[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/24 (2006.01)

[12] 发明专利说明书

专利号 ZL 200410061885.2

[45] 授权公告日 2009 年 6 月 10 日

[11] 授权公告号 CN 100499487C

[22] 申请日 2004.6.25
[21] 申请号 200410061885.2
[30] 优先权
[32] 2003. 6.25 [33] US [31] 10/603，648
[73] 专利权人 微软公司
地址 美国华盛顿州
[72] 发明人 D·莫根 A·加弗里莱斯库
J·L·布尔斯泰因 A·舍莱斯特
D·莱布兰克
[56] 参考文献
US5987611A 1999.11.16
CN1201573A 1998.12.9
US2004003290A1 2004.1.1
US6584508B1 2003.6.24
审查员 罗芳洁

[74] 专利代理机构 上海专利商标事务所有限公司
代理人 陈 斌

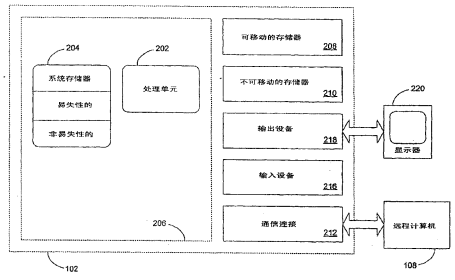
权利要求书 3 页 说明书 15 页 附图 9 页

[54] 发明名称

帮助应用穿越防火墙的方法

[57] 摘要

一种用于察觉性防火墙的应用的方法，它将其期望传送给防火墙而不需要防火墙改变其策略或危及网络安全。 为应用软件提供应用 API 来将应用的需求通知一个或多个防火墙，并提供将应用的需求通知一个或多个防火墙的防火墙 API。 拦截模块监视由应用和服务对本地计算机上的网络堆栈的连接和监听尝试。 拦截模块捕获这些尝试并确定什么用户在进行尝试、什么应用或服务在进行尝试，并实施防火墙策略查找来确定是否允许该用户和/或应用或服务连接到网络。 如果这样，拦截模块可命令主机和/或边界防火墙为所请求的连接配置自己。



1.一种计算机实现的方法，其特征在于，包括：

由操作系统和/或与所述操作系统关联的或是所述操作系统的一部分的实施模块通过第一应用编程接口从应用接收调用，所述调用具有参数用于所述应用想要建立的、至一个端点的连接；

通过所述操作系统和/或所述实施模块从所述应用接收一个指示，所述指示表示所述应用想要建立所述连接，所述指示包括由所述应用创建套接字和绑定所述套接字；以及

由所述操作系统和/或所述实施模块通过第二应用程序接口对防火墙进行调用，以按照所述参数建立所述连接。

2.如权利要求1所述的方法，其特征在于，还包括，在所述防火墙，以相关策略评估所述参数，并且如果所述参数符合所述策略，按照所述参数建立所述网络连接。

3.如权利要求1所述的方法，其特征在于，所述参数包括所述应用愿意被连接到的已知端点。

4.如权利要求3所述的方法，其特征在于，所述参数还包括将所述连接限制于一个单一连接的请求。

5.如权利要求4所述的方法，其特征在于，还包括，在已经建立所述连接之后，按照所述请求关闭所述连接。

6.如权利要求1所述的方法，其特征在于，所述参数包括对用于所述连接的带宽或连接节流的请求。

7.如权利要求1所述的方法，其特征在于，所述参数将所述连接限制于接口、本地地址或远程地址或它们的组合的一个子集。

8.如权利要求1所述的方法，其特征在于，所述参数包括用于所述连接的超时策略。

9.如权利要求1所述的方法，其特征在于，所述参数包括关闭或打开特定的协议选项。

10.如权利要求1所述的方法，其特征在于，所述参数包括与请求特别处理的流程的属性有关的信息。

11.如权利要求10所述的方法，其特征在于，所述信息包括对认证或加密

的请求。

12.如权利要求 1 所述的方法，其特征在于，所述指示包括打开一监听套接字。

13.如权利要求 1 所述的方法，其特征在于，所述指示包括连接至一套接字。

14.如权利要求 1 所述的方法，其特征在于，所述对防火墙的调用是通过防火墙应用编程接口进行的。

15.如权利要求 1 所述的方法，其特征在于，所述防火墙位于具有所述应用的计算机上。

16.如权利要求 1 所述的方法，其特征在于，所述防火墙包括一边界防火墙，并且还包括一个代理以将有关所述连接的信息传送至所述边界防火墙。

17.如权利要求 1 所述的方法，其特征在于，所述防火墙包括一边界防火墙，并且还包括一个认证过的协议以将有关所述连接的信息传送至所述边界防火墙。

18.一种计算机实现的方法，其特征在于，包括：

建立用于至端点的连接的策略；

通过被包括在与操作系统相关联的或是所述操作系统的一部分的实施模块内的拦截模块从一应用或一服务接收一连接尝试、一监听尝试或它们的组合；

通过所述拦截模块从所述连接尝试、所述监听尝试或所述它们的组合提取用户和应用或服务信息；

通过所述拦截模块从用户和应用或服务信息中识别用户和所述应用或所述服务；

通过所述拦截模块评估所述应用或服务信息以确定所述连接尝试、所述监听尝试或者所述它们的组合是否与多个策略中的一个或多个策略一致；以及

如果所述连接尝试、所述监听尝试或者所述它们的组合与所述多个策略中的一个或多个策略一致，则通过所述拦截模块配置防火墙以允许所述连接尝试、所述监听尝试或者所述它们的组合。

19.如权利要求 18 所述的方法，其特征在于，还包括，如果所述连接尝试、所述监听尝试或者所述它们的组合与所述多个策略中的一个或多个策略不一致，发送通知至所述应用或服务的用户。

20. 如权利要求 19 所述的方法，其特征在于，所述通知包括允许所述连接的选择。

21. 如权利要求 18 所述的方法，其特征在于，所述建立所述策略的步骤包括从所述应用或服务接收一个策略。

22. 如权利要求 21 所述的方法，其特征在于，其中接收所述策略的步骤包括通过应用编程接口接收所述策略。

23. 如权利要求 21 所述的方法，其特征在于，从所述应用或服务接收的所述策略包括使用一个或多个因特网协议地址、关于子网的信息、关于所述连接的范围的信息或它们的组合的入网或出网限制。

24. 如权利要求 21 所述的方法，其特征在于，从所述应用或服务接收的所述策略包括通信安全级别。

25. 如权利要求 24 所述的方法，其特征在于，所述通信安全级别包括认证。

26. 如权利要求 24 所述的方法，其特征在于，所述通信安全级别包括加密。

27. 如权利要求 18 所述的方法，其特征在于，所述防火墙包括位于具有所述应用的计算机上的主机防火墙。

28. 如权利要求 18 所述的方法，其特征在于，所述防火墙包括一边界防火墙，并且还包括一代理以传送有关所述连接的信息。

29. 如权利要求 18 所述的方法，其特征在于，所述防火墙包括一边界防火墙，并且还包括一认证过的协议以将有关所述连接的信息传送至所述边界防火墙。

帮助应用穿越防火墙的方法

技术领域

本发明通常涉及计算机或网络上的安全性，特别涉及防火墙及其与应用有关的使用。

背景技术

通常，防火墙是防止未经授权的用户访问网络或计算机上的某些文件的电子边界。可以作为用户计算机上的防火墙代码(“主机防火墙”)来提供防火墙。可供选择地，还可在网络边缘提供专用防火墙机构(“边界防火墙”)，它与网络外的计算机接口并具有内建的特殊安全预防措施，以便保护网络内计算机上的敏感文件。这个想法就是要保护一群较松散管理的机器，使它们对于网络外计算机用户是隐藏在边界防火墙之后的。边界防火墙所位于的机器常常称为“网关”或“专用网关”。如果配置用于保护网络不受因特网侵害，该机器常常称为“因特网网关设备”。

防火墙使用至少三种不同方法中的一个或多个来控制进出网络的通信流。在第一个方法中，称为静态信息包过滤，依靠一组过滤器来分析信息包。由过滤器批准的信息包被送往请求系统；所有其它的信息包被丢弃。在第二个方法中，称为代理服务，由防火墙从因特网取回信息，对照策略来评估信息，随后送往请求系统，反之亦然。在较新的第三种方法中，称为全状态检查(stateful inspection)，不检查信息包内容，而是将信息包的关键部分与可信信息(trusted information)数据库比较。对从防火墙内部向外部的传播的信息以特殊定义的特征监控，然后将流入信息与这些特征比较。如果比较产生了合理的匹配，则允许信息通过。否则它被丢弃。

防火墙是可定制的，意味着可根据若干条件添加或删除过滤器。作为例子，因特网协议(“IP”)地址可用来限制或阻止通信。作为例子，如果网络外部的某个 IP 地址正从服务器读取过多的文件，则防火墙可以阻塞所有到和/或从那个地址的通信。作为另一个例子，防火墙可阻塞所有对某个域名的访问，或只允许对特定域名的访问。作为又一个例子，公司可能设置一个网络，其中只有一

台或两台机器处理一个或多个特定协议，并在所有其它机器上禁止那些协议。还有另一个例子是使用端口来限制通信。例如，如果服务器机器正运行着Web(HTTP)服务器和FTP服务器，则Web服务器一般在端口80可用，而FTP服务器在端口21可用。公司可能在网络上除一台之外的所有机器上阻止端口21的访问。

因而，防火墙通过检查网络通信并只允许与已在防火墙内设置的策略一致的通信来确保安全。但是，尽管上述的通信控制方法用于过滤某些通信时工作良好，但为防火墙设置的规则或策略可能并不符合网络内一些应用的需求。因为防火墙不能具有所有现有和将来的应用的全部知识，所以防火墙执行试探法来区分安全的通信和潜在危险的通信。例如，防火墙可选择允许从可信网络内发起的连接，但不允许那些从可信网络外部发起的连接(例如，从因特网发起的)。

尽管试探法简化了防火墙策略设计，但一些应用与防火墙试探法不一致。结果，由这样一个应用来通信的尝试将失败，促使防火墙设计者实现和测试用于各个和每个失败的应用的专用工作环境。这些工作环境增加了防火墙复杂性和代码难度。

最近努力设计的防火墙控制协议("FCP")由于基本安全冲突而没有成功，该协议允许应用在专设的基础上修改防火墙策略。防火墙策略是由可信实体(例如，网络管理员)创建和管理的，而应用可能运行在不可信节点或端点上。允许不可信应用修改公司网络策略与防火墙的安全目标是不一致的。

发明概述

为了提供本发明的基本理解，以下提出了本发明一些实施例的简略概述。这个概述不是本发明的广泛概览。并不期望确定本发明的关键/重要元素或描述本发明的范围。它的唯一目的是以简化形式提出本发明的一些实施例作为稍后提出的更为详细的描述的序言。

按照本发明的一个实施例，提供了一种用于察觉性防火墙应用的方法，它将其期望传达给防火墙而不需要防火墙改变其策略或危及网络安全的方法。为此目的，可为应用程序提供应用应用编程接口("API")来将应用的需求通知一个或多个防火墙，描述它们当前或预期的活动，并描述对由应用发送或接收的网络数据的处理要求。

按照本发明的另一个实施例，提供了将应用的需求通知一个或多个防火墙的防火墙 API。应用 API 和防火墙 API 可通过作为例如计算机系统的操作系统的一部分提供的网络子系统来交互。

按照本发明的另一个实施例，提供实施模块以允许用户创建简单的防火墙策略或网络访问策略来允许或拒绝他们计算机上的非察觉性防火墙的应用和服务连接到网络。另外，实施模块允许这些策略是在每用户基础上的。用户不需要了解或使用用于端口、协议或 IP 地址的规则来使应用能够通过防火墙。为此目的，提供了套接字应用编程接口，它允许应用或服务用 IP 地址、子网信息或连接范围来描述其关于入网或出网限制的需求。用户还可定义通信安全级别(例如，认证和/或加密)。

按照本发明的另一个实施例，实施模块允许应用通过防火墙的透明穿越。实施模块包括拦截模块，它监视应用和服务对本地计算机上的网络堆栈的连接和监听尝试。拦截模块捕获这些尝试并确定什么用户在进行尝试、什么应用或服务在进行尝试，并实施防火墙策略查找来确定是否允许用户和/或应用或服务连接到网络。如果这样，拦截模块可命令主机和/或边界防火墙为所请求的连接配置自己。

本发明的其它特征在结合附图从以下详细描述中将变得显而易见，这些附图为：

附图说明

图 1 是说明由网络连接的计算机的示意图；

图 2 是示意图，概括地说明可用于实现本发明实施例的示例性计算机系统。

图 3 是方框图，说明可按照本发明实施例使用的图 2 计算机系统的结构细节；

图 4 所示的是流程图，说明察觉性防火墙的应用请求从诸如远程计算机之类的一个已知端点接收单一连接的过程的一个例子；

图 5 所示的是方框图，概括地表示图 2 计算机系统的部件及其与按照本发明实施例的拦截模块的交互；

图 6 所示的是方框图，示出图 5 的拦截模块的一般部件；

图 7 所示的是按照本发明的一个实施例可在失败的连接尝试后呈现给用户

的用户界面；

图 8 所示的是流程图，说明图 5 的拦截模块如何能够允许非察觉性防火墙的应用穿越防火墙的例子；以及

图 9 所示的是流程图，说明服务或应用如何能够将服务的网络需求通知防火墙代码和/或边界防火墙。

详细描述

在下列描述中，将描述本发明的各种实施例。为了说明，阐述了特定的配置和细节，以便提供实施例的彻底理解。但是，对于本领域的一个熟练技术人员而言，可以在没有这些特定细节的情况下实现本发明也是显而易见的。而且，为了突出所述实施例，可省略或简化众所周知的特征。

在进行本发明各种实施例的描述之前，先提供在其中本发明的各种实施例可以实现的计算机和网络环境的描述。尽管不是必要的，但本发明将在由计算机执行的诸如程序模块的计算机可执行指令通用环境中描述。通常，程序包括执行特定任务或实现特定抽象数据类型的例程、对象、组件、数据结构等等。这里所用的术语“程序”或“模块”可指单个程序模块或共同行动的多个程序模块。这里所用的术语“计算机”和“计算设备”包括任何以电子方式执行一个或多个程序的设备，诸如个人计算机(PC)、手持设备、多处理器系统、基于微处理器的可编程消费电子产品、网络 PC、小型机、板式 PC、膝上型计算机、具有微处理器或微控制器的消费用具、路由器、网关、集线器等等。本发明还可在分布式计算环境中使用，其中任务由通过通信网络链接的远程处理设备执行。在分布式计算环境中，程序可位于本地和远程两者的存储器设备中。

参考图 1 描述适合于结合本发明各方面的计算机网络环境的例子。示例计算机网络环境包括通过用云表示的安全网络 104 而彼此通信的若干计算机 102。安全网络 104 可包括许多众所周知的组件，诸如路由器、网关、集线器等，并允许计算机 102 通过有线和/或无线介质通信。当通过安全网络 104 彼此交互时，一个或多个计算机 102 可用作客户机、服务器或相对于其它计算机 102 的对等机。因而，本发明的各种实施例可在客户机、服务器、对等机或它们的组合上实现，尽管这里所包含的特定例子可能不引用所有这些类型的计算机。

这个例子中的安全网络 104 被认为是“安全的”网络，其中计算机 102 由通用的防火墙保护，在此例中被示为因特网网关设备 106。因特网网关设备 106

保护计算机 102 不受位于在此例中用云表示的公共或不安全网络 110 上的远程计算机 108 的侵害。尽管被描述为因特网网关设备 106，但这个网关设备可保护安全网络不受其它类型的不安全网络的侵害，不一定是因特网，还包括 LAN、WAN 或其它合适的网络。

尽管被示为具有多个计算机，但安全网络 104 可只包括单个计算机 102。另外，尽管不安全网络 110 被示为具有多个远程计算机 108，但它也可只有一个。

参考图 2，所示的是在此所述的本发明可以在其上实现的计算机 102 的基本配置的例子。在其最基本配置中，计算机 102 一般包括至少一个处理单元 202 和存储器 204。处理单元 202 执行指令以完成按照本发明各种实施例的任务。在完成这样的任务时，处理单元 202 可发送电子信号到计算机 102 的其它部分及计算机 102 外部的设备以产生某些结果。取决于计算机 102 的准确配置和类型，存储器 204 可以是易失性的(诸如 RAM)、非易失性的(诸如 ROM 或闪存)、或两者的某种结合。这种最基本配置用虚线 206 示于图 2。

计算机 102 还可具有附加的部件/功能。例如，计算机 102 还可包括附加的存储器(可移动的 208 和/或不可移动的 210)，包括(但不限于)磁盘、光盘或磁带。计算机存储介质包括以任何方法或技术存储信息的易失性的和非易失性的、可移动的和不可移动的介质存储信息(包括计算机可执行指令、数据结构、程序模块或其它数据)。计算机存储介质包括(但不限于)RAM、ROM、EEPROM、闪存、CD-ROM、数字通用盘(DVD)或其它光存储器、磁带盒、磁带、磁盘存储器或其它磁存储设备、或任何其它能够用于存储所要的信息并能由计算机 102 访问的介质。任何这样的计算机存储介质都可以是计算机 102 的一部分。

计算机 102 较佳地还包含通信连接 212，它允许设备与其它设备通信，诸如在安全网络 104 上的其它计算机 102 或不安全网络 110 上的远程计算机 108(图 2 只示出了一台远程计算机 108)。通信连接是通信介质的一个例子。通信介质一般包含在诸如载波或其它传输机制的调制数据信号中的计算机可读指令、数据结构、程序模块或其它数据，并包括任何信息传递介质。作为例子(而非限制地)术语“通信介质”包括无线介质，诸如声学、RF、红外及其它无线介质。这里所用的术语“计算机可读介质”包括计算机存储介质和通信介质两者。

计算机 102 还可具有输入设备 216，诸如键盘/小键盘、鼠标、笔、声音输入设备、触摸输入设备等。还可包括输出设备 218，诸如显示器 220、扬声器、

打印机等。这些设备在本领域中众所周知，不需要在此详述。

在随后的描述中，将参考可由一个或多个计算设备执行的动作和操作的符号表示法来描述本发明，除非另有指示。这样，将要理解这种动作和操作，它们有时被称为是由计算机可执行的，包括由计算机 102 的处理单元以结构化形式表示数据的电子信号的管理。这种处理转换数据或将它保存在计算机 102 的存储系统中的单元上，它以本领域那些熟练技术人员都理解的方式重新配置或者改变计算机 102 的操作。保存数据的数据结构是具有由数据格式定义的特定属性的存储器的物理单元。但是，虽然在前述的环境中描述本发明，但并不意味着限制本发明，如那些本领域熟练技术人员将意识到的，这里所述的几种动作和操作还可用硬件实现。

图 3 是方框图，说明按照本发明的一个实施例可使用的计算机 102 结构的细节。计算机 102 包括具有与其相关联的主机防火墙(host firewall)，如防火墙代码 302 所表示的操作系统 300。防火墙代码 302 可以是操作系统 300 的一个组件或者在计算机 102 上运行的分离的应用或程序。在所示例子中，防火墙代码 302 用作主机防火墙，它在那里保护它在其上运行的计算机 102。

计算机 102 还包括实施模块 304，它关联于或者就是操作系统 300 的一个集成部分。实施模块 304 的功能和部件在下面进一步描述。

按照本发明的一个方面，察觉性防火墙的应用 306 可以连接到操作系统 300 和/或实施模块 304。除了直接的连接，为察觉性防火墙的应用 306 提供应用 API308 来调用实施模块 304 的功能，将如下面进一步描述。

按照本发明的另一个实施例，非察觉性防火墙的应用 310 也可连接到操作系统 300 和/或实施模块 304。除了直接连接到操作系统 300 和/或实施模块 304 外，为非察觉性防火墙的应用 310 提供了套接字 API 312 来调用实施模块 304 的功能，将如下面还要进一步描述。

防火墙策略 314 被存储或者关联于计算机 102，并可以由操作系统 300 和/或防火墙代码 302 访问。在所示实施例中，将防火墙策略 314 示为数据库，但可以在几个数据库中保存防火墙策略 314 或者可以用另外的合适的方式存储防火墙策略 314。

可提供代理 320 用于与因特网网关设备 106 通信。另外，因特网网关设备 106 包括防火墙软件 324(后面称为“边界防火墙 324”)，可实现它，以便以已知方式保护安全网络 104 不受远程计算机 108 侵害。此外，按照本发明的一个方

面，在操作系统 300 上提供防火墙 API326 供防火墙代码 302 访问。

按照本发明的一个实施例，察觉性防火墙的应用 306 可通过应用 API 308 请求防火墙代码 302 和/或边界防火墙 324 的显式穿越。通过“显式(explicit)”，我们是指穿越防火墙代码 302 和/或边界防火墙 324 是由察觉性防火墙的应用 306 明确地请求的。如在背景章节中描述的，对于先前技术的网络系统，防火墙用试探法来猜测应用的意图。相反，对于本发明，提供了应用 API 308，因此察觉性防火墙的应用 306(或察觉性防火墙的服务)可显式描述它的需求并将它的请求传送到防火墙代码 302 和/或边界防火墙 324。

察觉性防火墙的应用 306 可请求各种其它可由防火墙代码 302 和/或边界防火墙 324 实施的服务。作为一个例子，察觉性防火墙的应用 306 可请求与安全网络 104 外部的一个或多个已知端点连接。连接可以是单一的、一次性连接或者可产生同一连接的许多实例。作为另一个例子，察觉性防火墙的应用 306 可请求入网和/或出网连接的带宽或连接节流(connection throttling)。还有另一个例子，察觉性防火墙的应用 306 可请求防火墙将连接范围限制到接口、本地或远程地址的子集。还有另一个例子，察觉性防火墙的应用 306 可请求只有认证过的客户可连接到特定端口。在另一个例子中，察觉性防火墙的应用 306 可请求实施最小或最大带宽规则和/或可为特定客户请求超时策略，诸如传输控制协议(“TCP”)客户。另外，察觉性防火墙的应用 306 还可请求特定的协议选项(诸如 SACK)打开或关闭，目的是减少攻击面。作为另外的一个例子，察觉性防火墙的应用 306 可描述需要特别处理的流程的一个或多个属性，诸如与机密数据的连接。

察觉性防火墙的应用 306 可通过应用 API 308 将其请求传送到防火墙代码 302 和/或边界防火墙 324。以下是可用于请求直接与诸如远程计算机 108 的远程计算机或节点通信的格式的结构的特定例子：

```
struct sockaddr Target;
...// 用端点信息初始化 Target 结构
setsockopt( s, SOL_SOCKET, SO_REQUEST_ACCESS,
&Target, sizeof(Target) );
```

在前述例子中，请求是针对特定套接字的。套接字选项名为 SOL_SOCKET、SO_REQUEST_ACCESS。参数描述在术语“struct sockaddr Target”之后；并包括远程端点或者特定远程计算机 108 的描述。可用其它数据结构来由察觉性防火

墙的应用 306 传送请求。

如果期望，操作系统 300 和/或实施模块 304 可向察觉性防火墙的应用 306 表示支持请求。同样地，操作系统 300 和/或实施模块 304 可返回一个值，表示已经接受请求的值并将它传送给防火墙，或者操作系统 300 不实现这个特定调用。可供选择地，操作系统 300 和/或实施模块 304 可返回正在检查状态的指示，并将让防火墙代码 302 和/或边界防火墙 324 最终作出决策。

察觉性防火墙的应用 306 可在应用安装后、请求连接后或者另外的合适时间进行它对应用 API 308 的调用。在向对应用 API308 请求的时候、请求连接的时候或者在另外的时间，可使防火墙代码 302 和/或边界防火墙 324 知道这个请求。按照本发明的一个实施例，可在察觉性防火墙的应用 306 进行连接的尝试时使防火墙代码 302 和/或边界防火墙 324 知道该请求。也就是说，或者察觉性防火墙的应用 306 尝试通过防火墙代码 302 和/或边界防火墙 324 发送一些内容，或者察觉性防火墙的应用 306 表示它正等待通过防火墙之一的通信。为此目的，事件可产生反调用，诸如通用套接字事件通知机制。可将反调用传送到实施模块 304。这样一个反调用的格式的例子阐述如下：

```
void SocketActivityCallback(
DWORD          dwProcessID,     // 引起套接字事件的过程
SOCKET         sock,            // 套接字句柄
SOCK_EVENT     event,           // 套接字事件(例如，绑定)
LPVOID         pDetails         // 套接字事件参数
DWORD          cbDetails        // 事件参数大小
);
```

对于前述反调用，提供以下参数：dwProcessID，发起事件的过程的 ID；sock，为之生成事件的套接字句柄；event，事件 ID，诸如 SOCKET_EVENT_BIND；pDetail，指向包含事件细节的斑点(blob)的指针，它是事件专用的；以及 cbDetails，事件细节斑点大小。可使用其它数据结构或通知机制来通知实施模块 304：察觉性防火墙的应用 306 正尝试建立连接。作为对于反调用的可供替换的例子，可使用输入/输出(I/O)调用。

在每个套接字事件发生后立即激活反调用。按照本发明的一个实施例，实施模块 304 在套接字事件发生时检查套接字事件并保存有关的套接字状态细节以允许对防火墙代码 302 和/或边界防火墙 324 进行适当的通信。

操作系统300和/或实施模块304利用防火墙API 326告知防火墙代码302：察觉性防火墙的应用306请求一个连接。通知可以是如上所述的，并可附加地包括应用专用信息，诸如应用信任级别、应用标识等等。防火墙代码306将请求与防火墙策略314比较并可能允许或拒绝请求。可能或可能不向应用给出指示。

另外，按照本发明实施例，防火墙代码302通知边界防火墙324：请求连接。这个信息可通过认证过的协议或通过代理320传送给边界防火墙324。边界防火墙324另外可对照它自己的策略(未示出，但在本领域中公知)检查请求。假设请求符合防火墙代码302和边界防火墙324两者的策略，则允许连接通过防火墙。

尽管描述为具有防火墙代码302和边界防火墙324二者，但本发明可在只有这些防火墙之一的系统中实现。例如，在只有一台计算机102的家庭网络上，唯一可用的防火墙可能是防火墙代码302。

图4所示的是察觉性防火墙的应用306请求从已知端点(例如，远程计算机108之一)接收单一连接(例如，TCP连接)的过程的例子。

在步骤400，察觉性防火墙的应用306创建一个新的套接字。在步骤402，察觉性防火墙的应用306绑定套接字以在端口N上接收连接。在步骤404，察觉性防火墙的应用306使用应用API 308通知操作系统300和/或实施模块304：它期望来自一个特定地址的连接。例如，这可使用如上所述的调用格式来完成。在步骤404，察觉性防火墙的应用306绑定套接字来以在端口N上接收连接。

在步骤406，察觉性防火墙的应用306激活接受(accept)API(未示出，但在本领域中公知)并且开始等待连接。察觉性防火墙的应用306激活接受API导致一个正在发送的通知，如上所述。操作系统300现在完全知道察觉性防火墙的应用306的意图和连接端点，并且在步骤408使用防火墙API 326告知防火墙代码302：期望来自一指定地址的单一连接在本地端口N上到达。通知还可包括应用专用信息，诸如应用可信级别、应用标识或其它信息。

在步骤410，防火墙代码302将察觉性防火墙的应用306的请求与防火墙策略314比较，并且允许或拒绝请求。在步骤412，防火墙代码302通知边界防火墙324：期望一个具有众所周知的属性的连接。

假设当远程节点在端口N上发起至察觉性防火墙的应用306的连接时，请求符合防火墙代码302和边界防火墙324的策略，则将允许通信。在步骤414，

远程计算机 108 建立连接。

在察觉性防火墙的应用 306 完成监听端口 N 之后，在步骤 416 关闭套接字。然后在步骤 418，操作系统 300 可执行清除，例如通知防火墙代码 302，它轮到与边界防火墙 324 通信。

如能从前述中所理解的，应用 API 308 和防火墙 API 326 提供这样的机制，通过这些机制可将请求传送至主机或边界防火墙。然后防火墙可相应地作出反应，如果请求符合防火墙策略 314(如果和边界防火墙的防火墙策略有关)，则可允许连接。因而，应用 API 308 和防火墙 API 326 为应用提供增强的协助，用于在不需要为每种类型的连接编写单独的应用专用的代码的情况下穿过防火墙。

对于刚才所描述的实施例，实施模块 304 用作操作系统 300 的组件，或者与其紧密地相关联，并且处理察觉性防火墙的应用 306 的请求。如果需要，实施模块 304 可在应用 API 308 与防火墙 API 326 的抽象级别之间提供转换。例如，应用 API 308 可处理套接字和连接，而防火墙 API 326 可处理端口和流。

按照本发明的另一个实施例，实施模块 304 另外可允许用户创建简单的防火墙策略或网络访问策略，从而允许或拒绝应用或服务穿过防火墙。下面将描述实施模块 304 的这方面的功能。尽管在此描述的实施模块 304 具有已经描述的功能和下面描述的其它功能，但也可为独立的功能提供独立的模块。另外，计算机诸如计算机 102 可包括只具有这些功能组的一个功能或者功能组的一部分功能的模块。然而，为了易于描述，在此的描述假设实施模块 304 至少具有这两个所述的功能组。

为了这个描述，配置为与非察觉性防火墙的应用 310 一起工作的实施模块 304 的一部分在此将称为拦截模块 500(图 5)。通常，拦截模块 500 配置为监视应用和服务的对本地计算机诸如计算机 102 上网络堆栈 508 的连接和监听尝试。拦截模块 500 捕获这些尝试并且确定什么用户正在进行尝试，确定什么应用或服务正在进行尝试，并且进行防火墙策略 314 查找以确定是否允许用户和应用/服务连接到网络。

图 5 所示的方框图一般表示计算机 102 的某些组件和那些组件与拦截模块 500 的交互。计算机 102 包括用户模式套接字接口 502(例如用户模式 Winsock)，内核模式套接字接口 504(例如内核模式 Winsock)和网络适配器 510。

通常，图 5 所示的每个组件以某些形式或者其它形式存在于现有的计算机

上，除了拦截模块 500 以外。按照本发明的一个实施例，这样安排拦截模块 500，使得它可以接收和捕获应用和服务的连接或监听尝试。为此，例如，拦截模块 500 可位于网络堆栈 508 与非察觉性防火墙的应用 310 之间，例如在网络堆栈 508 的接口处。如下面进一步描述的，拦截模块 500 从连接和/或监听尝试中提取连接需求，确定连接需求是否符合策略，并且如果符合，命令防火墙代码 302 创建一个较低级别的防火墙过滤器以允许连接。

通常，连接和监听尝试包括连接至一个端点或者由端点来连接的任何尝试。为此目的，如这里所用的，“连接”和/或“监听”尝试包括，特别是，发送请求、接收请求、加入请求和更新请求。

计算机 102 的监听和/或连接尝试一般包括参数，这些参数将允许拦截模块 500 确定应用或服务的需求。如一个例子，对于监听和连接尝试两者，一般请求端口的绑定。绑定可能是对于特定端口或者如果可能使用各种端口则对于通配符端口。监听尝试一般将包括套接字地址，在该地址应用或服务希望接收连接。另外，应用 ID 和用户 ID 可以从监听尝试的上下文中推断。从这个推断的信息，可对照应用和/或用户的策略评估特定套接字的请求，并且可基于那个策略允许或不允许连接。

如果进行连接请求，那个连接请求将包括与监听请求相似的信息，并且可包括端点地址。此外，可使用此信息并对照策略评估此信息，以便确定是否可以进行连接。

计算机 102 的一般策略可在防火墙策略 314 内形成，以或者允许或者拒绝在计算机 102 上的特定应用和服务对网络的连接。这个一般性策略可在设置计算机 102 的用户设置时手工地在计算机 102 上建立、也可由网络管理员来建立、或者可在建立用户的简档时设置为默认的设置。如果需要，策略可基于每个用户。这些一般的策略可能是，例如，“不要让任何应用连接至不安全的网络 110，除非拦截模块 500 具有不同的策略”可将一般的策略与由拦截模块 500 保存的策略分开存储。

按照本发明的一个实施例，在拦截模块 500 内的策略(和存储在策略高速缓存 612 中的，例如)可创建和存储为用户和/或服务/应用的请求的结果。例如，在将服务或应用安装在计算机上时、在发起一个连接时或者在其它合适的时间，可自动地或者通过用户界面来进行这个请求。请求可简单地包括所想要的连接的简单参数，诸如“允许应用 X 连接至因特网一次”或者，如其它非限制

的例子，与察觉性防火墙的应用 306 的描述一起在上面描述的任何请求。

按照本发明的一个实施例，用户和/或应用的请求不需要用于端口、协议或者 IP 地址的规则以使应用或服务能够穿过防火墙代码 302 和/或边界防火墙 324。而是，如上所述，在已经建立了一个策略之后，根据应用的连接请求，拦截模块 500 通过评估应用或服务的连接和监听尝试来确定应用或服务的需求。

图 6 所示的方框图示出拦截模块 500 的一般组件。拦截模块 500 包括逻辑引擎 600，它执行在此所述的拦截模块 500 的大多数基本操作。拦截接口客户 602 连接到逻辑引擎 600，配置为与网络堆栈 508 交互并捕获由应用诸如非察觉性防火墙的应用 310 进行的连接和/或拦截请求。配置和策略 API 604 配置和安排为与防火墙策略 314 或关联的策略管理器(未示出)的通信。

本地防火墙客户 606 配置为与防火墙代码 302 通信。防火墙穿越协议客户 608 被配置和安排为与边界防火墙 324 通信。

在图 6 所示的例子中，拦截模块 500 包括端点高速缓存 610、策略高速缓存 612 和过滤器高速缓存 614。端点高速缓存 610 存储拦截模块 500 当前正在管理的各种端点(即节点)的操作状态。它是由逻辑引擎 600 基于来自拦截接口客户 602 的输入来更新的。策略高速缓存 612 存储拦截模块 500 要实施的策略。在策略高速缓存 612 中的条目可与在端点高速缓存 610(即该给定策略被实施的端点)的条目相关联。单个策略条目可以和多个端点相关联。

拦截接口客户 602 处理监听和/或连接尝试的细节，与网络堆栈 508 交互，并且访问逻辑引擎 600 以通知逻辑引擎 600 拦截到的动作并且接收授权决策。配置和策略 API 604 是一个进入拦截模块 500 的外部接口。可向配置和策略 API 604 进行请求并且将请求存储在策略高速缓存 612。例如，可由应用在安装或者连接尝试时通过防火墙策略 314 来提供策略，或可由用户例如通过套接字 API 312(图 3)来提供。下面给出其它例子。使用本地防火墙客户 606 来命令防火墙代码 302 以创建合适的过滤器，类似地，防火墙穿越协议客户 608 被用来命令该边界防火墙 324 构建合适的滤波器，并且因而执行许多与代理 320 相同的功能。

过滤器高速缓存 614 包括用于逻辑引擎 600 已经创建的过滤器的条目。在过滤器高速缓存 614 中条目可与在端点高速缓存 610(例如，已经为其创建过滤器的端点)中的条目相关联。单个过滤器可与多个端点相关联。包括在过滤器

高速缓存 614 中的信息包括过滤器的细节(例如,5 元组,关联的 IPSec 策略等),将使用的相应的防火墙过滤器的句柄,和/或防火墙穿越协议客户 608 的识别信息。

现在转到拦截模块 500 的操作,在应用或服务试着建立连接之前,用户和/或应用或服务通过配置和策略 API 604 建立用于应用或服务的策略。在策略高速缓存 612 中存储策略。在建立策略之后,拦截接口客户 602 监视应用和服务对在计算机 102 上的网络堆栈 508 的连接和监听尝试。拦截接口客户 602 捕获这些尝试并且将它们发送给逻辑引擎 600。逻辑引擎 600 确定什么用户正在进行尝试、确定什么应用或服务正在进行尝试,并将那个信息存储在端点高速缓存 610 中。然后逻辑引擎 600 访问策略高速缓存 612 以确定是否允许用户和应用或服务连接到所请求的网络。

如果允许用户和应用或服务两者连接到网络,创建合适的防火墙配置诸如较低级别的防火墙过滤器,来允许应用或服务具有无拘无束的网络通信。将防火墙配置存储在过滤器高速缓存 614 中。本地防火墙客户 606 和网络穿越协议客户 608 可使用此过滤器信息来命令防火墙代码 302 和边界防火墙 324 以允许建立连接。

按照本发明的一个实施例,为拦截模块 500 提供通知客户 616。通知客户 616 配置和安排为与外壳通知管理器(未示出,但在本领域中公知)或者相似的组件,以便通知用户一个事件。例如,通知客户 616 可命令通知管理器以通知用户:应用或服务正在尝试访问因特网和操作系统 300 正在阻止此尝试,诸如图 7 的用户界面 700 所示。另外,通知客户 616 可命令通知管理器请求与继续阻止或允许访问有关的用户指令,诸如由图 7 中的 702 和 704 允许的。如果适合,通知客户 616 可等待和通知逻辑引擎 600:用户对查询的响应。

如果用户选择按钮 704,则允许连接,那个按钮的选择导致为那个应用(这里,应用 X)建立策略。如果需要,策略可只允许一次连接,可允许将来的连接,或者可允许在时限内(例如在一天内)的连接。

图 8 所示的是拦截模块 500 如何能够使非察觉性防火墙的应用 310 穿越诸如防火墙代码 302 和/或边界防火墙 324 的防火墙的例子。始于步骤 800,用户创建允许应用 X 连接到网络的策略,例如仅在用户运行该应用时。用户稍后在步骤 802 运行应用 X。应用 X 尝试连接和监听网络堆栈 508。拦截模块 500 在步骤 804 捕获这些连接和监听尝试。拦截模块 500 在步骤 806 确定哪个应用或

服务正在进行请求，并在步骤 808 确定哪个用户正在运行应用或服务。

根据这个信息，拦截模块 500 确定允许用户和应用连接到网络，并自动修改防火墙策略以允许监听本地端口及连接到所请求的端点。

因为这种用户专用策略只为给定用户建立，不同的用户不能访问网络。例如，在步骤 812，第二用户运行应用 X，并且在步骤 814 拦截模块 500 进行必需的许可检查，类似于步骤 806 和 808。在步骤 816，拦截模块 500 确定不允许第二用户在网络上运行应用 X 并返回错误给应用，例如通过通知客户 616。

图 9 是流程图，所示的是服务如何能够将服务的网络需求通知防火墙代码 302 和/或边界防火墙 324 的例子的步骤。始于步骤 900，在计算机上的一个服务，例如计算机 102 打开一个监听套接字。在步骤 902，服务使用 API，诸如套接字 API 312，以建立策略，例如表示只应该接受来自本地子网(例如安全网络 104)的入网通信。在步骤 904，服务绑定到套接字并且等待连接尝试。在步骤 906，在第二台计算机上的用户，诸如在安全网络 104 上的另一个计算机 102 打开尝试连接至在计算机 102 上的服务的应用。

在计算机 102 上的拦截模块 500 在步骤 908 拦截连接尝试，并将第二台计算机的子网与其自己的子网比较。在步骤 910，子网检查成功并且在第二台计算机 102 上的应用连接至在第一台计算机 102 上的服务。

在步骤 902 建立的相同策略可用于拒绝不是来自本地子网的计算机，诸如在步骤 912-916 中所示的。在步骤 912，在远程计算机 108 上的用户打开尝试连接至在第一台计算机 102 上的服务的应用。在步骤 914，在第一台计算机 102 上的防火墙代码 302 拦截连接尝试并且将远程计算机 108 的子网与其自己的子网比较。在步骤 916，子网检查未通过并且不允许在远程计算机 104 上的应用连接至在第一台计算机 102 上的服务。

在此列举的所有引用，包括出版物、专利申请和专利，被结合引用作为同样的扩充，与如果每个引用被单独地和明确地提示结合引用一样，并且在此作为整体提出。

在描述本发明的上下文中(尤其在以下权利要求书的上下文中)词语“a”和“an”和“the”和类似的指示物的使用将被解释以覆盖单数和复数两者，除非在这里另行指出或与上下文明显矛盾。词语“comrising”、“having”、“including”和“containing”将解释为“开口”的词语(即，意味着“including,but not limited to”(包括，但不限于))，除非另行指出。在这里值的范围详述只是意

在用作一种简约的方法，每单独的值都各自落在范围内，除非在此特别表示，并且将单独的值结合到说明书中，好象它是在此一个一个单独地列举的。可以任何合适的顺序执行在此描述的所有方法，除非在此另行指出或者与上下文明显矛盾。使用任何或所有例子，或者在此提供的示例性语言(例如"诸如")，只是想要更好地阐明本发明的实施例，并且不在本发明的范围上形成限制，除非另外要求。在说明书中的语言不应该解释为表示任何非要求的元素为实施本发明所必需的。

在这里描述了本发明的较佳实施例，包括发明人所知的完成本发明的最佳模式。这些较佳实施例的变体对于那些本领域的普通技术人员将在阅读前面描述的基础上变得显而易见。发明人期望熟练的技术人员适当地使用这些变体，并且发明人希望不同于如在这里明确描述的来实施本发明。相应地本发明包括所附权利要求书中所述的主题的、由适用法律许可的所有修改和本身。而且，在本发明的所有可能的变体中上述元素的任何组合也由本发明包括，除非这里另行指出或上下文明显矛盾的。

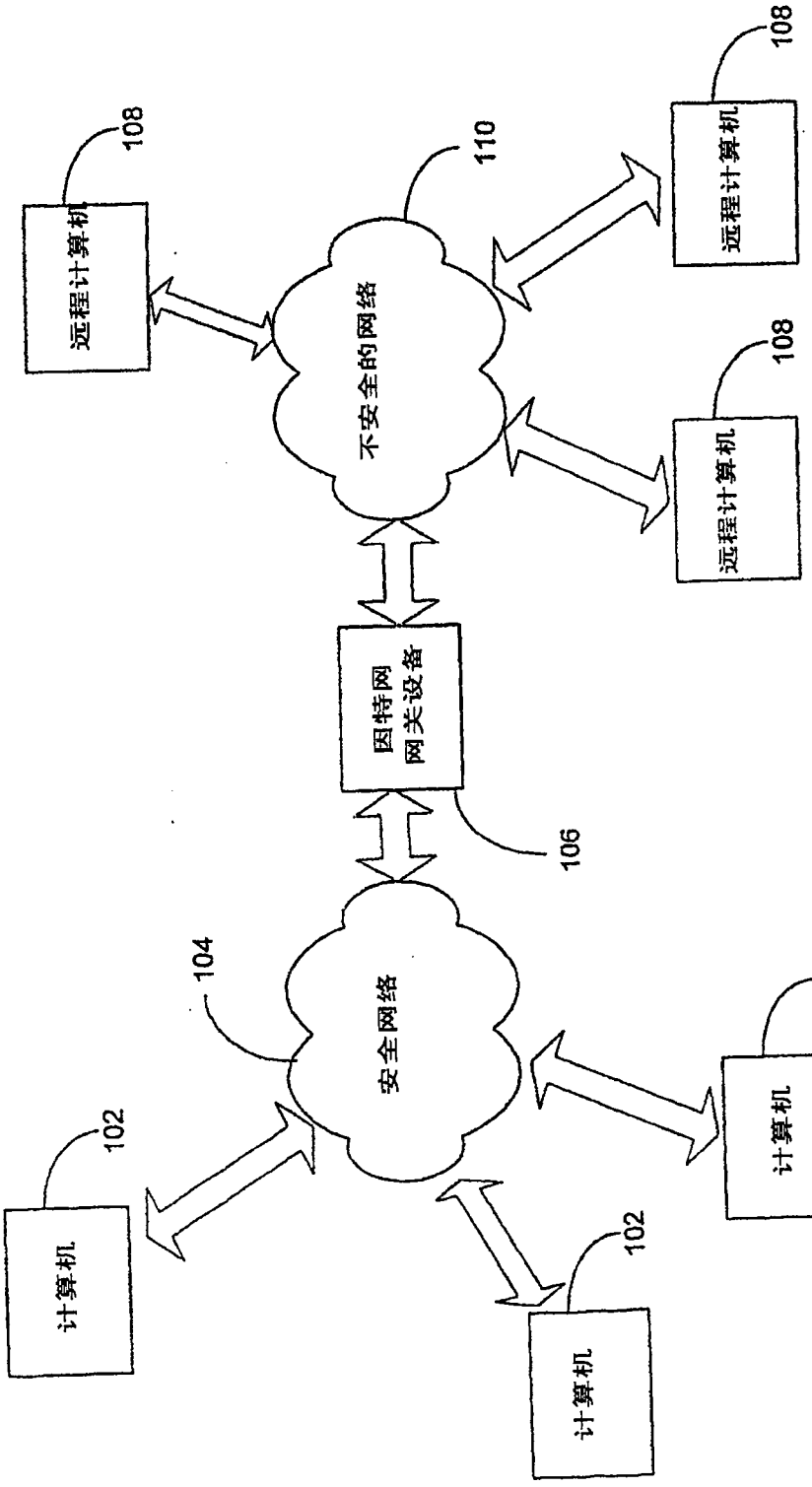

远程计算机
108
不安全的网络
110
远程计算机
108
远程计算机
108
因特网
网关设备
106
安全网络
104
计算机
102
计算机
102
计算机
102

图 1

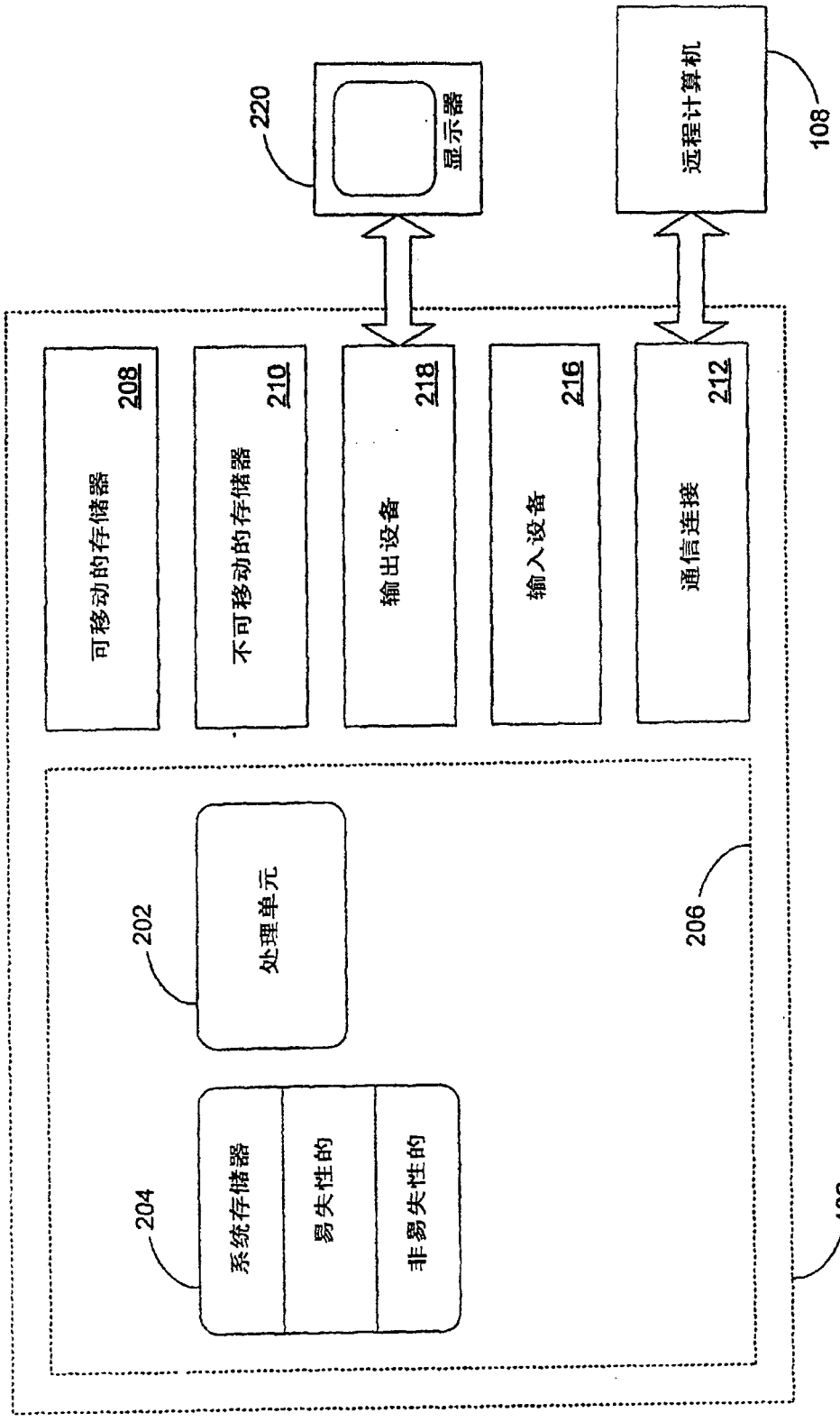

220
显示器
远程计算机
108
可移动的存储器
208
不可移动的存储器
210
输出设备
218
输入设备
216
通信连接
212
206
202
处理单元
204
系统存储器
易失性的
非易失性的
102

图 2

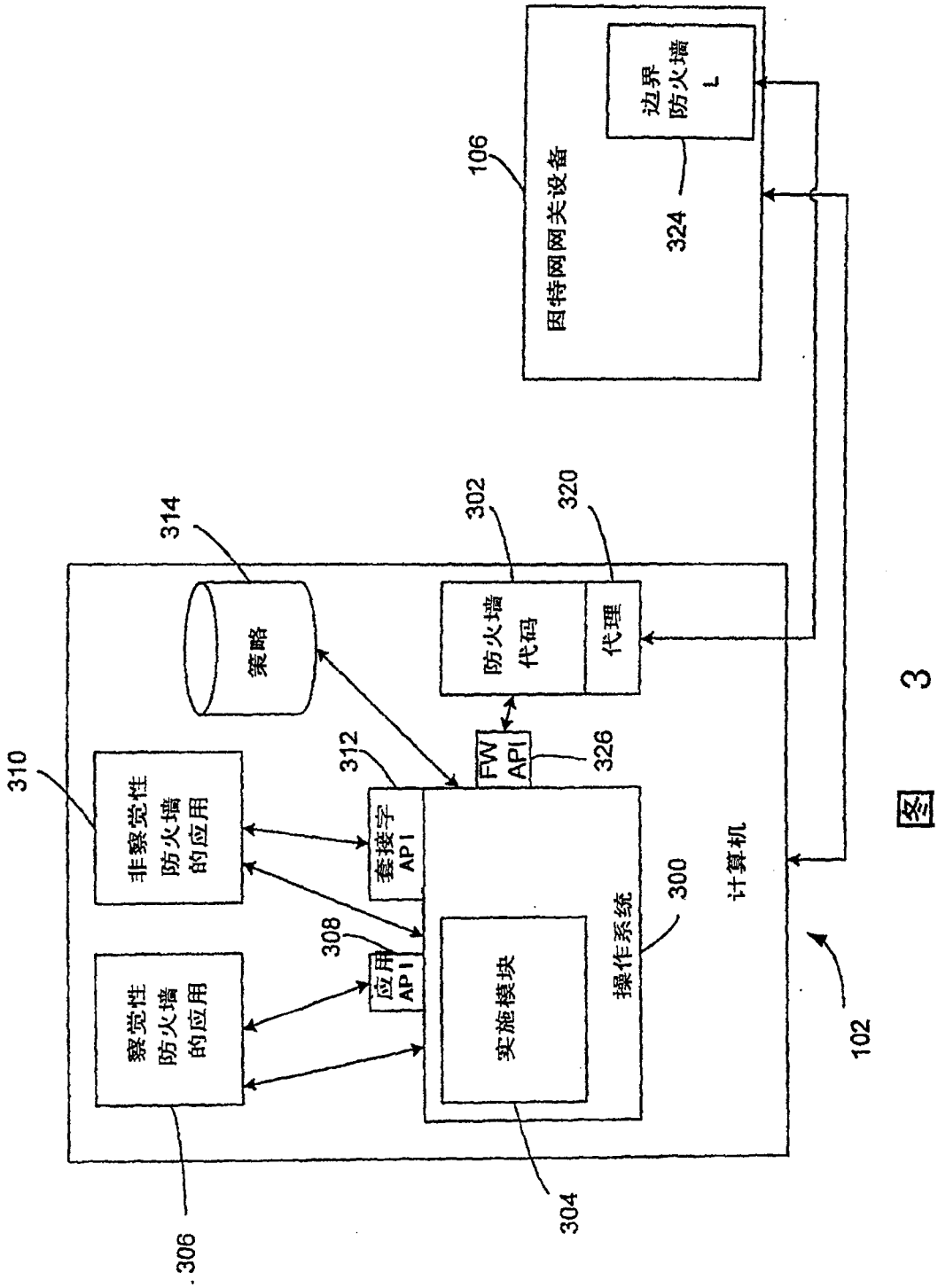

因特网网关设备
106
边界防火墙 L
324
策略
314
防火墙代码
302
代理
320
FW API
326
套接字 API
312
应用 API
308
非察觉性防火墙的应用
310
察觉性防火墙的应用
306
实施模块
304
操作系统
300
计算机
102

图 3

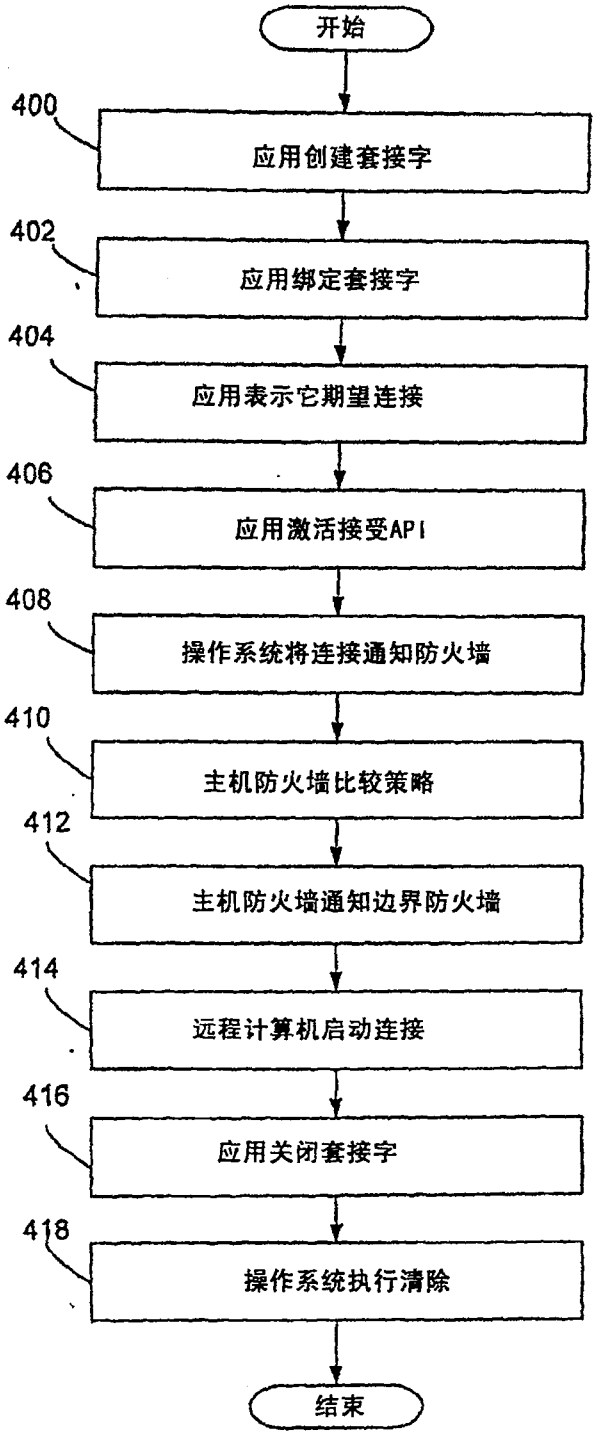

开始
400
应用创建套接字
402
应用绑定套接字
404
应用表示它期望连接
406
应用激活接受API
408
操作系统将连接通知防火墙
410
主机防火墙比较策略
412
主机防火墙通知边界防火墙
414
远程计算机启动连接
416
应用关闭套接字
418
操作系统执行清除
结束

图 4

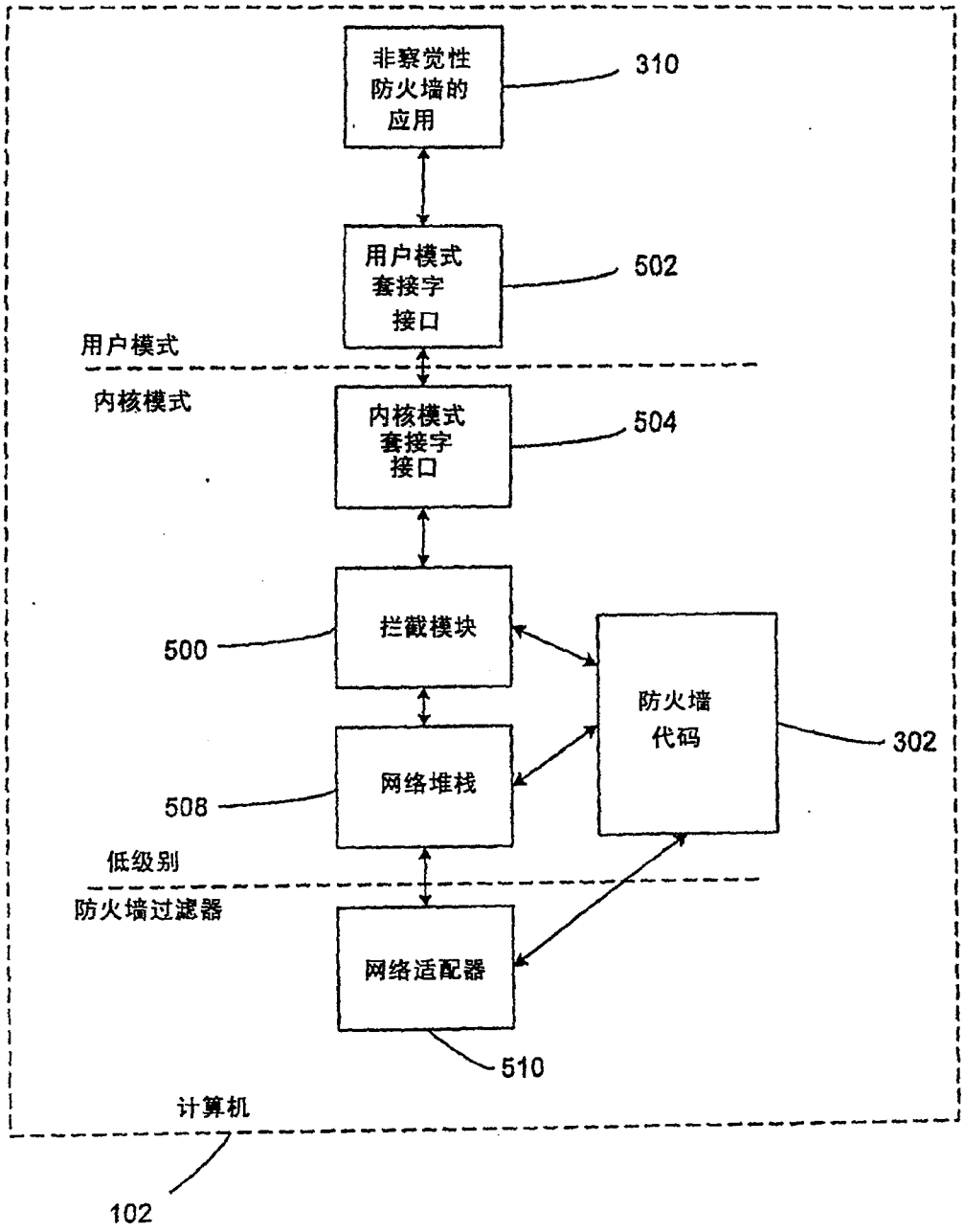

非察觉性
防火墙的
应用
310
用户模式
套接字
接口
502
用户模式
内核模式
内核模式
套接字
接口
504
拦截模块
500
防火墙
代码
302
网络堆栈
508
低级别
防火墙过滤器
网络适配器
510
计算机
102

图 5

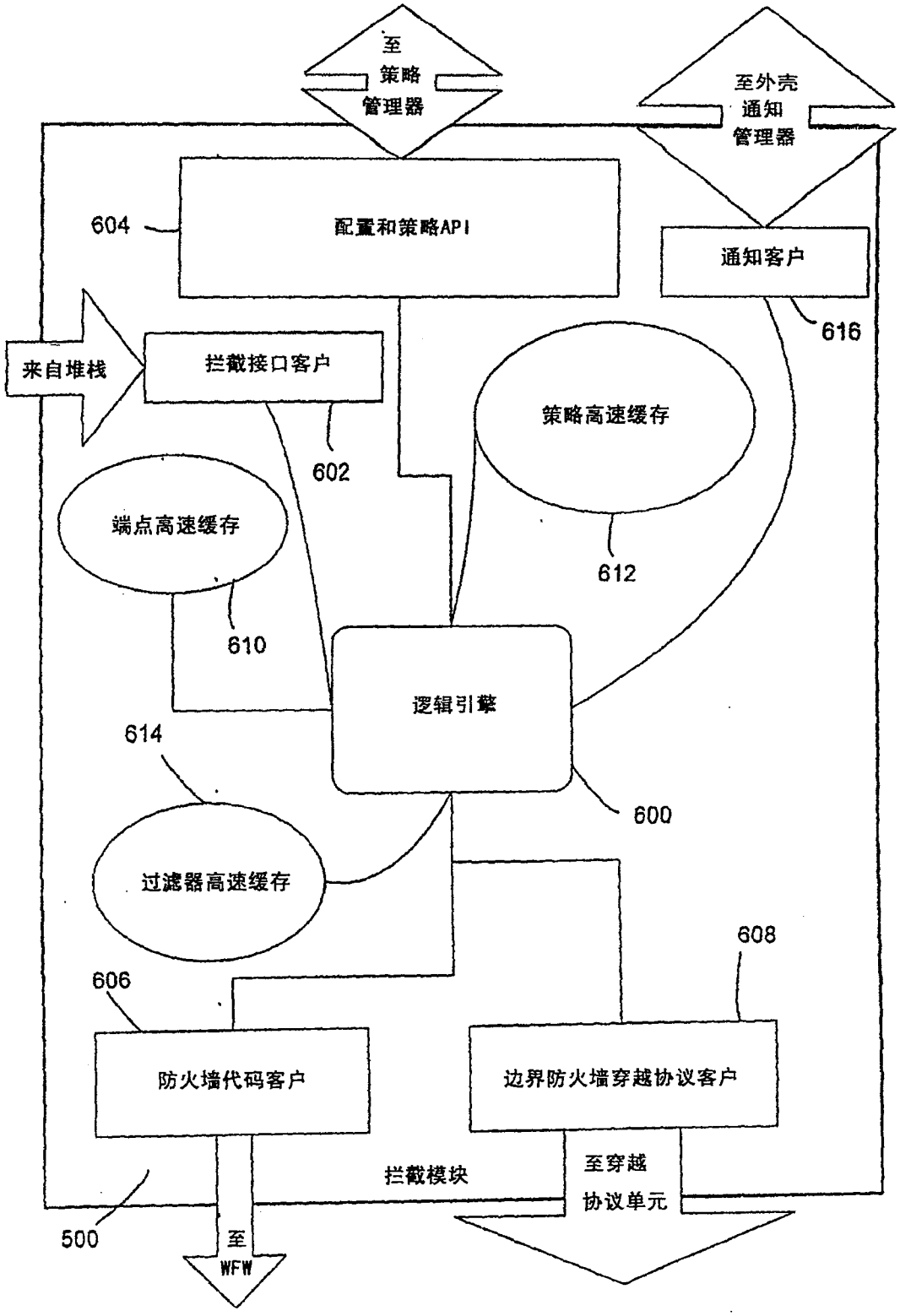

至
策略
管理器
至外壳
通知
管理器
604
配置和策略API
通知客户
616
来自堆栈
拦截接口客户
602
策略高速缓存
612
端点高速缓存
610
逻辑引擎
614
600
过滤器高速缓存
608
606
防火墙代码客户
边界防火墙穿越协议客户
拦截模块
至穿越
协议单元
500
至
WFW

图 6

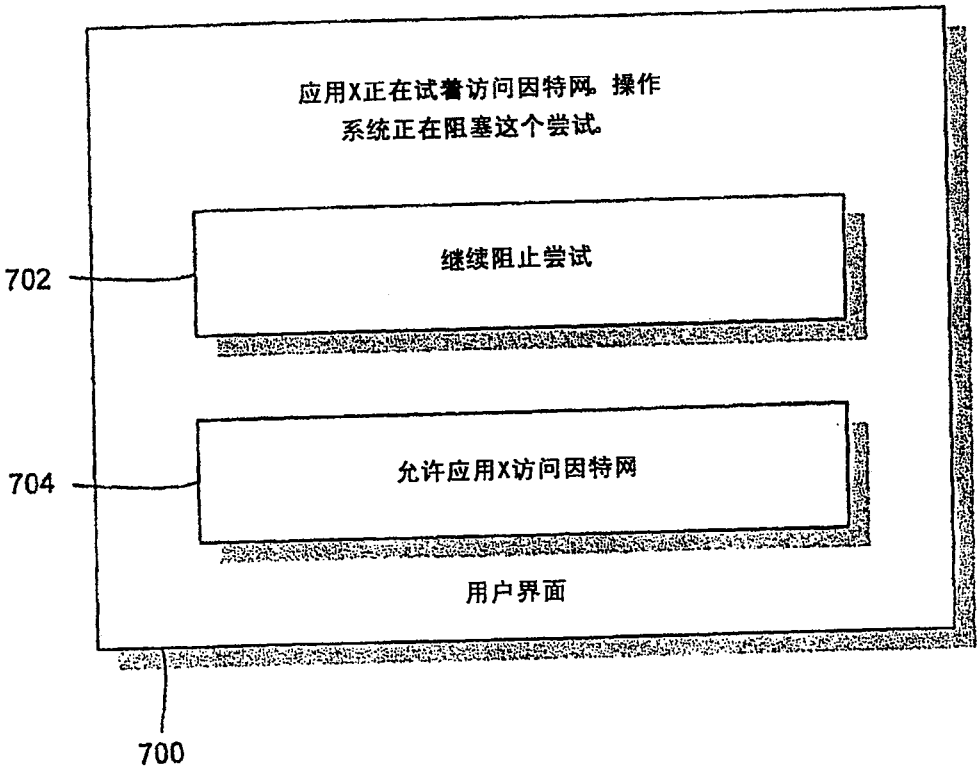

应用X正在试着访问因特网。操作
系统正在阻塞这个尝试。
继续阻止尝试
允许应用X访问因特网
用户界面
702
704
700

图 7

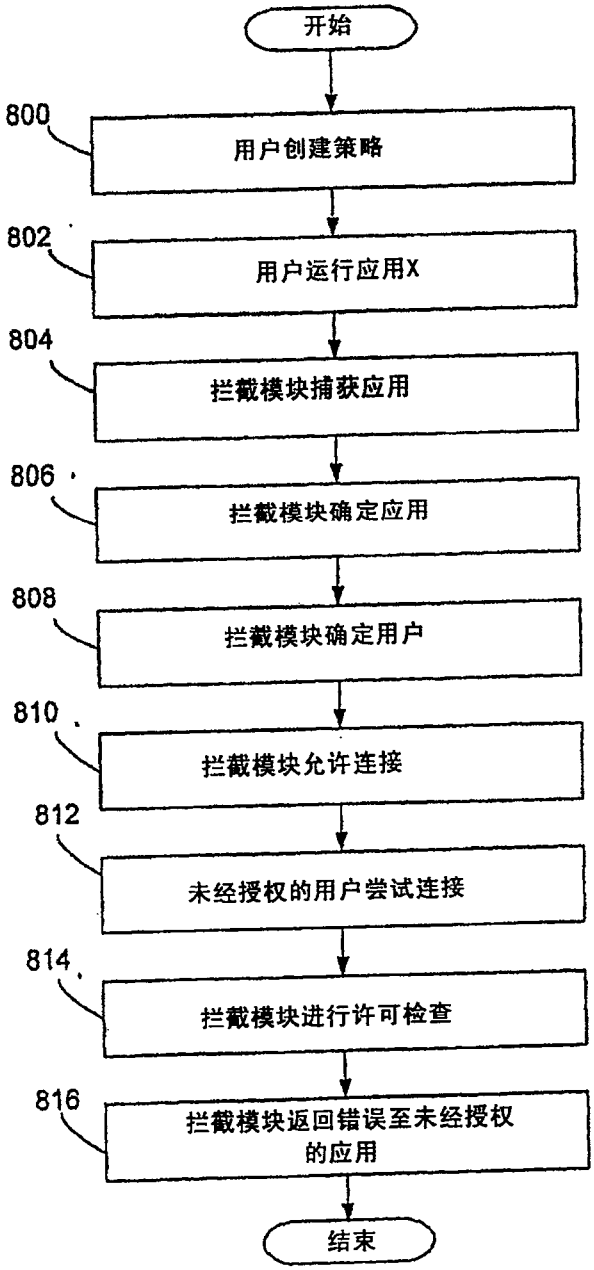

开始
800
用户创建策略
802
用户运行应用X
804
拦截模块捕获应用
806
拦截模块确定应用
808
拦截模块确定用户
810
拦截模块允许连接
812
未经授权的用户尝试连接
814
拦截模块进行许可检查
816
拦截模块返回错误至未经授权的应用
结束

图 8

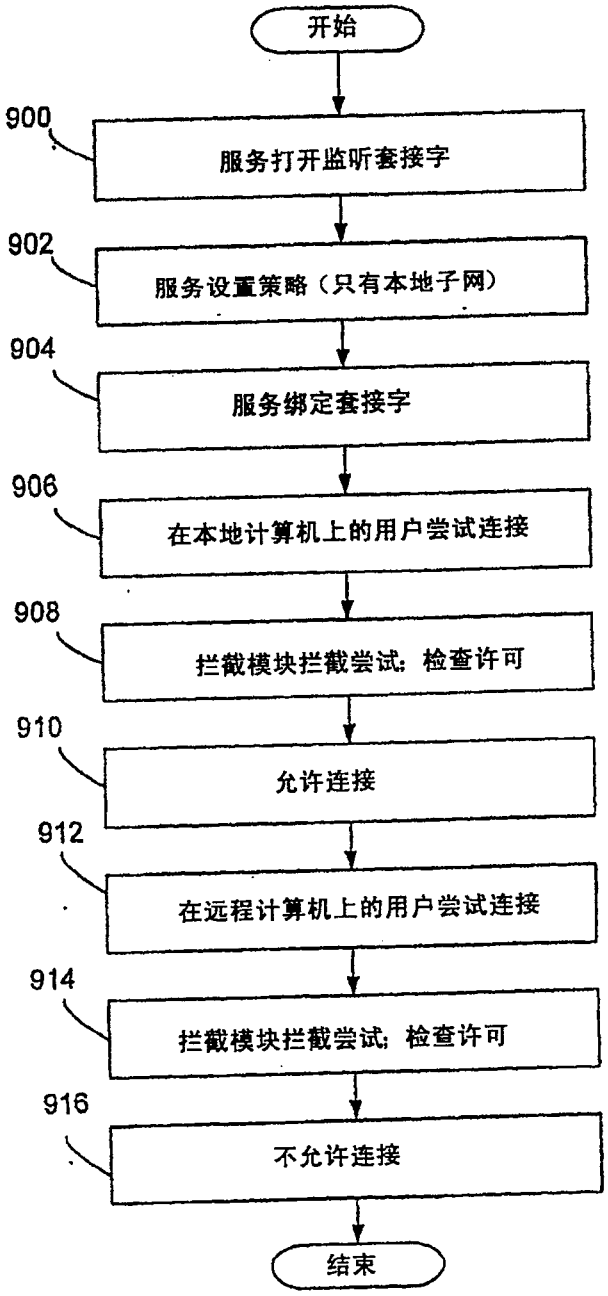

开始
900
服务打开监听套接字
902
服务设置策略（只有本地子网）
904
服务绑定套接字
906
在本地计算机上的用户尝试连接
908
拦截模块拦截尝试；检查许可
910
允许连接
912
在远程计算机上的用户尝试连接
914
拦截模块拦截尝试；检查许可
916
不允许连接
结束

图 9