[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 17/00 (2006.01)
H04L 9/32 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200580015562.2

[43] 公开日 2007 年 12 月 26 日

[11] 公开号 CN 101095134A

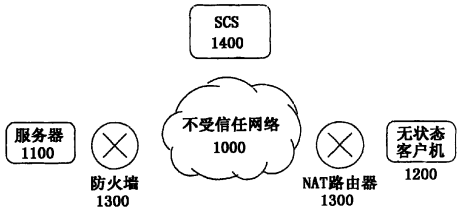
[22] 申请日 2005.4.12
[21] 申请号 200580015562.2
[30] 优先权
[32] 2004. 4.12 [33] US [31] 60/561,806
[86] 国际申请 PCT/US2005/012454 2005.4.12
[87] 国际公布 WO2005/101747 英 2005.10.27
[85] 进入国家阶段日期 2006.11.14
[71] 申请人 XDS 有限公司
地址 美国纽约州
[72] 发明人 布赖恩·吉莱斯皮 赫尔穆特·萨门
大卫·特雷西
[74] 专利代理机构 北京集佳知识产权代理有限公司
代理人 杨生平 杨红梅
权利要求书 7 页 说明书 12 页 附图 4 页

[54] 发明名称

自动发起和动态建立有防火墙的服务器和有防火墙的客户机之间的安全的因特网连接的系统和方法

[57] 摘要

使用会话控制服务器(SCS)自动且动态地发起和建立服务器和客户机之间的安全连接的系统和方法。 服务器和客户机均通过网络地址转换器或转换(NAT)路由器或防火墙连接到不受信任网络(如因特网)。 服务器和客户机均独立信任的 SCS 作为中间方来约定所需的连接参数，以建立服务器和客户机之间的安全连接。 该系统和方法不需要在客户机上进行任何用户配置并且无需服务器接受来自客户机的直接的连接请求或包，由此允许服务器防火墙对所有入站业务总是保持关闭。



1. 一种使用服务器和客户机均信任的第三方计算机自动发起和动态建立所述客户机和所述服务器之间的经由不受信任网络的安全连接的方法，所述服务器不接受来自任何客户机的直接的连接请求或包，所述客户机和所述服务器的每一个通过防火墙或网络地址转换器（NAT）路由器连接到所述不受信任网络，所述方法包括如下步骤：

在通电时通过所述客户机的用户的单一动作、在连接到所述不受信任网络时，或在所述客户机的网络参数发生任何变化时，所述客户机向所述第三方计算机自动发送连接请求，所述连接请求包括连接到所述服务器的请求；以及

使用所述第三方计算机经由所述不受信任网络在所述服务器和所述客户机之间交换连接参数，所述连接参数包括唯一连接标识符，以通过与所述客户机关联的 NAT 路由器建立所述服务器和所述客户机之间的安全连接，由此向所述客户机的所述用户提供到所述服务器的单一动作接入。

2. 根据权利要求 1 所述的方法，进一步包括以下步骤：

与所述服务器关联的防火墙接收来自所述客户机的包括所述唯一连接标识符的未经请求的包，以动态建立所述客户机和所述服务器之间的临时映射；以及

如果确定所述未经请求的包中的所述唯一连接标识符与所存储的唯一连接标识符匹配，则所述服务器使用所述动态建立的临时映射经由所述不受信任网络向所述客户机发送响应包。

3. 根据权利要求 1 所述的方法，进一步包括以下步骤：

所述服务器接收来自所述第三方计算机的所述客户机的目的地入站端口和与所述客户机关联的所述 NAT 路由器的公有地址；以及

所述服务器将所述服务器的目的地端口和与所述服务器关联的所述防火墙的 IP 地址以及用于所述客户机的所述唯一连接标识符发送给所

述第三方计算机。

4. 根据权利要求 3 所述的方法，进一步包括以下步骤：

所述客户机从所述第三方计算机接收使用所述服务器的所述目的地端口和与所述服务器关联的所述防火墙的所述 IP 地址将所述未经请求的包发送到所述服务器的指令；以及

如果确定在所述服务器的所述目的地端口上收到来自与所述客户机关联的所述 NAT 路由器的所述公有地址的所述未经请求的包，则所述服务器向所述客户机发送所述响应包。

5. 根据权利要求 3 所述的方法，进一步包括以下步骤：所述服务器使用自所述第三方计算机接收的所述客户机的所述目的地入站端口发起到所述客户机的所述安全连接。

6. 根据权利要求 2 所述的方法，其中所述接收步骤包括以下步骤：与所述服务器关联的所述防火墙接收来自所述客户机的包括所述唯一连接标识符的未经请求的 UDP 或 TCP 包。

7. 一种使用服务器和客户机均信任的第三方计算机自动发起和动态建立所述客户机和所述服务器之间的经由不受信任网络的安全连接的方法，所述服务器不接受来自任何客户机的直接的连接请求或包，所述客户机和所述服务器的每一个通过防火墙或网络地址转换器（NAT）连接到所述不受信任网络，所述方法包括如下步骤：

使用所述第三方计算机经由所述不受信任网络在所述服务器和所述客户机之间交换连接参数，所述连接参数包括唯一连接标识符；

与所述服务器关联的防火墙接收来自所述客户机的包括所述唯一连接标识符的未经请求的包，以动态建立所述客户机和所述服务器之间的临时映射；以及

如果确定所述未经请求的包中的所述唯一连接标识符与所存储的唯一连接标识符匹配，则所述服务器使用所述动态建立的临时映射经由所述不受信任网络向所述客户机发送响应包，由此通过与所述客户机关联

的 NAT 路由器建立所述服务器和所述客户机之间的安全连接。

8. 根据权利要求 7 所述的方法，进一步包括以下步骤：

所述服务器从所述第三方计算机接收所述客户机的目的地入站端口和与所述客户机关联的所述 NAT 路由器的公有地址；以及

所述服务器向所述第三方计算机发送所述服务器的目的地端口和与所述服务器关联的所述防火墙的 IP 地址以及用于所述客户机的所述唯一连接标识符。

9. 根据权利要求 8 所述的方法，进一步包括以下步骤：

所述客户机从所述第三方计算机接收使用所述服务器的所述目的地端口和与所述服务器关联的所述防火墙的所述 IP 地址将所述未经请求的包发送到所述服务器的指令；以及

如果确定在所述服务器的所述目的地端口上收到来自与所述客户机关联的所述 NAT 路由器的所述公有地址的所述未经请求的包，则所述服务器向所述客户机发送所述响应包。

10. 根据权利要求 8 所述的方法，进一步包括以下步骤：所述服务器使用自所述第三方计算机接收的所述客户机的所述目的地入站端口发起到所述客户机的所述安全连接。

11. 根据权利要求 7 所述的方法，其中所述接收步骤包括以下步骤：与所述服务器关联的所述防火墙接收来自所述客户机的包括所述唯一连接标识符的未经请求的 UDP 或 TCP 包。

12. 根据权利要求 7 所述的方法，进一步包括以下步骤：所述客户机向所述第三方计算机发送连接请求，所述连接请求包括连接到所述服务器的请求。

13. 根据权利要求 12 所述的方法，进一步包括以下步骤：在所述客户机通电时通过用户的单一动作、在连接到所述不受信任网络时或在所述客户机的网络参数发生任何变化时，所述客户机向所述第三方计算机自动发送所述连接请求，由此向所述客户机的所述用户提供到所述服务

器的单一动作接入。

14. 一种使用服务器和客户机均信任的第三方计算机自动发起和动态建立所述客户机和所述服务器之间的经由不受信任网络的安全连接的系统，所述服务器不接受来自任何客户机的直接的连接请求或包；其中所述客户机和所述服务器的每一个通过防火墙或网络地址转换器（NAT）连接到所述不受信任网络；其中所述客户机可操作来在通电时通过用户的单一动作、在连接到所述不受信任网络时或在所述客户机的网络参数发生任何变化时，向所述第三方计算机自动发送连接请求，所述连接请求包括连接到所述服务器的请求；并且其中所述服务器和所述客户机可操作来使用所述第三方计算机经由所述不受信任网络交换连接参数，所述连接参数包括唯一连接标识符，以通过与所述客户机关联的 NAT 路由器建立所述服务器和所述客户机之间的安全连接，由此向所述客户机的所述用户提供到所述服务器的单一动作接入。

15. 根据权利要求 14 所述的系统，其中与所述服务器关联的防火墙可操作来接收来自所述客户机的包括所述唯一连接标识符的未经请求的包，以动态建立所述客户机和所述服务器之间的临时映射；并且其中如果确定所述未经请求的包中的所述唯一连接标识符与所存储的唯一连接标识符匹配，则所述服务器可操作来使用所述动态建立的临时映射经由所述不受信任网络向所述客户机发送响应包。

16. 根据权利要求 14 所述的系统，其中所述服务器可操作来执行根据权利要求 1 所述的方法，该方法进一步包括以下步骤：

所述服务器接收来自所述第三方计算机的所述客户机的目的地入站端口和与所述客户机关联的所述 NAT 路由器的公有地址；以及

所述服务器向所述第三方计算机发送所述服务器的目的地端口和与所述服务器关联的所述防火墙的 IP 地址以及用于所述客户机的所述唯一连接标识符。

17. 根据权利要求 16 所述的系统，其中所述客户机可操作来接收来

自所述第三方计算机的使用所述服务器的所述目的地端口和与所述服务器关联的所述防火墙的所述 IP 地址将所述未经请求的包发送到所述服务器的指令；并且其中如果确定在所述服务器的所述目的地端口上收到来自与所述客户机关联的所述 NAT 路由器的所述公有地址的所述未经请求的包，则所述服务器可操作来向将所述客户机发送所述响应包。

18. 根据权利要求 16 所述的系统，其中所述服务器可操作来使用来自所述第三方计算机的所述客户机的所述目的地入站端口发起到所述客户机的所述安全连接。

19. 根据权利要求 15 所述的系统，其中所述服务器可操作来接收来自所述客户机的包括所述唯一连接标识符的未经请求的 UDP 或 TCP 包。

20. 根据权利要求 14 所述的系统，其中所述客户机是不执行任何用户功能或包含任何用户数据的无状态客户机。

21. 根据权利要求 14 所述的系统，其中所述客户机是单一功能网络感知的消费者设备。

22. 根据权利要求 21 所述的系统，其中所述单一功能网络感知的消费者设备是以下设备中的一种：蜂窝电话、音乐播放器/记录器、视频播放器/记录器、游戏播放器或便携式电子邮件设备。

23. 一种使用服务器和客户机均信任的第三方计算机自动发起和动态建立所述客户机和所述服务器之间的经由不受信任网络的安全连接的系统，所述服务器不接受来自任何客户机的直接的连接请求或包；其中所述客户机和所述服务器的每一个通过防火墙或网络地址转换器（NAT）连接到所述不受信任网络；其中所述服务器和所述客户机可操作来使用所述第三方计算机经由所述不受信任网络交换连接参数，所述连接参数包括唯一连接标识符；其中与所述服务器关联的所述防火墙可操作来接收来自所述客户机的包括所述唯一连接标识符的未经请求的包，以动态建立所述客户机和所述服务器之间的临时映射；并且其中如果确定所述未经请求的包中的所述唯一连接标识符与所存储的唯一连接标识符匹

配，则所述服务器可操作来使用所述动态建立的临时映射经由所述不受信任网络向所述客户机发送响应包，由此通过与所述客户机关联的所述 NAT 路由器建立所述服务器和所述客户机之间的安全连接。

24. 根据权利要求 23 所述的系统，其中所述服务器可操作来接收来自所述第三方计算机的所述客户机的目的地入站端口和与所述客户机关联的所述 NAT 路由器的公有地址；并且其中所述客户机可操作来接收来自所述第三方计算机的所述服务器的目的地端口和 IP 地址以及所述唯一连接标识符。

25. 根据权利要求 24 所述的系统，其中所述客户机可操作来接收来自所述第三方计算机的将所述未经请求的包发送到所述服务器的指令；并且其中如果确定在所述服务器的所述目的地端口上收到来自与所述客户机关联的所述 NAT 路由器的所述公有地址的所述未经请求的包，则所述服务器可操作来向所述客户机发送响应包。

26. 根据权利要求 23 所述的系统，其中所述服务器可操作来使用自所述第三方计算机接收的所述客户机的所述目的地入站端口发起到所述客户机的所述安全连接。

27. 根据权利要求 23 所述的系统，其中所述客户机是不执行任何用户功能或包含任何用户数据的无状态客户机。

28. 根据权利要求 23 所述的系统，其中所述客户机是单一功能网络感知的消费者设备。

29. 根据权利要求 28 所述的系统，其中所述单一功能网络感知的消费者设备是以下设备中的一种：蜂窝电话、音乐播放器/记录器、视频播放器/记录器、游戏播放器或便携式电子邮件设备。

30. 根据权利要求 23 所述的系统，其中所述客户机可操作来向所述第三方计算机发送连接请求，所述连接请求包括连接到所述服务器的请求。

31. 根据权利要求 30 所述的系统，其中所述客户机可操作来在所述

客户机通电时通过用户的单一动作、在连接到所述不受信任网络时、或所述客户机的网络参数发生任何变化时向所述第三方计算机自动发送所述连接请求，由此向所述客户机提供到所述服务器的单一动作接入。

自动发起和动态建立有防火墙的服务器和有防火墙的客户机之间的安全的因特网连接的系统和方法

相关申请

本申请要求 2004 年 4 月 12 日提交的美国临时专利申请 No. 60/561,806 的优先权，其全部内容通过参考结合于此。

技术领域

本发明涉及计算机组网和网络安全领域。更具体而言，本发明涉及自动且动态地发起和建立一个计算机（即服务器）和多个计算机（即客户机）之间的安全连接的方法，所述计算机中的每个计算机都在网络地址转换器路由器和/或防火墙之后。

背景技术

因特网在所连接的计算机数量上持续地经历快速的扩展，据估计，广泛可用的无线连接性和便携式计算设备的趋向将使得每天所连接的新计算机的数量呈指数地增加。这种快速扩展迅速提高了保护计算机免于受到未授权接入的损害的需要，并且已经开始导致因特网网络本身的许多可升级能力问题。例如，互联网协议版本 4（IPv4）使用 32 位 IP（互联网协议）地址，这意味着因特网上计算机的理论最大数量是大约 40 亿。然而，由于在如何分配和路由 IP 地址方面的低效，实际的极限值是非常低的。因此，IPv4 不能为当前因特网的扩展提供足够的唯一地址。较新版本的网络协议（IPv6）使用 128 位地址空间，并因此提供较大数量的 IP 地址，当然，在其被广泛采用以前，已使用其它技术来克服 IPv4 的地址限制并提供对因特网连接的计算机的安全保护。

现今广泛使用的一种这样的解决方案是网络地址转换（NAT），其

中仅当用户的计算机需要从内部网络伸出并连接到诸如，举例而言，Web服务器的公共因特网服务器时，才将内部网络，诸如 AOL 或其它因特网服务提供商（ISP）上所使用的私有地址转换成公有 IP 地址。假定任何一个时刻在因特网上通信的计算机的数量比连接但未激活的计算机的总数低得多，通过 NAT 仅向当前通信的计算机分配公有 IP 地址，由此降低了所需的 IP 地址数量。该方案还由于为 NAT 路由器或防火墙之后的计算机提供的匿名而提供了附加的安全性，通过从因特网发起的连接无法到达在 NAT 路由器或防火墙之后被提供匿名的计算机。

NAT 路由器主要围绕客户机/服务器模式来设计，这里，私有网络内的客户机发起到具有固定的 IP 地址和域名服务或服务器（DNS）名称的公用服务器的连接。

NAT 路由器之后的内部主机的匿名和不可访问性对于诸如 web 浏览器的客户机软件并不是问题，其只需要发起外出到公共可用的服务器的连接。然而，对于需要服务器通过穿过其 NAT 路由器的进入的连接安全地连接到客户机的应用，如文件共享、游戏应用、视频会议、IP 互联网承载语音电话，或者对于到不允许客户机从互联网直接连接到它们的计算机服务器的安全接入，这是个问题。

当这些计算机中的一个在 NAT 路由器之后时，如果不使用专门技术和连接类型、位置、服务或 NAT 路由器/防火墙类型的每个变化所需的通常是复杂的人工配置，其它计算机不能连接到该计算机。

因此，NAT 所建立的寻址和连接性的非对称特性的确产生了许多问题：a) 将广泛可用的互联网服务的安全性限制到仅出站的应用，如万维网；以及 b) 将潜在地对大消费者市场有吸引力的许多附加互联网应用和服务的可使用性和大量市场可用性限制到能够管理当前可用的 NAT 和 NAT 穿透技术强加的复杂的配置和系统管理要求的较小数量的专业训练的用户。

发明内容

因此，本发明的目的是提供克服上述缺点的自动发起和动态建立服务器和客户机之间的因特网连接的方法和系统。

根据本发明的一个实施例，所述方法和系统自动且动态地发起和建立服务器和有防火墙的客户设备（客户机）之间的连接，优选为受保护的连接，所述服务器和客户设备均通过网络地址转换器或转换（NAT）路由器或防火墙连接到不受信任的网络（如因特网）。本发明的安全连接的发起和建立无需在客户机上进行任何用户配置并且无需服务器接受来自客户机的任何直接的连接请求和/或包，由此有利地允许服务器防火墙对所有入站业务（inbound traffic）总是保持关闭。

本发明使得能够在因特网上创建动态实例化的虚拟点对点网络连接以根据需要安全地连接服务器和客户机，由此有利地以前所未有的易用性为一般用户提供对服务器的单一动作接入（如一次鼠标点击，或通电或网络插入动作）。

根据本发明的一个实施例，上述方法和系统利用服务器和客户机均独立信任的具有公有 IP 地址的第三计算机，例如受信任方，如会话控制服务器（SCS），作为中间方来安全地约定建立服务器和客户机之间的连接所需的连接参数，所述连接优选为安全连接。SCS 仅参与服务器/客户机连接建立，而不参与服务器和客户机之间的后续通信（即消息交换）。因此，本发明避免了与中继和在此讨论的其它基于服务器的技术关联的性能和安全问题。

客户机将包含其自身地址和随机产生的唯一标识符（针对到每个服务器的每个客户机连接请求是不同的）的连接请求发送到 SCS，由此向 SCS 提供了客户机的连接参数，否则这些连接参数会被 NAT 路由器和/或由防火墙隐藏。可将客户机编程为在通电时、连接到任何新的有 NAT 的网络时、其网络参数发生任何变化时总是自动执行该步骤，由此在无需任何用户配置或干预的情况下提供了与服务器的安全连接的自动

和动态发起/建立和重新建立。

然后 SCS 为客户机和服务器的每一个提供各自的连接参数，然后这些参数在它们之间安全地交换，使得首先客户机的连接参数被递送给服务器并被服务器唯一地识别，且最后在成功地完成先前步骤时，服务器通过客户机的 NAT 路由器或防火墙发起到客户机的安全连接，由此使得能够通过安全地克服客户机 NAT 路由器或防火墙强加的入站业务限制而建立外部发起的连接，并且允许服务器保持其自己的 NAT 路由器/防火墙对所有来自不受信任网络的入站业务关闭。

根据本发明的一个实施例，一种用于自动发起和动态建立经由不受信任网络的安全连接的系统包括：客户设备，通过防火墙或网络地址转换器（NAT）路由器连接到不受信任网络；服务器，通过防火墙连接到不受信任网络并且不接受来自任何客户设备的直接的连接请求或包；以及受信任计算机，连接到不受信任网络，用于在服务器和客户设备之间交换连接参数而无需对客户设备进行配置。客户设备经由受信任计算机接收来自服务器的唯一连接标识符。服务器的防火墙从客户设备接收包括所述唯一连接标识符的未经请求的包以动态建立客户设备和服务器之间的临时映射。如果自客户设备接收的未经请求的包中的唯一连接标识符与所存储的唯一连接标识符匹配，则服务器使用动态建立的临时映射经由不受信任网络向客户设备发送响应包，由此通过 NAT 路由器建立服务器和客户设备之间的安全连接。

为了理解本发明，必需理解即使利用计算机安全方面的所有进步，因特网仍然是固有地不安全的环境，因为难以使“易用性”问题和受信任的接入单元相协调。通过提供消除了欺骗性用户假扮合法用户的可能性的方法途径，本发明切中问题的要害，同时本发明没有增加、而事实上是消除了一般用户会觉得是负担的许多单元。

以上相当广泛地概括了本发明的特点和技术优点以便于较好地理解以下对本发明的详述。以下将描述本发明的附加特点和优点，其形成

了本发明的权利要求的主题。本领域的技术人员应理解，所公开的特定概念和实施例可以容易地用作修改或设计实现本发明的相同目的的其它结构的基础。本领域的技术人员亦应认识到，这样的等同构造并不背离在所附权利要求中所提出的本发明的实质和范围。结合附图考虑以下描述将会更好地理解被认为是本发明特性的，关于其组织和操作方法的新特征，以及进一步的目的和优点。然而，应当清楚地理解，每个图都仅用来图示和描述，而并非对本发明的限制。

附图说明

可参照在此通过举例给出且并非意图使本发明仅限于此的描述来理解本发明，而结合附图可得到对本发明的最佳理解，在附图中：

图 1 是示出在 NAT 或防火墙之后的连接到不受信任网络的各个计算机的示例性框图；并且

图 2-8 是示出根据本发明的一个实施例自动发起和动态建立服务器和客户机之间的连接的步骤的示例性框图， 其中，服务器和客户机的每一个均处于防火墙或 NAT 路由器之后。

具体实施方式

根据本发明的一个实施例，所述系统和方法自动且动态地发起并建立服务器和有防火墙的客户设备之间的连接，优选为安全连接。现在转到图 1，所示为服务器 1100 和客户设备（客户机 1200），两者通过网络地址转换器或转换（NAT）路由器或防火墙 1300 连接到不受信任网络 1000（如因特网）。服务器和客户机之间的连接在不要求在客户机 1200 上进行任何用户配置并且服务器 1100 未接受来自客户机 1200 的任何直接的连接请求和/或包的情况下被发起和建立，由此允许服务器防火墙 1300 对所有入站业务总是保持关闭。

根据一个实施例，本发明利用具有公有 IP 地址的第三计算机 1400，

例如诸如会话控制服务器（SCS）的受信任方，该第三计算机 1400 被服务器 1100 和客户机 1200 两者独立地信任且安全地连接到该两者。客户机 1200 将包括其自身地址和随机产生的唯一标识符（针对向服务器的每个客户机连接请求是不同的）的连接请求发送到 SCS 1400，由此向 SCS 1400 提供客户机的连接参数，否则这些连接参数会由 NAT 路由器 1300 和/或由防火墙 1300 隐藏。根据本发明的一个方面，可将客户机 1200 编程为在通电时、连接到任何新的有 NAT 的网络时、其网络参数发生任何变化时总是自动执行该步骤，由此提供与服务器 1100 的安全连接的自动和动态发起/建立和重新建立，而无需任何用户配置或干预。

SCS 1400 为客户机 1200 和服务器 1100 的每一个提供各自的连接参数，然后这些参数在它们之间安全地交换，使得首先客户机的连接参数递送给服务器 1100 并被服务器 1100 唯一地识别，且最后在成功地完成先前步骤时，服务器 1100 通过客户机的 NAT 路由器或防火墙 1300 发起到客户机 1200 的安全连接，由此使得能够通过安全地克服客户机 NAT 路由器或防火墙 1300 强加的入站业务限制而建立外部发起的连接，并且允许服务器 1100 保持其自己的 NAT 路由器/防火墙 1300 对来自不受信任网络的所有入站业务关闭。

SCS 仅参与服务器/客户机连接建立，而不参与服务器和客户机之间的后续通信（即消息交换）。因此，本发明避免了与中继和其它基于服务器的技术关联的性能和安全问题。

中继技术是客户机-服务器通信的一种改变形式，并且依赖于两个客户机，所述两个客户机使用它们两者都可连接到的、具有公有 IP 地址的服务器。NAT 路由器之后的这两个客户机彼此之间不能进行直接连接，但每一个可与具有公有 IP 地址的服务器进行连接。该服务器然后充当中继并且将消息从一个客户机转发到另一个客户机。该方法的缺点在于，由于依赖服务器来中继客户机之间的所有通信，其需要使用服务器的可用处理能力和可用网络带宽来连接客户机，因此其性能和可升级能

力性依赖于这些参数。此外，不断地在服务器上进行客户机间数据通信的拷贝，由此会产生附加的安全威胁。

UDP 穿孔技术基于允许应用 “穿孔”通过 NAT 路由器并且建立彼此之间的直接连接的防火墙的一般特性。

根据本发明的一个示例性实施例，以下描述用于自动发起和建立 NAT 路由器或防火墙 1300 之后的服务器 1100 和客户机 1200 之间的经由不受信任网络 1000 的安全连接的系统、方法和计算机指令。应理解在此描述的所有交互都发生在诸如因特网的不受信任网络 1100 上。亦应理解，在此描述的所有交互可能发生在非安全连接上。现在结合图 2-8 描述根据本发明一个示例性实施例的到服务器 1100 的自动和动态客户侧连接。

如图 2 所示，在步骤 2000，服务器 1100 发起和建立（或永久保持）到 SCS 1400 的安全连接。根据本发明的一个方面，该连接可在诸如具有 IPSEC 的网络工作层（OSI 层 3）上形成。根据本发明的另一个方面，该安全连接可使用诸如具有安全套接层（SSL）的应用层（OSI 层 7）机制。服务器 1100 和 SCS 1400 之间的所有后续通信都可以在该安全通信信道上进行。

如图 3 所述，在步骤 2010，客户机 1200 发起与 SCS 1400 的安全连接。根据本发明的一个方面，该安全连接可使用诸如具有安全套接层（SSL）的应用层（OSI 层 7）机制。客户机 1200 和 SCS 1400 之间的所有后续通信都可以在该安全通信通道上进行。

如图 4 所示，在步骤 2020，客户机 1200 向 SCS 1400 发送请求以便被连接到期望的服务器 1100。这可以是诸如用户请求的客户机发起事件的结果，或者可将客户机 1200 编程为在通电时、连接到任何新的有 NAT 的网络时、其网络参数发生任何变化时总是自动执行该步骤，由此提供与服务器 1100 的安全连接的自动和动态发起/建立和重新建立，而无需任何用户配置或干预。

在步骤2030，SCS 1400向服务器发送包括指定目的地入站端口、客户机NAT公有地址的唯一标签，并且从服务器1400接收随机产生的连接标识符（ID）。应理解，根据本发明的一个实施例，服务器1100所提供的目的地入站端口在发起、建立和使用与客户机1200的安全连接的整个过程中保持关闭。如图5所示，通过使用该SCS提供的信息，服务器1100对将可能由服务器1100建立的到客户机1200的连接的其自己的一端进行配置。该配置的特性依赖于将建立的安全连接的特性，然而通常会涉及一些密钥产生和交换。例如，根据本发明的一个方面，该安全连接可在诸如具有IPSEC的网络工作层（OSI层3）上形成。根据本发明的另一个方面，该安全连接可使用诸如具有安全套接层（SSL）的应用层（OSI层7）机制。

如图6所示，在步骤2040，SCS 1400指示客户机1200将包含所述ID的未经请求的UDP或TCP包发送到服务器提供的IP地址和目的地端口。SCS 1400对将可能由服务器1100建立的到客户机1200的安全连接的客户机端进行配置。对于客户机侧，该配置的特性依赖于将形成的安全连接的特性，然而通常会涉及一些密钥产生和交换。例如，根据本发明的一个方面，该安全连接可使用诸如具有安全套接层（SSL）的应用层（OSI层7）机制。

在步骤2050，客户机1200将UDP或TCP包发送到SCS 1400所提供的服务器IP地址和目的地端口。应理解服务器1100和服务器的防火墙1300仍保持对客户机1200关闭。由此，在步骤2050，在客户机NAT路由器1300中建立客户机1200和服务器1100之间的临时映射。该映射包括客户机的真实IP地址和源端口（私有侧）和NAT假扮的客户机IP地址和源端口（公有侧）之间的转换。在形成之后，该映射将在一小段时间内保持有效，由此允许服务器1100在已经创建的映射的指定的时间帧内根据那个映射直接连接到客户机1200。

在步骤2050，服务器的防火墙1300看见所述UDP或TCP包，将

其中的 ID 和 NAT 公有地址与它从 SCS 1400 接收到的 ID 和 NAT 公有地址进行比较。如果匹配，则服务器的防火墙 1300 向服务器 1100 通知该事件。在步骤 2050，服务器的防火墙 1300 则总是丢掉未经请求的包，即该包从不进入服务器的 IP 堆栈，如图 7 所述。服务器的防火墙 1300 继续检查指定目的地端口上的进入包以察看它们是否为询问包。根据本发明的一个实施例，服务器的防火墙 1300 检查标签的所有三个元素以提防安全攻击，如冒充真实客户机 1200 的主机的连接请求。服务器的防火墙 1300 将仅考虑来自 NAT 公有地址、去往指定目的地端口并且包含随机生成的 ID 的包。作为进一步的安全保证，作为该技术的一部分，可对 UDP/TCP 包进行加密。

在步骤 2060，服务器 1100 使用由服务器的防火墙 1300 转发的源端口来发起到客户机 1200 的 UDP 或 TCP 连接。应理解，在步骤 2050 创建的 NAT 映射保持合理的一段时间（在收到 UDP 或 TCP 包后至少几秒钟，当然可能更长）。根据本发明的一个方面，参见图 8，在步骤 2060，服务器 1100 可以以此方式通过 NAT 连接到客户机。

本领域的技术人员将理解，客户机 1200 在其网络地址参数变化时，如在客户机 1200 移动到不同的连接位置时，将自动地连接以及动态地重新连接到服务器 1100，除了单一用户动作如通电、一次鼠标点击或一次键击以外无需任何用户干预。因此，应理解，借助于本发明的实施例，将客户机 1200 连接到服务器 1100 不要求客户机 1200 知道任何用户信息或处理或执行任何用户功能。

举例来说，根据本发明的一个实施例，人们将理解本发明适用于通过 TCP/SSL 建立服务器 1100 和无状态客户机 1200 之间经由互联网的安全连接。无状态客户机 1200 通常定义为不执行任何用户功能或包含任何用户数据的计算机。更确切地，无状态客户机 1200 可构建为包括 CPU、存储器、帧缓冲器和网络端口、鼠标和键盘输入和可选的 IO 端口的网络设备。它由内置的软件来操作，仅执行网络和显示管理固定功能，且

不允许任何对其它软件的下载或执行。它不运行任何应用程序。其唯一的用途是作为远程人接口设备。所述内置软件实现网络堆栈以允许经由类似因特网的网络与服务器通信。

客户机的无状态性是在于人与应用交互的情景，或所有的执行都是在服务器侧进行的计算环境。在任何时刻都没有应用状态或数据驻留在客户机中。它所具有的唯一状态具有临时特性并且与网络连接性有关，即 TCP 连接状态。根据一个实施例，本发明仅使用在 TCP 上实现安全套接层（SSL）的无状态客户机的网络堆栈，如在此详细描述的，并因此实现了在任何情况下不能执行任何用户功能的无状态客户机 1200 和服务器 1100 之间的安全连接的自动和动态建立。

无状态客户机 1200 经由 TCP/SSL 自动连接到 SCS 1400 并且通过新建立的连接发送所请求的服务器 1100 的名称。

SCS 1400 检测来自套接连接的无状态客户机 IP 地址。SCS 1400 读取所请求的服务器名称并确定其是否具有到所需服务器 1100 的连接。如果 SCS 1400 没有这样的到所需服务器 1100 的连接，则 SCS 1400 或者等待直到它获得这样的连接，或者指示无状态客户机 1200 稍后重试。如果服务器 1100 连接到 SCS 1400，则 SCS 1400 将无状态客户机 IP 地址发送到服务器 1100。服务器 1100 读取该无状态客户机地址，生成唯一的 32 位随机数标识符（所述 ID）并且将该 ID 连同其 IP 地址和端口发送到 SCS 1400。然后服务器 1100 指示其防火墙 1300 探测具有设置给所述 ID 的值的初始序列号的来自无状态客户机的公有 IP 地址的“TCP SYN”（TCP 连接请求）包。

同时，SCS 1400 将服务器 IP 地址、端口和 ID 转发到无状态客户机 1200。此时，无状态客户机 1200 产生到服务器 IP 地址和端口的未经请求的 TCP 连接请求，该请求具有设置给所述 ID 的值的初始序列号。该外出的包将准备（prime）在去往服务器 1100 的途中的任何 NAT，并且还将服务器 IP 地址和端口以及所述 ID 保存在无状态客户机的网络堆

栈的底部的 SEQ 转换器层中。一旦这样的包到达服务器 1100，服务器的防火墙 1300 就查找匹配并且执行以下三个任务：a) 存储无状态客户机地址/端口、服务器地址/端口和序列号；b) 通知服务器 1100 并提供无状态客户机公用端口；以及 c) 丢掉该包。

现在服务器 1100 打开将穿过服务器防火墙 1300 的到无状态客户机 IP/端口的 TCP 连接。服务器的防火墙 1300 看见外出 TCP 连接请求（设置 SYN 旗标），找到匹配并且设置 TCP ACK 旗标和确认号。在外部，应理解该包看起来象是对自无状态客户机 1200 接收的未经请求的 TCP 连接请求的响应，并且它通过 NAT 网关传送回到无状态客户机 1200。

在此包到达无状态客户机 1200 时，SEQ 转换器层对该包进行匹配并且删除 TCP ACK 旗标，使得无状态客户机 TCP 堆栈看到来自服务器 1100 的实际连接请求。

无状态客户机 TCP 堆栈接受该连接，并以具有 SYN 和 ACK 旗标设置两者的 TCP 包做出响应。该 TCP 包被删除了 SYN 旗标并存储了无状态客户机序列号和先前存储的 ID 之间的差异的 SEQ 转换器层来匹配。应理解在网络上，该 TCP 包看起来象是 TCP 3-向握手的第三方。

当来自无状态客户机 1200 的 TCP 包到达服务器的防火墙 1300 时，对该 TCP 包进行匹配并且设置 SYN 旗标。该 TCP 包穿过服务器的防火墙 1300，因为它是对连接请求的响应。来自服务器 1100 的实际第三 TCP 握手包没有变化地穿过，因为它被当做正常的确认包。在无状态客户机 1200，每个到达的包获得通过先前存储的序列差异调整的其确认号，并且每个外出的包获得通过该差异调整的其序列号。应理解在服务器 110 和无状态客户机 1200 之间的连接的终结时专门的旗标毁坏（flag mangling）并非必需。

尽管已详细描述了本发明及其优点，应理解可在所附权利要求限定的精神和范围内对本发明进行各种变化、替换和更改。而且，本发明

的范围并不是想要局限于说明书中所描述的过程、机器、制造、物质组成、装置、方法和步骤的特定实施例。根据本发明的公开内容，本领域的技术人员将理解，可根据本发明来利用现有或以后开发的执行与在此描述的对应实施例基本相同的功能或实现与其基本相同的结果的过程、机器、制造、物质组成、装置、方法或步骤。因此，所附权利要求意图在于在其范围内包括这样的过程、机器、制造、物质组成、装置、方法或步骤。

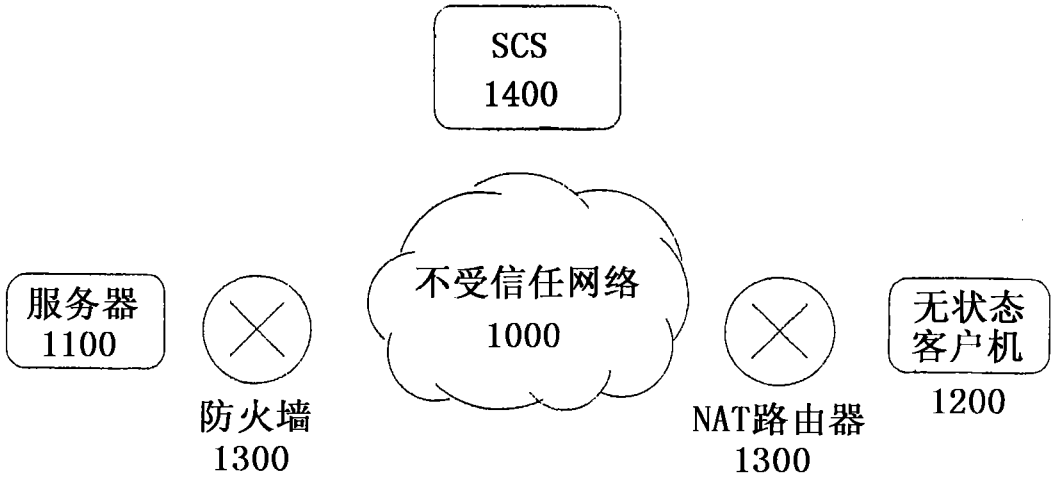

SCS
1400
不受信任网络
1000
服务器
1100
防火墙
1300
NAT路由器
1300
无状态
客户机
1200

图1

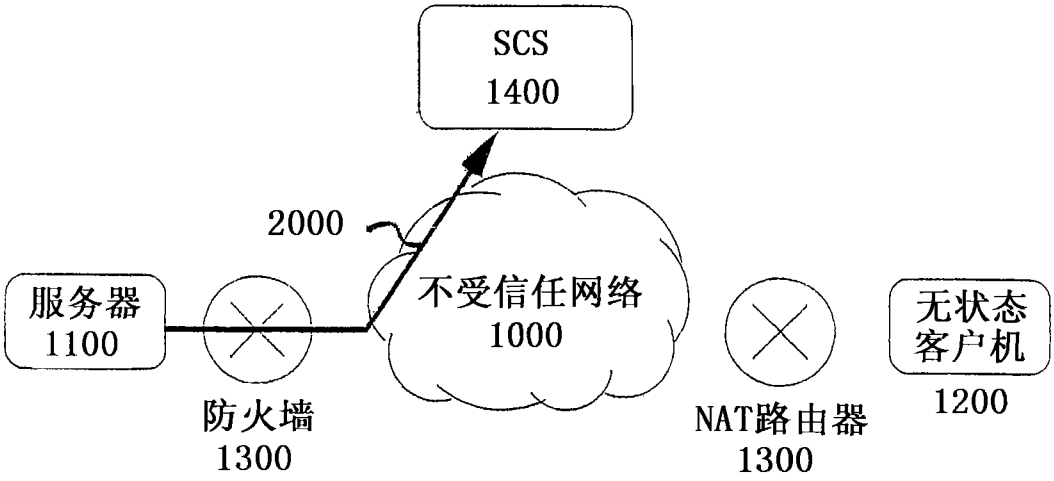

SCS
1400
2000
不受信任网络
1000
服务器
1100
防火墙
1300
NAT路由器
1300
无状态
客户机
1200

图2

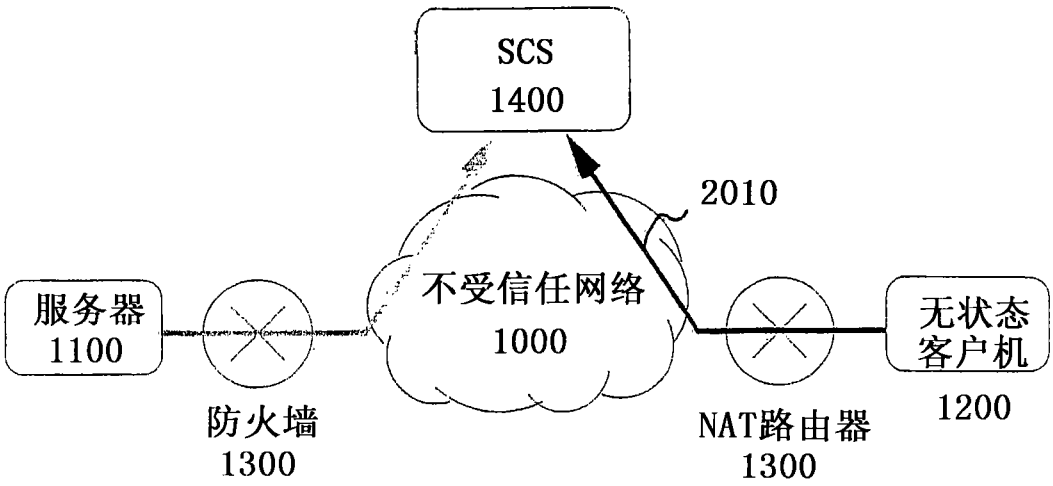

SCS
1400
2010
不受信任网络
1000
服务器
1100
防火墙
1300
NAT路由器
1300
无状态
客户机
1200

图3

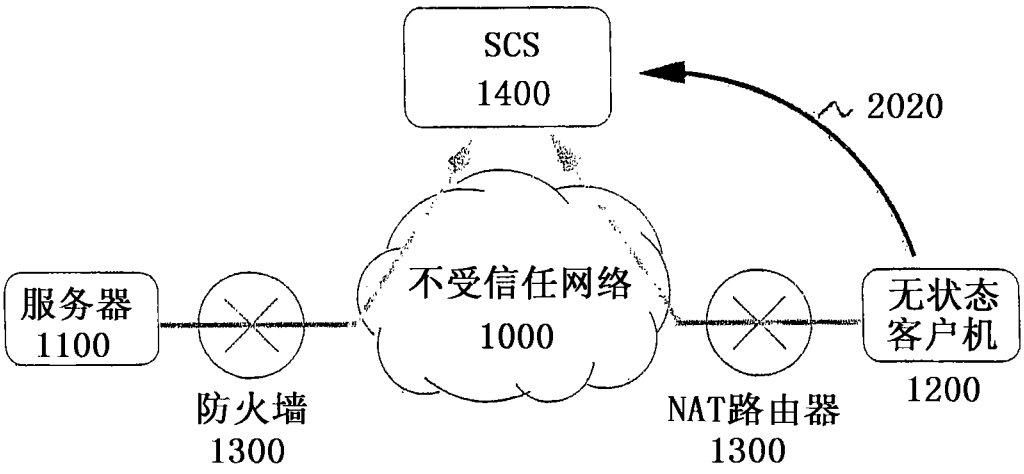

SCS
1400
2020
不受信任网络
1000
服务器
1100
防火墙
1300
NAT路由器
1300
无状态
客户机
1200

图4

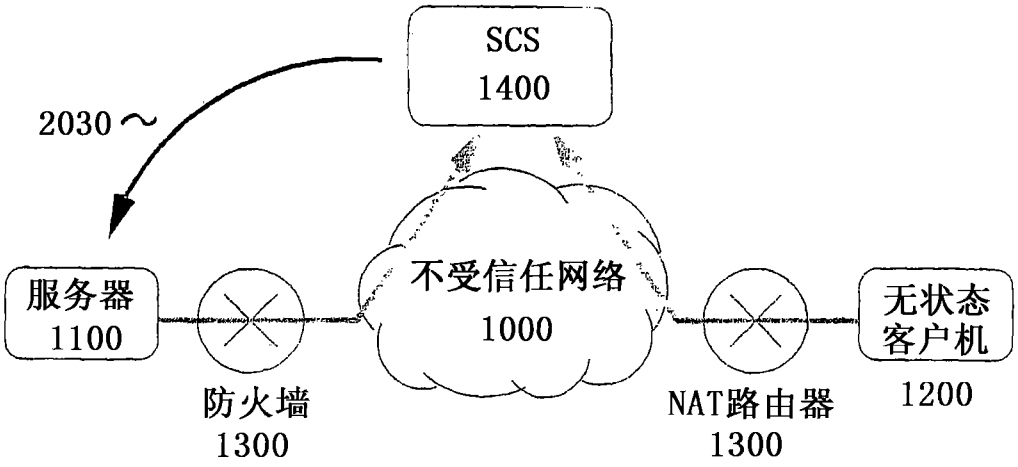

SCS
1400
2030
服务器
1100
不受信任网络
1000
无状态
客户机
1200
防火墙
1300
NAT路由器
1300

图5

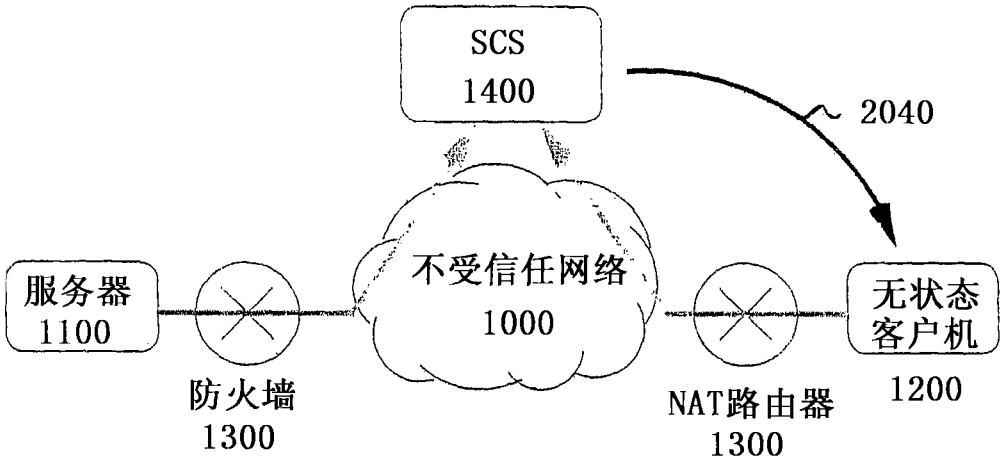

SCS
1400
2040
服务器
1100
不受信任网络
1000
无状态
客户机
1200
防火墙
1300
NAT路由器
1300

图6

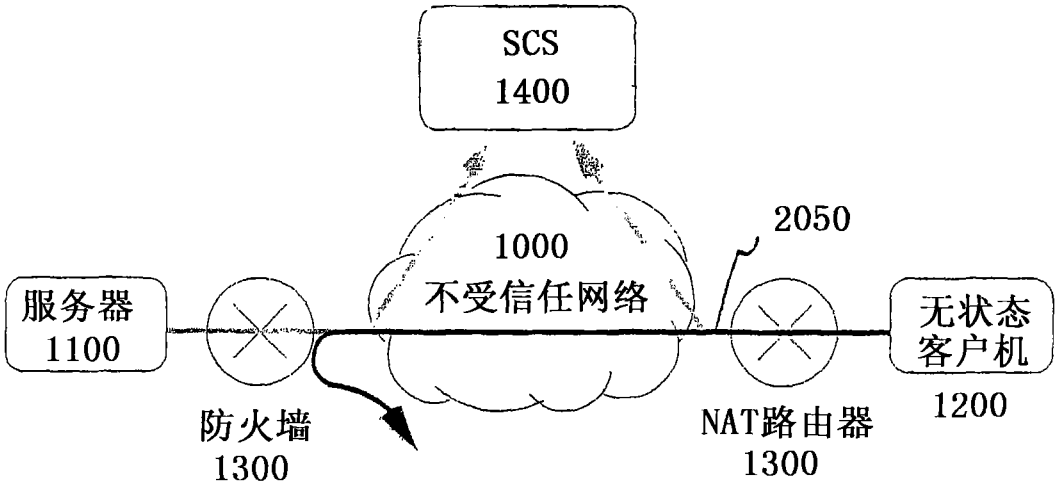

SCS
1400
1000
不受信任网络
2050
服务器
1100
防火墙
1300
NAT路由器
1300
无状态
客户机
1200

图7

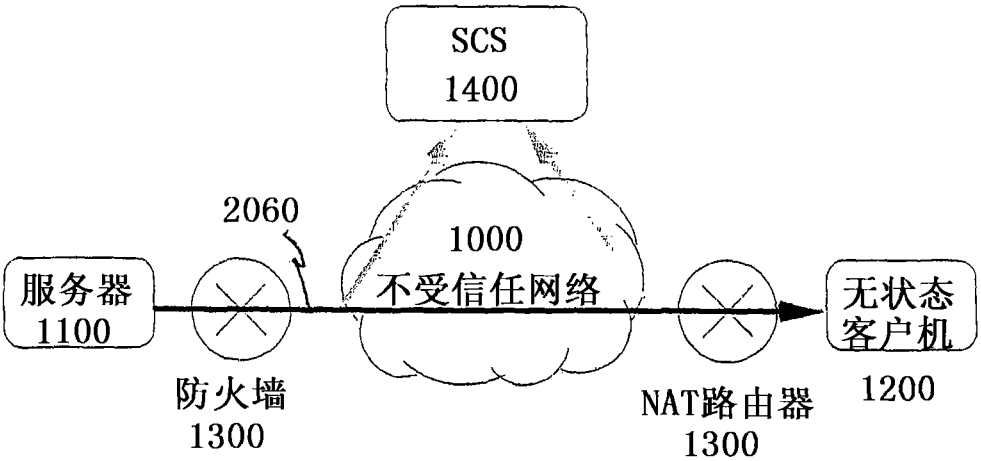

SCS
1400
2060
1000
不受信任网络
服务器
1100
防火墙
1300
NAT路由器
1300
无状态
客户机
1200

图8