述方法包括以下动作：

在防火墙处接收来自客户的访问请求，因为客户并不知道防火墙是作为所述服务器的一网关在操作，故所述请求被引导至服务器；

在防火墙处产生一个或多个认证凭证，该凭证表明服务器与防火墙之间的信任级别；

防火墙发送要客户向防火墙认证的请求，所述请求包括所述一个或多个防火墙认证凭证，以便客户知道服务器与防火墙之间的信任级别而不必单独请求；

在防火墙处接收来自客户的所述一个或多个认证凭证；

防火墙验证所述一个或多个认证凭证；以及

随后，使客户能够通过防火墙来访问服务器。

46. 如权利要求 45 所述的方法，其特征在于，还包括以下动作：

在防火墙与服务器之间建立安全连接；以及

把从客户处接收的数据通过安全连接转发到服务器。

47. 如权利要求 45 所述的方法，其特征在于，还包括以下动作：

在防火墙处接收来自客户的数据；

防火墙签署所接收的数据；以及

防火墙把已签署的数据转发到服务器。

48. 如权利要求 45 所述的方法，其特征在于，所述服务器包括主机或网关。

49. 如权利要求 45 所述的方法，其特征在于，所述客户包括另一防火墙。

50. 如权利要求 45 所述的方法，其特征在于，所述客户维持与另一服务器的单独连接，并且其中只有前往专用网络的数据会穿过防火墙。

51. 如权利要求 50 所述的方法，其特征在于，所述另一服务器为一单独且完全不同的虚拟专用网络的一部分。

用透明虚拟专用网络减少网络配置复杂性

技术领域

本发明一般涉及虚拟专用网络（VPN），尤其涉及访问 VPN 的有效方式。

发明背景

VPN 是对广域网（WAN）的有吸引力的成本效益型替代。就其根本而言，VPN 使远程站点或客户能够通过公共网络（通常为因特网）与专用网络连接。一旦连接，远程站点或客户即作为专用网络的本地部分、从而作为指定虚拟专用网络而出现。设计良好的 VPN 会使一个公司受益匪浅。例如，它能延伸地理连通性、改善安全性、相对传统 WAN 减少操作成本、为远程客户减少通行时间及传输成本、改善生产率、简化网络布局，并能提供全球联网机会。

普通类型的 VPN 系统有两种：远程访问型及站点至站点型。远程访问，也称为虚拟专用拨号网络（VPDN），是一种客户－局域网（LAN）连接，如果公司中有员工需要从各种远程位置与专用网络连接会使用这种方式。远程访问 VPN 允许公司的专用网络与远程客户之间采用安全、加密的连接，这种连接常常通过第三方服务提供商来实现。站点至站点 VPN 使用了专用设备及大规模加密，通过诸如因特网的公共网络来连接多个站点。站点至站点 VPN 可以以企业内部互联网或外部互联网为基础。不论 VPN 为何种类型，设计良好的 VPN 会集安全性、可靠性、可扩展性、网络管理及政策管理为一体。

VPN 使用几种方法来保障连接和数据安全。这通常会涉及某种类型的加密或防火墙，或两者兼具。加密是获取一台计算机向另一台计算机发送的数据，并把数据编码成一种只能被另一台计算机所解码的形式的过程。典型的计算机加密系统属于以下两类之一：对称密钥加密或公共密钥加密。在对称密钥加密中，每一台计算机具有一密码，用于在通过网络把信息包发送到另一台计算机之前对信息包进行加密。为了对消息进行解码，接收已加密信息包的计算机也必须知道该密码。

公共密钥加密利用了专用密钥与公共密钥的结合。专用密钥会被保密，而公共密钥一般可以为任何请求者所获得。专用密钥与公共密钥的关系是一方解密由另一方加密的数据。因而，可以使用公共密钥解密的数据表明是相应专用密钥的持有者对该数据进行了加密，并因此把相应专用密钥的持有者标识为加密数据的来源。与此类似，通过用公共密钥加密数据，发送者能保证只有专用密钥持有者能解码该数据。

公共密钥加密的常见用处涉及安全套接层（SSL）。SSL 为因特网浏览器和网络服务器使用的因特网安全协议，用于传输敏感信息。SSL 采用安全同步信息交换在 TCP/IP 连接上开始安全会话。在同步信息交换过程中，用于确定对称加密/解密密钥的信息会采用公共密钥加密来交换。此同步交换使客户与服务器之间就其将采用的安全级别达成一致。同步交换结束后，SSL 会加密和解密所采用应用协议例如：http、nntp、telnet 等的字节流。这意味着 http 请求和回答中的所有信息均已完全加密，包括：URL、客户请求、所有已提交的表格内容（如信用卡号）、任何 http 访问授权信息（如客户名称与密码）和所有从服务器发送到客户的数据。SSL 和诸如传输层安全（TLS）等的其它协议是在较高的网络协议层中操作。

另一种形式的 VPN 安全性被称为因特网协议安全性（IPSec）。当与诸如因特网密钥交换（IKE）的密钥协商技术组合时，IPSec 会提供已提高的安全性特征，如：对安全的非 TCP 通信量更广泛的认证能力。因此，只有适应 IPSec 的系统可以利用此协议。与 SSL 和 TLS 不同，IPSec 可以在较低的网络协议层中操作。

当然，VPN 并不适合所有类型的网络访问。例如，对公共网站的访问、传递因特网电子邮件和其它类型的访问等预期是发源于专用网络外部，并且不需要认证。因此为了正常操作，需要支持一定类型的外部和未经认证的访问。然而，允许外部访问专用网络会带来多种安全性风险。

防火墙会在专用网络与另一网络（如因特网）之间提供强大的屏障，这些网络通常会处于不同信任域以内。为应对由外部访问带来的安全性风险，防火墙可对开放端口的数量、所通过的信息包的类型及允许的协议进行限制。

防火墙可以是软件和/或硬件的组合，它可以过滤掉通过外部网络连接进入专用网络或计算机系统的信息。若过滤器对一输入信息包进行标记，则不允许此信息包通过。典型的防火墙使用三种技术中的一种或多种来控制通信流进出网络，

这些技术包括：静态信息包过滤、代理服务和/或动态信息包过滤。静态信息包过滤，顾名思义，会利用一组过滤器来分析成块的数据。通过过滤器的信息包会被适当发送，而所有其它信息包会被丢弃。若使用代理服务，则防火墙会检索来自网络的信息，并随后发送至请求系统，反之亦然。一种更新的技术称为动态信息包过滤，它并不检查每一个信息包的内容，而是把信息包的某些关键部分与受信任信息的数据库进行比较。它会监控从防火墙内部向外部传输的信息的特殊定义特征。随后把输入信息与这些特征进行比较。若此比较产生合理的匹配，则信息能够通过。否则会被丢弃。

虽然 VPN 是对 WAN 的有吸引力的替代，但目前使用 VPN 服务器进行远程访问存在各种缺点。例如，如果客户希望通过 VPN 连接至 web 网和专用网络，那么所有网络通信量必须经过 VPN。然而，这会造成效率、保密兼容性等问题。之所以造成效率问题，是因为该连接必须首先经过专用网络，随后返回至 web 网。因而，多余的通信量会通过专用网络发送。亦造成保密问题，因为此 web 网冲浪可能违背网络政策。然而，即使因特网上存在高效并保密地支持此类应用的连接，但由于所有数据均通过与 VPN 连接的网络的防火墙转发，故此连接不会被使用，从而还造成连通性问题。

目前的 VPN 使用也常常造成多重网关，每一网关均用于分开的网络。多重 VPN 网关可能削弱安全性，并且也可能造成连通性问题。例如，由于 VPN 客户似乎是从本地连接至 VPN，故该客户不能立即参与多重 VPN 连接。因此，如果客户希望从一网络向一单独的网络下载信息，那么客户必须首先与第一 VPN 服务器建立连接；向客户存储器下载信息；断开与第一 VPN 服务器的连接；与第二 VPN 网络建立 VPN 连接；并随后从客户存储器向第二网络服务器下载信息。这会造成极低的时间及内存管理效率。

目前的 VPN 系统的另一缺点为：跟踪专用网络内部各种 VPN 网关的复杂性。它要求客户知道每一 VPN 网关一定的配置信息，如 IP 地址、认证信息等等。此外，客户可能不知道或可能不能直观判断：必须使用哪一个 VPN 网关来访问专用网络内部的特定服务器。由于 LAN 配置改变，客户可能需要及时更新设置，以便于继续访问 VPN。

因此，需要透明的 VPN，它会使客户能够访问网络而不一定要求由客户请求或发送的所有信息必须经过该网络。此外，还需要能够同时访问不止一个网络，并简化对专用网络的访问而不会削弱安全性需要。

发明内容

根据本发明的示范性实施例，可以克服目前 VPN 的以上已证实的不足之处和缺点。例如，示范性实施例提供了一种包括资源及防火墙的专用网络。该防火墙通过控制客户对专用网络资源的期望访问而起到网关的作用。拒绝服务本发明提供一种用于建立与专用网络资源的连接而同时平衡客户与防火墙之间的认证处理要求以共同防卫拒绝服务攻击（denial of service attack）的计算机程序产品和方法。

该计算机程序产品和方法提供用于由防火墙来接收来自客户的要访问专用网络资源的请求。来自客户的请求是在对防火墙却无任何了解的情况下向专用网络资源作出的。防火墙随后可请求客户提供客户凭证以认证客户。再者，防火墙可向客户发送其自身的凭证，使客户认证自己。防火墙也可接收客户凭证。

产生防火墙凭证及客户凭证会消耗数量上相近似的防火墙及客户处理资源。防火墙随后会验证客户凭证并响应该验证为访问专用网络资源建立安全通道。因此，随后利用该安全通道把来自客户的数据通过防火墙转发到专用网络资源。

根据本发明的另一示范性实施例，提供与专用网络资源建立连接的计算机程序产品和方法，用于启动一系列认证事务，这些认证事务被设计用于在请求访问专用网络资源的客户上和作为专用网络网关来操作的防火墙上施加相称的处理负担。客户最初并不知道防火墙是作为该专用网络的网关在操作。此外，每一认证事务会递增客户与防火墙之间的信任级别，直到客户与防火墙的认证得到充分验证。

该系列认证事务可包括根据这些事务之一来认证客户的方法，并要求客户以一种要求类似处理负担的方式进行认证。在该系列认证事务结束后，客户被准许通过防火墙来访问专用网络资源。

根据本发明的另一示范性实施例，通过由防火墙从客户处接收被引导至服务器的访问请求，提供一种能通过防火墙、但无需客户了解防火墙情况便能访问服

务器的方法。由于客户并不知道防火墙是作为服务器的网关在操作，故访问请求会被直接引导至服务器。防火墙产生一个或多个认证凭证，该凭证表明服务器与防火墙之间的信任级别，并发送要使客户向防火墙认证的请求。此请求包括一个或多个防火墙认证凭证，以便客户了解服务器与防火墙之间的信任级别而不必再进行单独请求。防火墙随后会从客户处接收并验证一个或个多认证凭证。之后，防火墙使客户能够通过防火墙来访问服务器。

随后的说明中会提出本发明的其它特征和优点，并且其中一部分在说明中会显而易见或可以通过实践本发明而掌握。借助在所附权利要求书中特别指出的手段及其组合，可以实现并获得本发明的其它特征和优点。本发明的这些和其它特征在以下说明和所附权利要求书中会变得更加完全清楚，或可以通过按下文所述来实践本发明而掌握。

附图说明

为了对可获得本发明上述及其它优点和特征的方式进行描述，将通过参考附图中说明的特定实施例对在上文中简要描述的本发明进行更加具体的描述。理解到这些图式只是说明本发明的典型实施例，因此不会认为它们限制本发明的范围，以下将利用附图对本发明进行更为具体和详细地进行描述，其中：

图 1 所示是典型的 VPN 连接；

图 2 所示是根据本发明示范性实施例的 VPN 连接；

图 3 所示是根据本发明示范性实施例的透明 VPN 连接的功能性；

图 4 显示了根据本发明把客户和专用网络连接的方法的示范性动作和步骤；以及

图 5 所示为本发明提供适当操作环境的一个示范性系统。

具体实施方式

本发明延及以透明虚拟专用网络（VPN）减少网络配置复杂性的方法、系统和计算机程序产品。本发明的实施例可以包括一台包括各种计算机硬件的专用或通用计算机，以下参考图 5 的更详细地论述。

图 1 描述一典型的 VPN 基础结构，其中远程用户能利用诸如因特网的公共网络与专用网络建立连接。主局域网（LAN）125 可以由（例如）远程 LAN 100 利用站点至站点 VPN 115 和专用设备来访问用于大规模数据加密。站点至站点 VPN 115 可以以企业内部互联网、外部互联网等为基础。如果一公司拥有一个或多个希望以单一专用网络相联接的远程场所，则可以创建企业内部互联网 VPN，使 LAN 与 LAN 连接。同样，当一公司与另一公司具有密切关系（如伙伴、供货商或客户）时，他们可以建立企业外联网 VPN，使 LAN 与 LAN 连接，并使所有不同公司能够在共享环境中工作。

作为替代或与之结合，远程用户 130 或家庭用户 105 能利用远程访问 VPN 120 来与主 LAN 125 连接。希望建立大型远程访问 VPN 120 的公司可以向企业服务提供商（ESP）（未示出）外购或建立自己的 VPN 网关。ESP 建立网络访问服务器（NAS），并为远程用户 130 和 105 的计算机提供客户软件。远程用户 130 和 105 随后能够拨通免费号码到达 NAS，并使用他们的 VPN 客户软件经由用于公共或专用网络的入网点（POP）135 和 110 来访问公司网络。

图 1 中，VPN 通信量是通过路由器 140 和 145 在诸如因特网的公共网络发送。路由器是专门的计算机，会沿着各种路径向其目的地发送网络通信量。路由器有两项单独但相关的工作。首先，它会确保信息不会到达不需要该信息的地方。其次，它会确保信息能够到达预计的目的地。因此，路由器对于处理两个单独的计算机网络非常有用。它会连接两个网络，从一个网络向另一个网络传递信息。它也会形成相互间的网络保护，防止一个网络的通信量不必要地泄漏到另一个网络。

图 2 对客户 200 怎样访问网络 225 的做了更加详细的描述。通常，客户 200 能通过因特网 205 来访问网络 225。从客户 200 发往网络 225 的数据穿过防火墙 210 或 VPN 网关 230 或 235 之一。当前，如果客户 200 希望通过 VPN 网关 230 或 235 来访问网络 225，那么客户 200 必须知道对应的 VPN 网关 230 或 235 的 IP 地址。（VPN 网关经常使用 IP 地址而不是域名作为额外的安全措施）。例如，若特定服务器 240 是用于专用网络 225 的邮件服务器，则客户 200 必须知道网关 230 的 IP 地址，该网关是特定邮件服务器 240 的 VPN 网关。与此类似，若特定服务器 245 为用于专用网络 225 的记帐服务器，则客户 200 必须知道网关 235 的 IP 地址，网关 235 是特定记帐服务器 245 的 VPN 网关。为了能够在专用网络 225 中访问特定

服务器 240 或 245，客户 200 应向 VPN 网关提供适当的凭证。这些凭证可以是诸如以下项目之一或其组合：用户名称、客户 IP 地址、密码、通行证、智能卡、信用卡号等。

根据本发明的示范性实施例，客户 200 可尝试经过防火墙 210 来访问专用网络 225。与当前的设计不同，由于发往专用网络 225 的信息包会根据信息包网络路由选择程序而出现在防火墙外（左）侧，故客户不需要知道防火墙的 IP 地址。此外，防火墙 210 有能力向客户 200 要求凭证。防火墙 210 所执行的要求的类型可包括各种加密协议的应用，如：安全套接层（SSL）、传输层安全（TLS）等。如本领域的熟练技术人员所认识到：SSL 和 TLS 是用于传输敏感信息的安全协议。

然而，在透明 VPN 中通常使用安全协议（如以上提到的协议）类型造成的问题是其具有发生拒绝服务（DoS）攻击的潜在可能性。如本领域的熟练技术人员所认识到：DoS 攻击属于这样一种事件，其中，由于资源为无效请求所淹没，用户通常期望具有的资源服务会被剥夺。例如，服务丢失可能是无法利用一特定的网络服务（如：电子邮件），或暂时丢失所有网络连通和服务。

拒绝服务攻击可能出现在透明 VPN 设置中的客户或者网络上。例如，当防火墙接收到消息并返回已签署的要求时，DoS 攻击可能出现在防火墙中。由于已签署的要求比发送消息需要多得多的处理工作，故攻击者可以通过向防火墙发送一串信息包而轻易将它淹没，从而拒绝为合法客户服务。与此类似，当客户接收来自防火墙的未经签署的要求、指示客户提供适当的安全凭证时，客户处可能出现 DoS 攻击。通过向客户转移处理负担，可创建一攻击途径。任何人均可以向客户发送未经签署的消息，造成客户与防火墙联系并尝试计算量很大的认证过程。

为对付 DoS 攻击的潜在问题，本发明提供了替代类型的认证。一示范性实施例使用零知识证明（zero-knowledge proof）向客户要求凭证。简单而言，零知识证明涉及客户与防火墙之间的一序列交换，它会随着通信的进展递增两者之间的信任级别。这些交换可以是在数个演化序列中，包括将附加了原始消息的消息、一系列随机问题如名称或时间等向请求者返回。

更正式而言，零知识证明是双方之间的交互式证明协议，包括一证实器（prover）和一验证器（verifire）。证实器使验证器相信一陈述而不必暴露关于怎样证明该陈述的任何信息。零知识证明通常包括几个回合。零知识证明中的

一典型回合可能由来自证实器的“承诺”消息、继之以来自验证器的要求、以及继之以证实器对该要求的响应组成。虽然证实器有可能猜测到对一给定回合的适当响应，但该协议可以重复，直至连续正确猜测的不太可能达到可接受的水平。换言之，若在该证明的每一回合中有一半机会能猜测到正确的响应，则在 20 次反复后，正确猜测 20 次响应中每一次响应的概率低于 2^{-20} 即 0.0000009536。依据所有回合中证实器的响应，验证器确定是接收还是拒绝该证明。

执行零知识证明可包括防火墙 210 匿名向客户 200 提出要求。采用上述零知识证明技术，客户 200 可提交其具有凭证并且这些凭证是正确的证明，而不需要实际向防火墙 210 提供凭证。因此，如本申请中所用的术语“凭证”应从广义上解释为包括以凭证为基础的零知识证明以及凭证本身。作为替代或与之结合，在实际凭证提交之前，客户 200 可请求防火墙 210 对其自身进行识别。

可以根据示范性实施例进行修改并用于对付 DoS 攻击的另一认证过程被称为单 b 边认证过程。此过程使一装置能够以某种方式写入消息，使得此消息只能由此特定装置来写。此认证机制为单边性的，因为接受者无需为完成认证过程而与发送者进行进一步交流。该消息中包含消息接受者（如客户）解码该消息并确定此消息一定来自此特定装置所需要的所有信息。

本发明是依据与基于公共密钥的消息发送者的（例如）网址选择组合使用的公共密钥/专用密钥密码系统。以下说明显示在本发明中应怎样使用单边认证。客户 200 可以请求访问网络 225 中的特殊主机或服务器，如特定服务器 240 或 245。最初，客户 200 未觉察到有防火墙 210，且只打算将请求传送至网络 225 中的特定主机（请注意，并未示出受防火墙 210 保护的特定服务器）。但由于防火墙 210 可以保护网络 225 中的一台特定主机，故该要求首先会传送至防火墙。

在向网络 225 中期望访问的主机转发请求之前，防火墙 210 需要验证客户 200 已经被授权访问网络 225 中的特定主机。虽然防火墙 210 可自由地请求客户 200 对自身进行认证，但客户 200 不知有防火墙 210 且可能怀疑防火墙 210 正试图进行攻击，如 DoS 攻击或安全破坏。因此，客户 200 可能不对防火墙 210 的认证请求作出响应，并因此不能访问网络 200 中期望访问的主机。

然而，本发明能够以单边方式使防火墙 210 获得客户 200 的信任。例如，示范性实施例可以使防火墙 210 与网络 225 内期望访问的主机具有信任关系。如此

一来，可以使防火墙 210 得到期望访问的主机的专用密钥，或网络 225 内期望访问的主机会代表防火墙 210 使用其专用密钥。从而，当防火墙 210 请求客户 200 的凭证时，防火墙 210 可包括采用网络 225 内期望访问主机的专用密钥来加密的消息或网址，以表明防火墙 210 受到网络 225 中期望访问主机的信任。若客户 200 能够采用网络 225 中期望访问主机的公共密钥来解密该消息，则客户 200 知道该消息已采用期望访问主机或服务器的专用密钥加密，并因此能够推断防火墙 210 受到网络 225 中期望访问主机的信任。

在使用该单边认证过程时，客户 200 亦能为各种有利原因而创建并保持一已认证公共密钥/网址关联性的高速缓存。例如，在有高速缓存的情况下，客户 200 就能用它来认证输入的消息，特别是所到达的是无公共密钥的消息时。然而对于包含公共密钥的消息，由于仍必须为这些消息执行上述程序，故最初看来高速缓存并不能减少接收者的处理负担。这通常是对的，但有一例外使该高速缓存非常有价值。如上所述，接收者可能是 DoS 攻击的目标，此攻击中充满了无效的输入消息。高速缓存可用于防止此攻击。若输入消息的数量超出接收者能够充分处理的数量，则接收者会根据简化的程序来处理输入消息。例如，可将消息的公共密钥和网址与高速缓存中已经存在的公共密钥/网址关联进行比较。如未能找到匹配，则该消息会被丢弃。如找到匹配，则使该消息经过上述全部认证程序。在 DOS 攻击过程中，此程序会过滤掉无效消息而不会在无效消息上面浪费宝贵的解密时间，从而使接收者能够继续接收有效输入消息。当然，此程序只能解密那些公共密钥和网址已经存在于高速缓存中的消息。它不允许接收者接收那些带一个有效但先前并未看到过的公共密钥和网址的输入消息。在 DOS 攻击过程中，这是客户可能愿意采取的一个折衷办法。一旦接收者成功经受住 DOS 攻击，它随即会恢复成更完全的程序。

在客户 200 向防火墙 210 提供凭证之后，防火墙 210 会对这些凭证进行验证并与客户协商安全通道 215，用于访问专用网络 225 的服务器 240 和 245。从那时起，客户 200 会为发往专用网络 225 的服务器 240 和 245（或其它服务器）的数据包使用安全通道 215。发往其它服务器（如服务器 250）的其它数据包会通过因特网 205 发送到服务器 250，而无需首先通过专用网络 225。

在本发明的一替代示范性实施例中，防火墙 210 利用一个已认证通道 220 向专用网络 225 的服务器 240 和 245 转发数据包，该通道向服务器表示：客户已经通过在防火墙中执行的安全检查。已认证的通道 220 可包括（例如）由防火墙 210 证明的已签署数据，它特别表示：客户 200 已经被授权访问专用网络 225。

在本发明的另一替代示范性实施例中，该防火墙可以是在通往网络 225 的路径中嵌套的防火墙或几个防火墙 211 和 212 之一。每一防火墙 211 和 212 起到一个检查点的作用，用于控制专用网络 225 的安全方面。

如本领域的熟练技术人员所认识到的：通常防火墙不会要求用户提供凭证来避免拒绝服务攻击，这些攻击会使防火墙变得负担过重，并拒绝为所有试图访问专用网络的用户服务。根据本发明的示范性实施例，此问题可以通过在允许客户 200 访问专用网络 225 之前，由防火墙 210 发送未经签署的信息包来要求客户 200 并使客户 200 执行密码或其它处理而得到解决。如本领域的熟练技术人员所认识到的：此过程一般称为难题防御（puzzle defense）。防火墙 210 通过请求客户 200 在被准需访问专用网络 225 之前解决一难题而向其转移处理（或另一）负担。

图 3 显示怎样将客户 300 路由至服务器 340、并通过防火墙 335 的示范性实施例。如本领域的熟练技术人员所认识到：可用域名例如：www.company.com 将客户 300 路由至防火墙 335。客户 300 通过因特网服务提供商（ISP）315 连接至因特网 310，该提供商了解至少一个域名系统（DNS）服务器 305。当客户 300 开启它的浏览器，请求连接至 http://www.company.com 时，它可以为 http://www.company.com 这个特定 IP 地址向 DNS 服务器 305 请求信息。若 DNS 服务器 305 了解 www.company.com 这个特定的 IP 地址，则它能够向客户 300 提供此信息。客户 300 随后将附带该特定 IP 地址信息的数据转发到它的 ISP 315，ISP 315 随后会以用于到达服务器 340 的路由选择数据库将该数据转发到一个或多个其它 ISP（如 ISP 320 和 330）。在去往服务器 340 途中，该数据会通过防火墙 335。应该注意的是，DNS 信息会把 http://www.company.com 的通信量引导至防火墙 335。从而客户无需特别了解防火墙 335 或服务器 340，而只需一域名即可。

防火墙 335 此刻会向客户 300 要求凭证。此要求的形式可以是：防火墙并不对客户 300 访问服务器 340 的请求作出回答。如此一来，客户 300 会知道，为了能够访问受保护的服务器 340，它需要发送凭证。

可按照包括功能步骤和/或非功能动作（functional steps and/or non-functional acts）的方法对本发明进行描述。以下描述的动作和步骤可在实践本发明中执行。通常，功能步骤根据所完成的结果来描述发明，而非功能动作则描述用于获得某一特殊结果的更特定的行动。虽然可以按一特殊顺序来描述或主张这些功能步骤和非功能动作，但不必将本发明限制于动作和/或步骤的任何特殊顺序或组合。

图 4 说明用于在平衡客户与防火墙之间的认证要求以共同防卫拒绝服务攻击时建立与专用网络的连接的示范性步骤与动作。用于开始认证事务的系列的步骤 400 可包括从客户处接收请求访问专用网络资源的动作 405。此系列的认证事务被设计用于在请求访问专用网络资源的客户上和作为该专用网络网关操作的防火墙上施加相称的处理负担。此外，客户最初并不知道防火墙是作为该专用网络的网关在操作。而且，每一认证事务会递增客户与防火墙之间的信任级别，直到客户与防火墙的认证得到充分验证。

用于开始系列的步骤 400 也可包括用于根据此系列事务之一来向客户认证的步骤 410。此外，用于向客户认证的步骤 410 也可包括由防火墙发送防火墙凭证以认证防火墙的动作 415。产生防火墙凭证会消耗一定量的有限的防火墙处理资源。

用于开始的步骤 400 也可包括用于要求客户提供凭证的步骤 420。用于要求的步骤 420 也可进一步包括要求客户凭证的动作 422 和接收客户凭证的动作 424。产生客户凭证会消耗一定量的有限的客户处理资源，此消耗在数量上与有限的防火墙处理资源消耗类似。

最后，在该系列认证事务结束后，准许客户通过防火墙来访问专用网络资源的步骤 400 可包括以下动作。首先是验证客户凭证的动作 442。接着是建立安全通道的动作 444，用于为响应客户凭证的验证而访问该专用网络的专用网络资源。随后是利用安全通道、通过防火墙从客户向专用网络资源转发数据的动作 446。最后是提供防火墙签署数据包的动作 448。已签署数据包是从客户发往专用网络资源，且该签署表示客户已经通过防火墙中执行的最低的安全级别。

签署的动作 448 使防火墙能够利用已认证的通道向服务器转发数据包，如已签署数据，这是向服务器表示：客户已经通过了防火墙中执行的安全检查。在动

作 448 中，IPSec 认证头（AH）工具是在防火墙与服务器之间建立一条已认证隧道的办法之一。此外，防火墙可以为嵌套式的或是几个防火墙之一，其中每一防火墙起到控制专用网络安全方面的检查点的作用。防火墙也可利用其高速缓存来辨认：它最近已验证一特定客户的凭证并根据防火墙高速缓存中提供的凭证来签署该数据。

本发明范围内的实施例还包括用于承载或含有计算机可执行指令的计算机可读媒质或存储于其上的数据结构。此计算机可读媒质可以是能够被通用或专用计算机所访问的任何可利用的媒质。举例而言，但并非限制，此计算机可读媒质可以包括 RAM、ROM、EEPROM、CD-ROM 或其它光盘存储器、磁盘存储器或其它磁存储装置、或任何可用于承载或储存所需的计算机可执行指令或数据结构形式的程序编码装置并且可由通用或专用计算机存取的其它媒质。当通过网络或另外的通信连接（或有线、或无线，或有线与无线的组合）向计算机传送或提供信息时，计算机会适当地将该连接视为计算机可读媒质。从而可将任何此类连接适当地定义为计算机可读媒质。以上各项的组合也应包括在计算机可读媒质的范围内。计算机可执行指令包括例如促使通用计算机、专用计算机、或专用处理装置执行某一功能或一组功能的指令和数据。

图 5 和以下论述旨在提供可执行本发明的适当计算机环境的简明、概括的描述。虽然未做要求，但大致会按照计算机可执行指令来描述本发明，如由网络环境中的计算机执行的程序模块。一般而言，程序模块包括执行特殊任务或实施特殊抽象数据类型的例行程序、程序、对象、组件、数据结构等。计算机可执行指令、相关的数据结构和程序模块代表用于执行本文所揭示方法之步骤的程序编码装置的例子。特殊序列的此类可执行指令或相关数据结构代表用于执行此类步骤中所描述功能的对应动作的例子。

本领域的熟练技术人员会明白，可以在具有许多类型的计算机系统配置的网络计算机环境中实践本发明，这些计算机系统配置包括：个人计算机、手持式装置、多处理器系统、基于微处理器或可程式化的客户电子设备、网络 PC、小型计算机、大型计算机等等。也可以在分布式处理环境中实践本发明，在此环境中，任务由通过通信网络链接（或通过有线链接、无线链接，或通过有线或无线链接

的组合）的本地和远程处理装置来执行。在分布式处理环境中，可将程序模块定位于本地和远程存储装置中。

参考图 5，用于执行本发明的一示范性系统包括以传统计算机 520 为形式的通用计算装置，它包括：处理单元 521、系统存储器 522、以及系统总线 523，它可以把包括系统存储器 522 等的各种系统组件耦合到处理单元 521。系统总线 523 可以是几种总线结构类型的任一种，这些总线结构包括：存储器总线或存储器控制器、外围总线、以及采用多种总线构造的任一种的本地总线。系统存储器包括只读存储器（ROM）524 和随机存取存储器（RAM）525。可在 ROM 524 中存储基本输入/输出系统（BIOS）526，包含譬如在启动过程中协助在计算机 520 内的元件之间传送信息的基本例程。

计算机 520 也可以包括：用于读写磁硬盘 539 的磁硬盘驱动器 527、用于读写可移动磁盘 529 的磁盘驱动器 528、以及用于读写可移动光盘 531 的光盘驱动器 530，如 CD-ROM 或其它光学媒质。磁硬盘驱动器 527、磁盘驱动器 528 和光盘驱动器 530 分别由硬盘驱动器接口 532、磁盘驱动器接口 533 和光盘驱动器接口 534 连接到系统总线 523。这些驱动器及其相关计算机可读媒质可以非易失性地存储计算机可执行的指令、数据结构、程序模块和用于计算机 520 的其它数据。虽然本文所述的示范性环境中使用了磁硬盘 539、可移动磁盘 529 和可移动光盘 531，但也可使用用于存储数据的其它类型的计算机可读媒质，包括磁带、闪存卡、数字化视频光盘、Bernoulli 磁盒、RAM、ROM 及类似媒质。

可将包括一个或更多程序模块的程序编码装置存储于硬盘 539、磁盘 529、光盘 531、ROM 524 或 RAM 525 上，包括操作系统 535、一个或更多应用程序 536、其它程序模块 537 和程序数据 538。客户可以通过键盘 540、指向装置 542 或其它输入装置（未示出）如：麦克风、操纵杆、游戏垫、碟式卫星天线、扫描仪或类似装置向计算机 520 输入命令和信息。这些和其它输入装置常常通过与系统总线 523 耦合的串行端口接口 546 连接到处理单元 521。或者，可由其它接口，如：并行端口、游戏端口或通用串行总线（USB）来连接这些输入装置。监视器 547 或其它显示装置也通过接口（如视频适配器 548）连接到系统总线 523。除监视器外，个人计算机通常还包括其它外围输出装置（未示出），如扬声器和打印机。

可在网络环境中操作计算机 520，采用与一台或多台远程计算机如：远程计算机 549a 和 549b 逻辑连接来进行。虽然图 5 中只说明存储装置 550a 和 550b 及其相关应用程序 536a 和 536b，但远程计算机 549a 和 549b 可各为另一个人计算机、服务器、路由器、网络 PC、对等装置或其它公共网络节点，并通常包括与计算机 520 有关的上述多个或所有元件。图 5 中描述的逻辑连接包括局域网（LAN）551 和广域网（WAN）552，两者通过例子呈现于此，且并不限制本发明。此类联网环境在办公室范围或企业范围的计算机网络、企业内部互联网和因特网中经常使用。

当在 LAN 联网环境中使用时，通过网络接口或适配器 553，计算机 520 会被连接到本地网络 551。当在 WAN 联网环境中使用时，计算机 520 可包括调制解调器 554、无线链接、或用于通过广域网 552（如因特网）建立通信的其它装置。把可以是内置或外置的调制解调器 554 经过串行端口接口 546 连接到系统总线 523。在联网环境中，可以把关于计算机 520 而描述的程序模块或部分存储于远程存储装置中。应该明白，所显示的网络连接只是例子，且可以采用其它通过广域网 552 建立通信的装置。

可以以其它特定形式来具体化本发明而不会背离其精神或本质特征。应该认为所述实施例的所有方面只是说明而非限制。因此，本发明的范围是由后附的权利要求书而不是由前述描述来指出。根据本权利要求书的等效技术方案的含义与范围所进行的所有改变均会包含于权利要求书范围内。

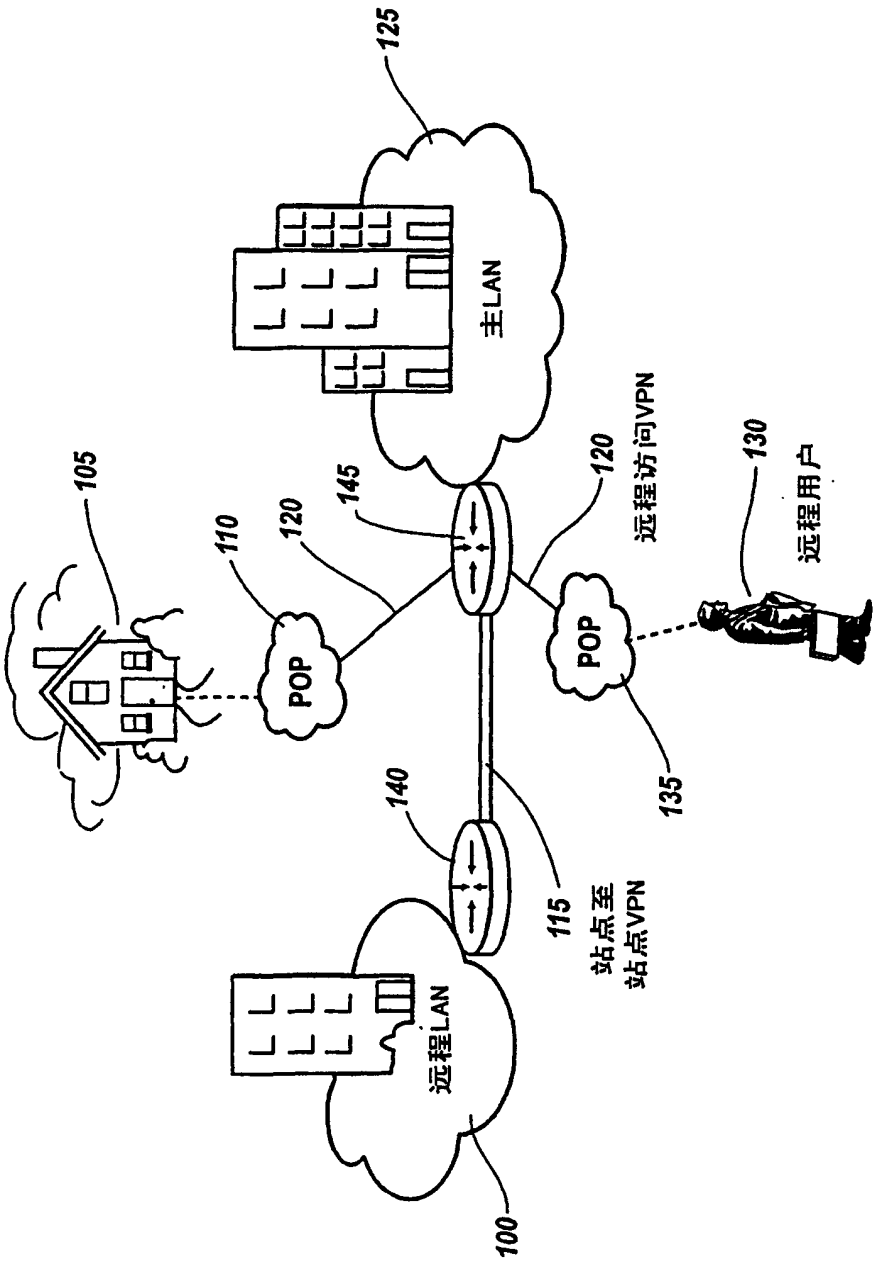

125
主LAN
105
110
120
145
120
远程访问VPN
130
远程用户
POP
POP
135
140
115
站点至
站点VPN
远程LAN
100

图 1

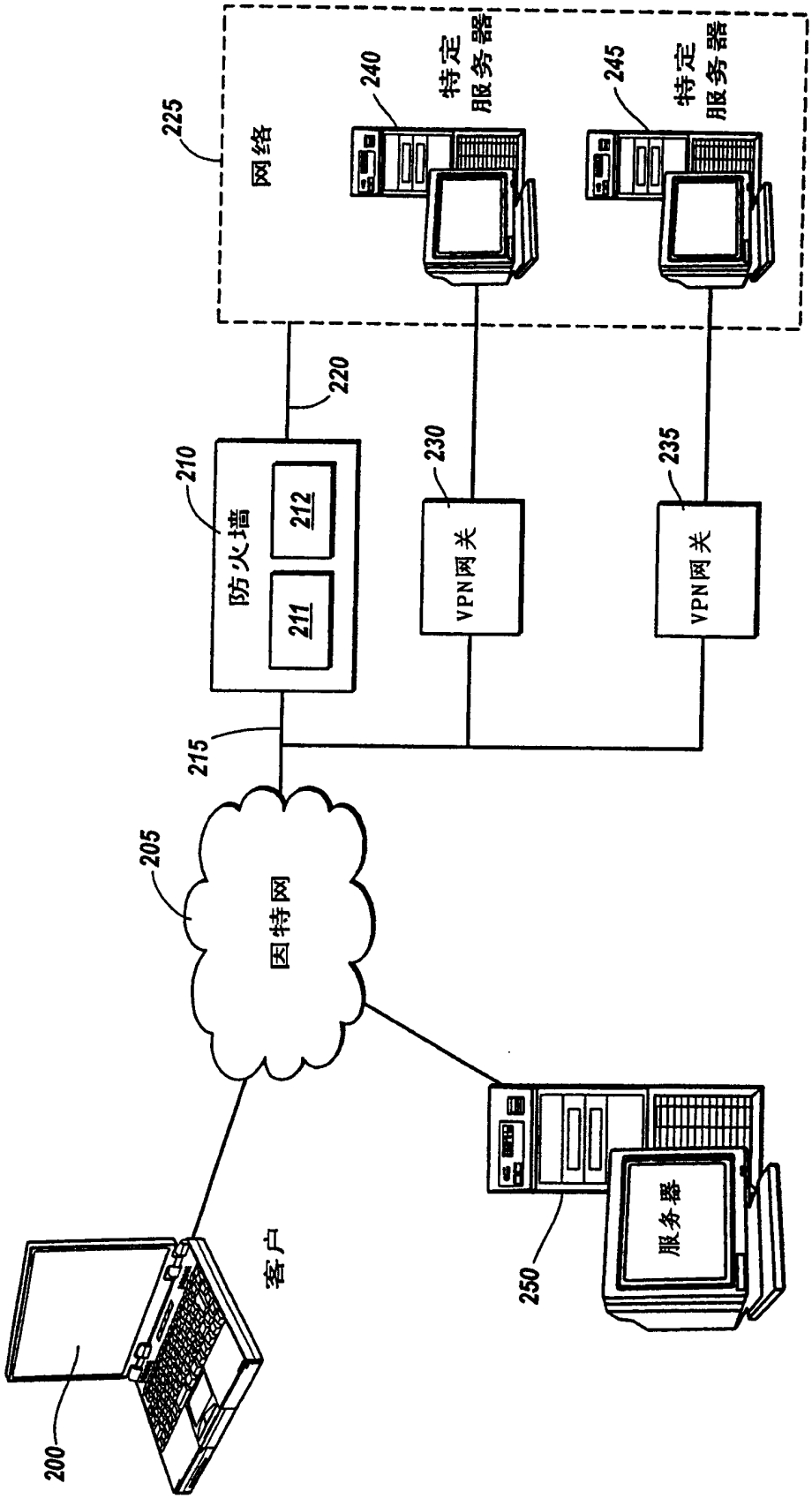

225
网络
240
特定服务器
245
特定服务器
220
210
防火墙
212
211
230
VPN网关
235
VPN网关
215
205
因特网
250
服务器
客户
200

图 2

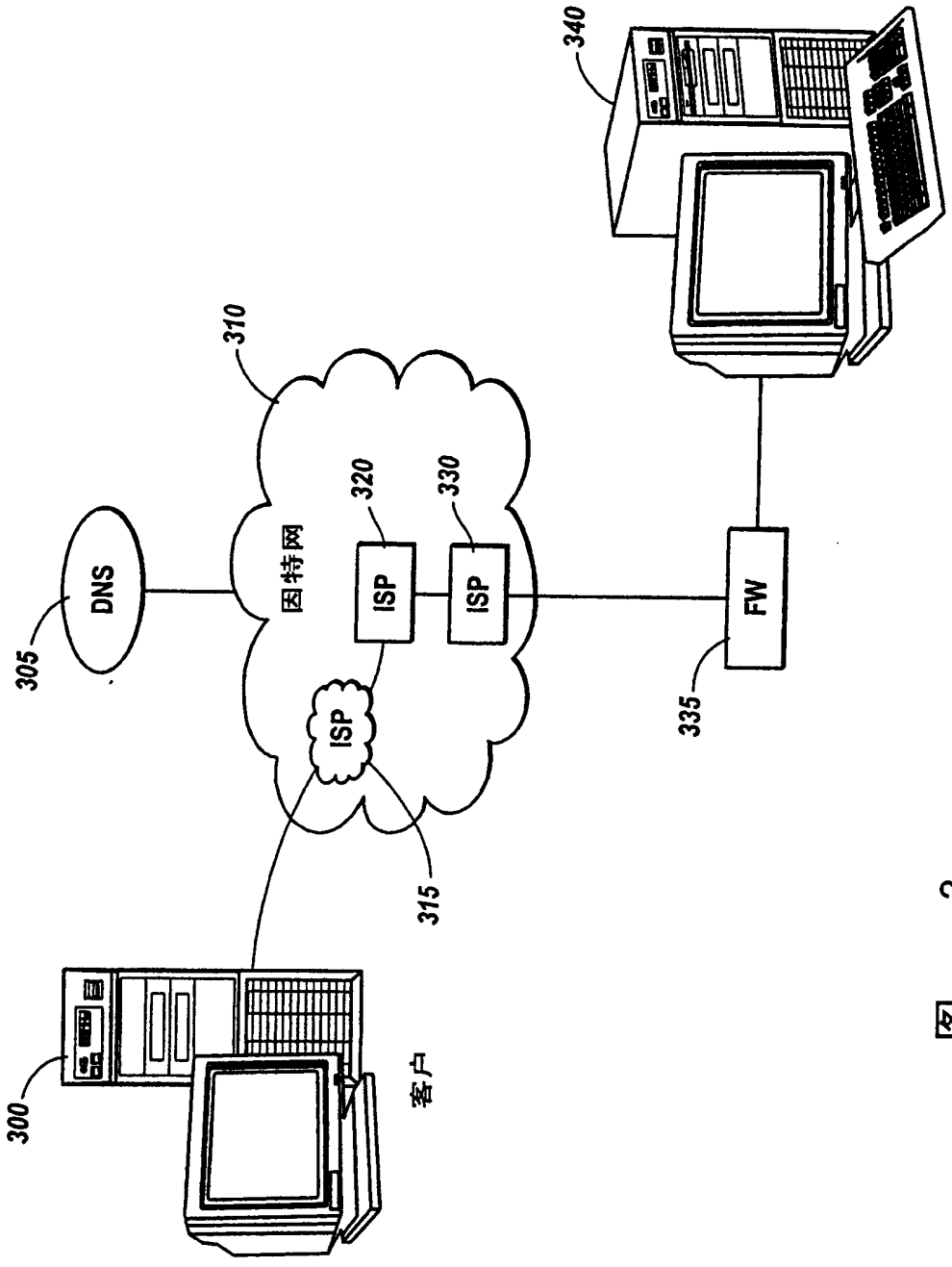


图 3

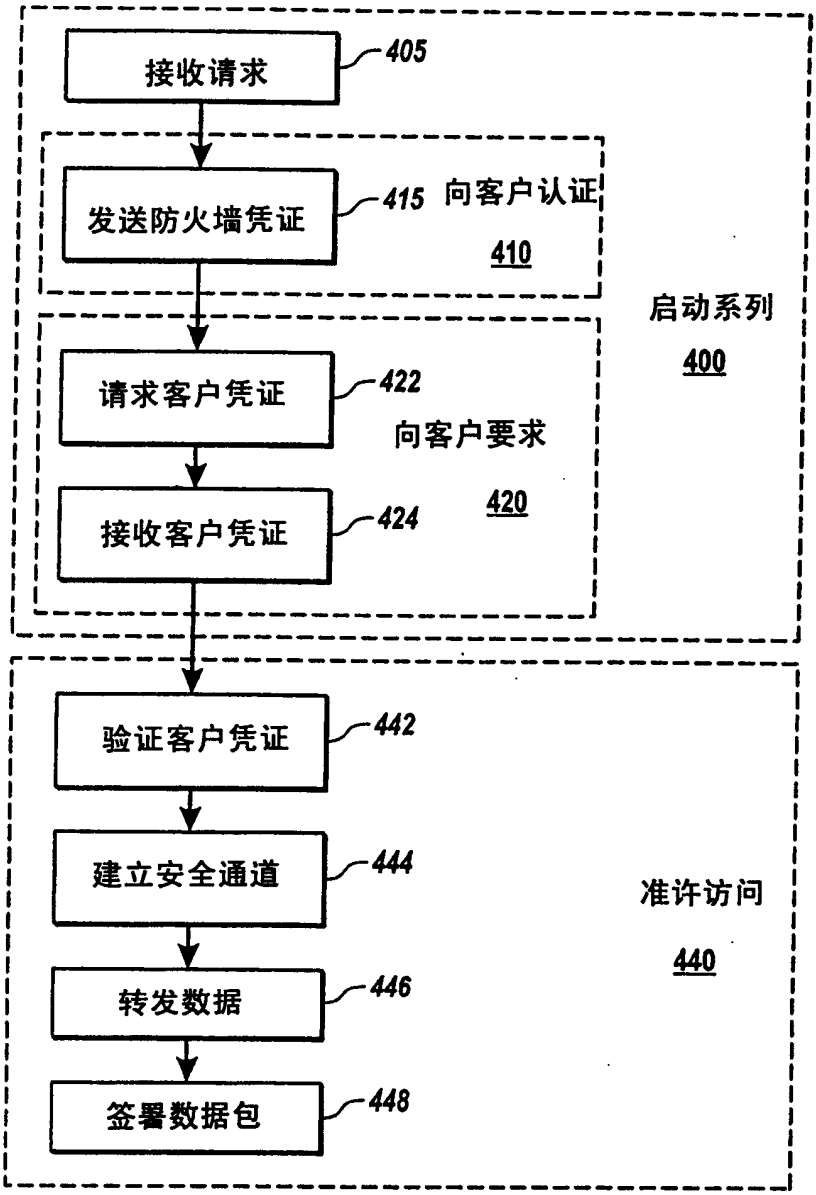

接收请求
405
发送防火墙凭证
415
向客户认证
410
启动系列
400
请求客户凭证
422
向客户要求
420
接收客户凭证
424
验证客户凭证
442
建立安全通道
444
准许访问
440
转发数据
446
签署数据包
448

图 4

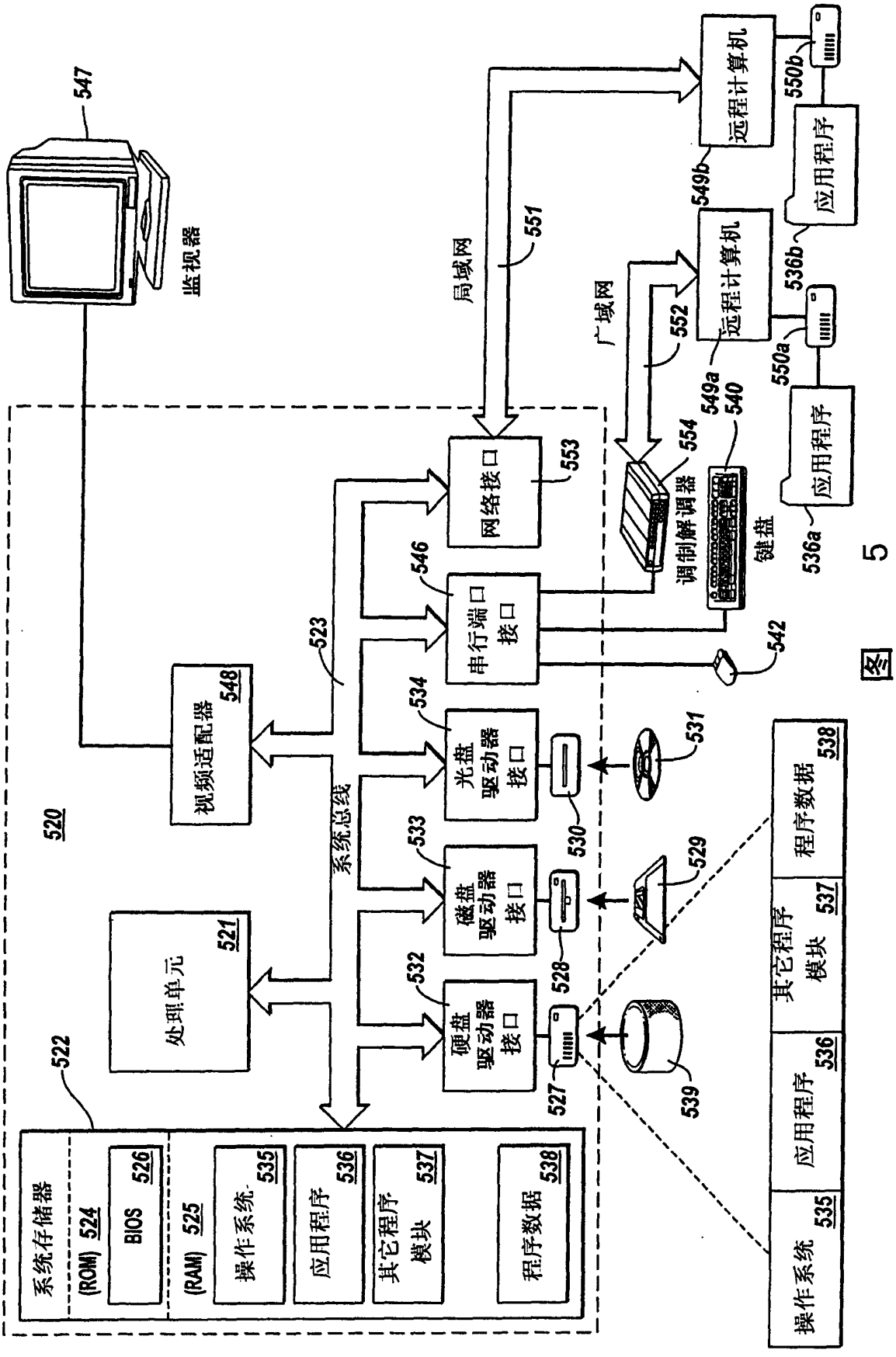

547
监视器
局域网
551
广域网
552
远程计算机
549b
550b
应用程序
536b
550a
549a
540
554
远程计算机
应用程序
网络接口
553
调制解调器
键盘
536a
546
串行端口接口
542
523
534
光盘驱动器接口
531
视频适配器
548
系统总线
520
533
磁盘驱动器接口
530
529
处理单元
521
532
硬盘驱动器接口
528
522
527
539
其它程序模块
537
程序数据
538
系统存储器
(ROM) 524
BIOS 526
(RAM) 525
操作系统
535
应用程序
536
其它程序模块
537
程序数据
538
操作系统
535
应用程序
536

图 5