

[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷

G06F 1/24



[12] 发明专利申请公开说明书

[21] 申请号 01805889.2

G06F 11/30 G06F 15/173
G06F 15/16 H04L 9/00

[43] 公开日 2003 年 3 月 26 日

[11] 公开号 CN 1406351A

[22] 申请日 2001.2.26 [21] 申请号 01805889.2

[30] 优先权

[32] 2000.3.2 [33] US [31] 09/517,276

[86] 国际申请 PCT/US01/05925 2001.2.26

[87] 国际公布 WO01/65343 英 2001.9.7

[85] 进入国家阶段日期 2002.8.30

[71] 申请人 查克波特软件技术有限公司

地址 以色列拉马特甘

[72] 发明人 戈嫩·芬克 阿米拉·哈鲁斯

[74] 专利代理机构 北京三友知识产权代理有限公司

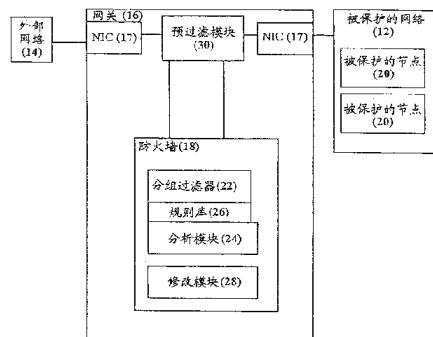
代理人 李 辉

权利要求书 5 页 说明书 13 页 附图 3 页

[54] 发明名称 快速分组过滤与处理系统、装置及方法

[57] 摘要

一种通过增加一个具有预过滤模块(30)的防火墙(18)进行分组过滤的方法、装置及系统(图1)，该预过滤模块(30)根据分组是否是从一个特定连接接收的来执行有关该分组的一个有限动作组，否则，该分组就被转发给防火墙(18)进行处理。



10

I S S N 1 0 0 8 - 4 2 7 4

1、一种用于加速分组过滤的系统，该系统包括：

(a) 一个源节点，用于传输一个分组；

(b) 一个目的节点，用于接收所述分组；

5 (c) 一个防火墙，插置于所述源节点和所述目的节点之间，用于根据至少一个规则执行分组过滤；以及

(d) 一个预过滤模块，与所述防火墙通信，用于从所述防火墙接收至少一个指令并在所述防火墙之前接收所述分组，使得如果根据所述至少一个指令所述分组被允许，则所述预过滤模块处理所述分组，或者所述预过滤模块将所
10述分组转发给所述防火墙进行处理。

2、如权利要求 1 所述的系统，其中在所述源节点和所述目的节点之间的分组传输形成一个连接，且所述防火墙判定所述连接是否被允许，使得所述至少一个指令包括所述分组的至少一个用于标识一个被允许连接的参数，使得如果所述连接被允许，则所述预过滤模块处理所述分组。

15 3、如权利要求 2 所述的系统，其中，如果所述分组有一个选择的话路控制字段值，则所述防火墙从所述预过滤模块接收来自所述被允许的连接的一个分组。

4、如权利要求 2 所述的系统，其中，所述至少一个用于标识所述被允许连接的参数包括用于所述分组的一个源地址和一个目的地址。

20 5、如权利要求 4 所述的系统，其中，所述至少一个用于标识所述被允许连接的参数进一步包括用于所述分组的一个源端口和一个目的端口。

6、如权利要求 2 所述的系统，其中，如果已经有一段预定时间没有接收到所述被允许连接的一个附加分组，则所述连接被所述防火墙删除。

25 7、如权利要求 2 所述的系统，其中，如果接收到一个用于所述连接的、具有表示连接状态信息的特定话路控制字段值的分组，则所述分组被转发给所述防火墙。

8、 如权利要求 2 所述的系统，其中，所述预过滤模块进一步包括：

(i) 一个连接数据库，用于存储所述分组的用于标识所述被允许连接的所述至少一个参数。

9、 如权利要求 8 所述的系统，其中，所述预过滤模块进一步包括：

(ii) 一个分类引擎，用于分析所述分组的至少一部分，并将所述分组的所述至少一部分与所述至少一个参数进行比较。

10、 如权利要求 9 所述的系统，其中，所述预过滤模块进一步包括：

(iii) 一个修改器，用于如果从所述被允许连接接收到所述分组，则在所述分组上执行至少一个动作，所述至少一个动作是根据来自所述防火墙的指令确定的。

11、 如权利要求 10 所述的系统，其中，所述预过滤模块以一个硬件装置实施。

12、 如权利要求 10 所述的系统，进一步包括：

(e) 一个计算装置，插置于所述源节点和目的节点之间，其中所述预过滤模块和所述防火墙由所述计算装置操作。

13、 一种在网络上用于加速分组过滤的系统，该系统包括：

(a) 一个防火墙，位于该网络上，用于根据至少一个规则在分组上执行分组过滤；以及

(b) 一个预过滤模块，位于该网络上并与所述防火墙通信，用于从所述防火墙接收至少一个指令，所述至少一个指令判定一个简单比较，还用于在所述防火墙之前接收在该网络上传输的分组，使得如果该分组根据所述简单比较被允许，则所述预过滤模块至少在该网络上传输该分组。

14、 如权利要求 13 所述的系统，其中，如果该分组不被允许，那么，如果该分组是从该网络上接收的，则所述预过滤模块将该分组转发给所述防火墙进行处理；或者如果该分组是从所述防火墙接收的，则所述预过滤模块放弃该分组。

15、如权利要求13所述的系统，进一步包括：

- (c) 一个源节点，用于传输该分组；以及
- (d) 一个目的节点，用于接收该分组；

其中，在所述源节点和所述目的节点之间的分组传输形成一个连接，并且所述防火墙判定所述连接是否被允许，使得所述至少一个指令包括所述分组的至少一个用于标识一个被允许连接的参数，使得如果所述连接被允许，则所述预过滤模块至少在该网络上上传输该分组。

16、如权利要求15所述的系统，其中，如果所述连接不是一个被允许的连接，则所述预过滤模块放弃该分组。

17、一种接收分组的装置，在一个具有一个用于传输分组的网络及一个在该网络上过滤该分组的防火墙的加速分组过滤系统中使用，并且在该防火墙之前接收该分组，该装置包括：

- (a) 一个存储器，用于存储至少一个指令以分析来自该防火墙的分组的至少一个参数，所述至少一个指令包括所述至少一个用于标识该分组的参数；以及

- (b) 一个分类引擎，用于分析该分组的至少一部分，并根据所述至少一个指令将该分组的所述至少一部分与所述至少一个参数进行比较。

18、如权利要求17所述的装置，进一步包括：

- (c) 一个修改器，用于如果该分组被允许则在该分组上执行至少一个动作，所述至少一个动作是根据来自所述防火墙的所述至少一个指令确定的。

19、一种在一个与一个防火墙连接的网络上用于加速分组过滤的方法，该方法包括下列步骤：

- (a) 提供一个预过滤模块，用于在防火墙之前接收一个分组；
- (b) 由所述预过滤模块接收所述分组；
- (c) 判定所述分组是否被允许；以及
- (d) 如果所述分组被允许，则所述预过滤模块处理所述分组。

20、如权利要求 19 所述的方法，进一步包括步骤：

(e) 或者，将所述分组转发给该防火墙。

21、如权利要求 20 所述的方法，其中如果所述分组是从该网络上接收的，则执行步骤 (e)。

22、如权利要求 21 所述的方法，其中如果所述分组是从该防火墙接收的，则放弃该分组。

23、如权利要求 19 所述的方法，其中步骤 (d) 包括以一个优先权号码标注所述分组的步骤。

24、如权利要求 19 所述的方法，其中如果该分组作为多个分片被接收，则步骤 (d) 包括判定一个分片是否为一个重复分片的步骤，使得如果所述分片为一个重复分片，则该方法进一步包括以下步骤：

(e) 放弃所述重复分片。

25、如权利要求 19 所述的方法，其中步骤 (c) 是根据从该防火墙接收的至少一个指令判定的。

26、如权利要求 25 所述的方法，其中所述分组有一个目的地址，并且步骤 (d) 包括将所述分组转发给所述目的地址的步骤。

27、如权利要求 26 所述的方法，其中步骤 (d) 包括由所述预过滤模块在所述分组上执行至少一个动作的步骤，所述至少一个动作是根据来自该防火墙的一个指令确定的。

28、如权利要求 25 所述的方法，其中所述分组设有至少一个参数，所述至少一个指令根据所述至少一个参数标识所述分组为一个被允许分组，使得步骤 (c) 包括分析所述分组以取得所述至少一个参数的步骤。

29、如权利要求 28 所述的方法，其中该防火墙根据至少一个先前接收的分组的至少一个源地址和一个目的地址对所述至少一个先前接收的分组进行分类，所述源地址和所述目的地址一起形成一个连接，使得该防火墙将用于标识所述连接为一个被允许连接的所述源地址和所述目的地址作为所述至少一个指

令发送给所述预过滤模块。

30、如权利要求 29 所述的方法，其中该网络与多个接口通信，所述预过滤模块与所述多个接口中的每一个相连，使得步骤 (c) 包括判定所述分组是否是从所述被允许连接及一个被允许接口接收的步骤，使得只有当所述分组通过所述被允许接口从所述被允许连接接收时，所述分组才被允许。
5

快速分组过滤与处理系统、装置及方法

技术领域

本发明涉及一种用于分组交换网络上的快速分组过滤系统、装置及方法，尤其涉及一种通过基于话路的过滤提高分组过滤效率的系统、装置及方法。

背景技术

连通性与安全性是绝大多数机构的计算机环境的两个相互制约的目标，典型的现代计算机系统围绕网络通信而建立，提供对大量服务的透明访问。这些服务的全球化可能是现代计算机方案中的一个最重要的特征，对连通性的需求既来自机构内部也来自机构外部。

保护网络服务不被未经授权使用对任何机构都是头等重要的。随着对提高安全性的需求的增长，控制访问网络资源的手段已变成一种管理优先权。为了节约成本和维持产量，访问控制必须便于配置，并且对用户和应用而言必须是透明的。安装成本和故障时间的最小化也是重要因素。

分组过滤是一种方法，其允许连通但通过控制所通过的通信量提供安全性，因此既防止了单个网络内的也防止了相互连接网络之间的非法通信企图。

在此引入美国专利第 5, 835, 726 号（申请日为 1996 年 6 月 17 日）和第 5, 606, 668 号（申请日为 1993 年 12 月 15 日）作为参考，它们描述了通过在一个计算机网络中控制出入的数据分组流量而提供网络安全性的方法，该分组流量通过分组过滤控制，该分组过滤控制根据一个用户生成的规则库来执行，该用户生成规则库接着被转换成一组过滤语言指令。该规则库中的每个规则均包含一个源、目标、服务、接收还是拒绝分组，是否注册、加密、和/或鉴别事件。该组过滤器语言指令安装和执行于位于计算机内作为防火墙的检查

引擎上。检查引擎执行详细检查以判定一个分组是否应被允许通过防火墙。该防火墙位于计算机网络中使得所有进出该要被保护的网络的通信均被强迫通过防火墙。因此，当分组出入网络时，就会根据组成所述规则库的规则被过滤。

根据这些参考，检查引擎作为一个虚拟分组过滤机，其通过对每个分组判定拒绝还是接收分组。如果分组被拒绝，它就被放弃。如果它被接收，然后该分组就可能被修改。修改可能包括加密、解密、签名生成、签名验证或地址转换，所有的修改都根据该规则库中的内容进行。

不幸的是，该公开方法的一个缺陷是大量的计算负荷被施加到操作防火墙的计算机上。以前公开的分组过滤处理要求对每个分组进行单独分析，其通过与确定通过防火墙的分组入口所依据的规则组进行很多不同的比较来进行。但是，一旦在两个通过防火墙建立的节点之间的话路或连接已经判定被允许，那么在绝大多数情况下，更加细致的分析可能就不需要了。这样，来自一个被允许连接的分组的继续分析的要求将减少或甚至消除，这将显著地减少防火墙所带来的计算负荷，并加速分组过滤的过程，同时仍然保持被保护系统的安全性。

因此，需要一种下述的快速分组过滤系统、装置和方法（其将是实用的），即：根据从其接收一个分组的连接，进行快速分组过滤，使得如果一个分组是从一个被允许的连接接收的，则完全的分组分析的需求将被减少或消除，而同时仍然保持快速有效地修改分组的能力，优选地采用修改过程的硬件加速。

发明内容

本发明为一种通过增加一个具有预过滤模块的防火墙，加速一个分组交换网络（优选地是一个IP网络）上的分组过滤的系统、装置及方法。根据该分组是否是从一个先前被防火墙允许的连接接收的，该预过滤模块执行有关分组的有限动作组。如果该分组是从这样一个被允许的连接接收的，则该预过滤模块将该分组转发给它们的目的地，可选地在分组上执行一个或多个动作。否则，该分组将被转发给防火墙进行处理。优选地，一旦防火墙移交与预过滤模块连

接的责任，或“卸载”（OFF-LOADED）该连接，防火墙就不再从该连接接收其它分组，直到该连接发生超时，或者接收到一个带有特殊话路控制字段值（表明话路结束）的分组为止，使得该连接被关闭。

例如，对于本发明的关于IP网络的优选实施例中，这样一个话路控制字段值是一个为分组设置的FIN/RST标志。

减少或甚至是消除一个来自被允许连接的分组所需的分析量的一个优点是：防火墙可选择地增加硬件加速。该硬件加速的优点是比基于软件的分组处理快得多，从而能显著提高防火墙系统的效率。另外，修改程序的硬件加速可保持快速有效地修改分组的能力，因为修改程序需要较少的修改分组的“智能”而处理速度更快，而分组分析程序则具有与之相反的特征。因此，可选和优选地、该预过滤模块以硬件实现。

根据本发明，提供一种用于加速分组过滤的系统，该系统包括：(a)一个传输一个分组的源节点；(b)一个接收该分组的目的节点；(c)一个插置于该源节点和目的节点之间的防火墙，用于根据至少一个规则执行分组过滤；以及(d)一个与防火墙通信的预过滤模块，用于从该防火墙接收至少一个指令并在防火墙之前接收该分组，使得如果该分组根据该至少一个指令被允许，则该预过滤模块处理该分组，或者该预过滤模块将该分组转发给防火墙进行处理。

根据本发明的另一个实施例，提供一种网络上的分组加速过滤系统，该系统包括：(a)一个位于该网络上的防火墙，用于根据至少一个规则在该分组上执行分组过滤；以及(b)一个位于该网络上并与防火墙通信的预过滤模块，用于从防火墙接收至少一个指令，该至少一个指令判定一个简单比较，该预过滤模块还在防火墙之前接收在网络上传输的分组，使得如果该分组根据该简单比较被允许，则该预过滤模块至少在该网络上传输该分组。

根据本发明的又一个实施例，提供一种在一个用于加速分组过滤的系统中使用的用于在防火墙之前接收分组的装置，其中该系统具有一个用于传输分组的网络和一个该网络上的用于过滤该分组的防火墙，该装置包括：(a)一个存

储器，用于存储至少一个指令以分析来自防火墙的分组的至少一个参数，该至少一个指令包括标识该分组的至少一个参数；以及（b）一个分类引擎，用于分析该分组的至少一部分，并根据该至少一个指令将该分组的该至少一部分与该至少一个参数相比较。

根据本发明的再一个实施例，提供了一种与防火墙相连接的网络上加速分组过滤的方法，该方法包括下列步骤：（a）提供一个预过滤模块以在防火墙之前接收一个分组；（b）由该预过滤模块接收该分组；（c）判定该分组是否被允许；以及（d）如果该分组被允许，则由该预过滤模块处理该分组。

以下，术语“网络（network）”包括在任意两个或更多的允许数据传输的计算机装置之间的一种连接。

以下，术语“计算机装置（computational device）”包括但不限于装有操作系统如 WindowsTM、或 Linux 的个人计算机（PC）；MacintoshTM 计算机；装有 JAVATM-OS 操作系统的计算机；诸如 Sun MicrosystemsV 及 Silicon GraphicsTM 的计算机工作站；以及其他一些装有 UNIX 操作系统版本如 AIXTM 或 Sun MicrosystemsTM 的 SOLARISTM 的其他计算机；任何其他已知和能得到的操作系统的计算机；任何型号的计算机；任何可连接到分组交换网络并有一个操作系统（包括但不限于 VxWorksTM 和 PSOSTM）的装置；或任何可连接到分组交换网络的装置，该装置可传输及接收分组，并至少有一个数据处理器，例如一个网络处理器，包括但不限于一个桥接器、一个开关或一个路由器。以下术语“视窗（WindowsTM）”将包括但不限于由微软公司提供的 WindowsNTTM、Windows98TM、Windows2000TM、WindowsCETM 和上述操作系统的任何升级版本。

本发明的方法可被描述为由一个数据处理器执行的一系列步骤，这些方法可选择软件、硬件、固件或它们的结合来实现。对于本发明，可以用基本上任何一种合适的程序语言（本领域的普通技术人员可以容易地选择出来）来编写一个软件应用程序。所选择的程序语言应当与根据其执行软件应用程序的计算机装置相匹配。合适的程序语言的例子包括但不限于 C、C++ 和 JAVA。

附图说明

通过下面参照附图对本发明具体实施例的详细描述，可以更好地理解本发明的前述的和其他的目的、方面和优点。其中：

图 1 为本发明的一个系统的示意方框图；

图 2 为本发明的图 1 的预过滤模块的示例优选实施例的示意方框图；

图 3 为本发明的示例方法的流程图。

具体实施方式

本发明为一种通过增加一个具预过滤模块的防火墙加速分组过滤的系统、装置和方法。该预过滤模块执行一个关于该分组的简单比较，例如根据该分组是否是从一个已先前被防火墙允许的连接接收的。如果该分组是从这样一个被允许连接接收的，那么该预过滤模块就将该分组转发给其目的地，可选地，在分组上执行一个或多个动作。否则，该分组将被转发给防火墙进行处理。另外，优选地，如果这些分组带有需要防火墙干预的特殊的话路控制字段值，则该分组被转发给防火墙进行处理。例如，对于本发明的关于 IP 网络，特别是关于 TCP/IP 通信的 IP 网络的实施例中，这样的话路控制字段值包括一组该分组的 SYN/FIN/RST 标志，这样的话路控制字段值标明了携带有连接状态信息的分组，因此对防火墙判定该连接状态以进行分组的接收和分析很重要。可选地，如果该预过滤模块不能执行某些功能，则分片分组也被转发给防火墙，该某些功能为比如本发明的关于 IP 网络，特别是关于 TCP/IP 通信的 IP 网络的实施例中的虚拟合片（virtual defragment）功能。

一旦防火墙已判定一个连接被允许，或具有允许执行该简单比较的至少一个参数，则该防火墙就优选地把一个带有该新被允许分组的详细内容的信息发送给该预过滤模块。优选地，一旦防火墙转交与预过滤模块连接的责任，或“卸载”（OFF-LOADED）该连接，则防火墙不再从该连接接收其他的分组，直到该连

接发生超时 (timeout)，或者接收到一个带有特殊的话路控制字段值（表明话路结束，如在 IP 网络实施例中的 FIN/RST 标志）的分组为止，使得该连接被关闭。如果在一段预定时间内防火墙没有接收到一个分组则发生“超时”。

为了利用硬件加速的优点，该预过滤模块优选以硬件实现，这种硬件加速要比基于软件的分组处理快得多。因此，尽管该预过滤模块也能够以软件或固件实现，但是该预过滤模块优选以基于硬件的装置实施。可选地，为方便安装与操作起见，该预过滤模块及防火墙可作为一个组合装置实现，它们可以是一个增加于一个网络的网关节点的“黑匣子”，或者作为该网关节点的替代物。

本发明的系统、装置与方法的原理与操作可参考附图和相关说明得以更好的理解，应该理解的是这些附图仅为了说明本发明而给出的，并不用于限制本发明。虽然以下说明以 IP 网络特别是关于 TCP/IP 分组通信的 IP 网络为主展开，但应该理解的是仅为了说明本发明而给出的，并不用于以任何方式限制本发明。

现在参看附图，图 1 为本发明的一个系统的示意方框图，系统 10 设有一个被保护的分组交换网络 12，使得数据以分组的形式传输。被保护的网络 12 由一个网关 16 与一个外部的分组交换网络 14 隔开，该网关 16 可选地为任何类型的计算机装置，这里也可称做“中间节点”。例如，外部网络 14 可选地为因特网，网关 16 通过一个硬件连接器，如图示的 NIC17，与每一个外部网络 14 和被保护的网络 12 相连。

网关 16 操作一个用于执行分组分析和分组过滤的防火墙 18。被允许从外部网络 14 通过网关 16 的分组接着被多个被保护的节点 20 中的一个接收，该被保护的节点 20 连接到被保护的网络 12。这种网络通信是典型的双向，使得分组从被保护的网络 12 被网关 16 接收以传输给外部网络 14，反之亦然。

防火墙 18 可优选地如前述的美国专利 5, 835, 726 及 5, 606, 668 所说明的那样实施。防火墙 18 设有一个分组过滤器 22 用于执行分组过滤。分组过滤器 22 依次优选地包括一个分析模块 24 用于分析分组、以及一个规则库 26。

规则库 26 优选包括一个或多个根据系统管理员或其他控制用户的偏爱所确定的规则。分析模块 24 将被分析的分组的内容抽出并与规则库 26 中的规则相比较。如果比较结果是根据规则库 26 该分组被允许，则分组过滤器 22 允许该分组进入被保护的网络 12。

另选地，如果该分组根据规则库 26 不被允许，则可选地放弃该分组；如果规则库 26 不是特别允许该分组通过，则该分组也可被可选地判定为不被允许。

另外可选且优选的是，如果分组被接收，分组过滤器 22 设有一个修改模块 28 用于对分组进行修改。

防火墙 18 的其他可选功能包括：能够执行分组计数，以判定属于一个特定连接的所有分组上被传输的数据量；能够修改分组内的地址；能够加密分组。具体的分组加密已在前述的美国专利 5, 835, 726 中有所描述，简言之，分组可选地被加密后在两防火墙 18 之间进行传输，使得分组被加密以通过外部网络 14。例如，加密也可以可选地用于防火墙 18 和外部网络 14 的一个节点之间的通信。被加密的分组然后由接收方的防火墙 18 解密并被传递给被保护的网络 12。因此，解密和传输的过程是自动的，并以一种对通信软件透明的方式进行。

防火墙 18 的这些设置按照前述的美国专利 5, 835, 726 及 25, 606, 668 优选地实施。但是，在被允许进入网关 16 之前，通过防火墙 18 传递所有的分组将会给防火墙 18 带来极大的计算负荷。因此，根据本发明，网关 16 也设置有一个在防火墙 18 之前接收分组的预过滤模块 30，但是其优选地直接与被保护的网络 12 相连。就被允许进入被保护的网络 12 的分组而言，预过滤模块 30 也优选地从防火墙 18 接收指令。更优选地，这些指令由防火墙 18 根据先前接收的一个或多个相关分组的分析来确定，使得如果一个先前接收的相关分组已被允许进入被保护的网络 12，则当前分组也应被允许进入被保护的网络 12。因此，如果预过滤模块 30 判定当前分组被允许进入，那么优选地，预过滤模

块 30 将该分组直接传递给被保护的网络 12。

为了提高预过滤模块 30 的操作效率，优选地预过滤模块 30 只执行每个分组的限定分析。特别是，更加优选地，每个分组只有一部分被预过滤模块 30 分析。最优先地，预过滤模块 30 只根据一个简单比较分析每个分组。通过“简单比较”是指以一个或多个预定义参数的形式抽出信息，其中该预定义参数被与这些参数的一个预定义模式相比较。

在一个简单比较的具体优选实施例中，分组只在预过滤模块 30 能够判定该分组是否是通过一个允许的数据传输接收的之前被分析。这样一个允许的数据传输可以被称为是一个源节点和一个目标节点之间的一个连接，该源节点例如从外部网络 14 启动该连接，而该目标节点例如一个被保护的节点 20 接收该连接。可以理解为一旦该连接建立，该源节点和目标节点之间的通信可选地为双向的。

关于分组分析，一个“连接”是根据至少一个，优选为多个的描述分组所属数据传输的参数来确定的。这些参数的例子包括但不限于：源地址及该分组的端口、目标地址及该分组的端口、该分组的协议及分组被通过其接收的接口。该连接被用于对分组进行分类、并判定分组是否被允许出入或离开被保护的网络 12。

防火墙 18 根据一个或多个先前被接收并被检查的分组确定每一个连接。防火墙 18 根据带有规则库 26 的分析模块 24 的输出检验分组的内容、判定来自相应连接的分组是否应被允许进入和/或离开被保护的网络 12。另外，根据存储在规则库 26 的规则，分析模块 24 能够判定一个或多个与每一个连接关联的动作。这些动作的例子包括但不限于：执行计数动作以计数分组内的数据量、加密/解密分组、通过重写地址字段执行网络地址转换（NAT）等等。一个修改分组的优选实施例是，通过由预过滤模块 30 根据防火墙 18 的指令而分配给分组一个优先权号码来标记分组。该优先权号码确定了分组的传输顺序，从而确定其“优先权”。

防火墙 18 接着将相关指令传递给预过滤模块 30，该指令至少涉及分组是否被允许进入被保护的网络 12，而更优选地，还涉及来自该连接的后续分组所应采取的动作。

可选的且优选的，预过滤模块 30 执行一个防欺骗方法。因为预过滤模块 30 可选地被连接于多个网络，分组可来自于这些网络中的任何一个。该防欺骗方法判定标有最初来自某网络的 IP 分组是否真的来自那个网络。因为预过滤模块 30 知道哪个网络与哪个接口连接，所以预过滤模块 30 可判定从一个特定接口接收的一个分组是否被允许。

在一个加速器如预过滤模块 30 中实现防欺骗方法的最简单方式是：将有关网络接口的信息作为预过滤模块 30 能够得到的连接信息的一部分。因此，如果一个来自一个允许的源节点的分组被发送给一个允许的目的地，并且已通过预定接口到达，则该分组可被预过滤模块 30 处理。另选地且可选地，即使只有接口不正确，预过滤模块 30 也可判定分组违法，其应由防火墙 18 进一步检查分组是否有效。还有不将接口作为预过滤模块 30 的一部分的其他方式实现防欺骗方法，也包括在本发明的范围内。

如图 2 所示在预过滤模块 30 的优选实施例中，预过滤模块 30 是以硬件实现的，或至少是以固件实现的，而不是以纯软件实现的。硬件的好处是执行所需动作要比软件快得多，图 2 的示意方框图是一个预过滤模块 30 部件的基于逻辑而不是结构的示意图。例如，部件间的物理连接未图示，该连接可以是一个比如所有部件都连接在其上的 PCI 总线。可选地，部件可以通过基本上任何型号的内部和/或外部总线进行连接。

在该实施例中，预过滤模块 30 可被描述为一个“装置”；优选地设有一个存储器 36。预过滤模块 30 设有一个连接数据库 32 用于存储来自防火墙 18 的指令，该数据库存储在存储器 36 中。连接数据库 32 存储至少一个或多个确定连接所需要的分组的参数，但也优选地存储至少一个要在来自该连接的分组上执行的动作。

预过滤模块 30 也优选地设有一个包括一个数据处理器的分类引擎 38，以至少部分地分析来自分组的信息，并从连接数据库 32 取得信息。预过滤模块 30 也优选地设有一个修改器 34，用于执行来自该连接的分组的一个或多个相关动作，该动作优选地存储于前述的连接数据库 32 内。

预过滤模块 30 也可选并优选地传输关于传送给防火墙 18 的至少一个分组的特定、选择信息，这些选择信息可选地包括至少但不限于前述的用于分析分组的参数中的一个。预过滤模块 30 与防火墙 18 之间的通信可选并优选地根据数个实施例之一进行。在第一个实施例中，在一个状态或事件驱动的实现中，预过滤模块 30 一接收这样的信息就主动通知防火墙 18。另选地，在一个第二实施例中，在轮询的实现中，防火墙 18 询问预过滤模块 30。例如，该轮询可选地在一个特定时间间隔过后、或者根据一个例如向系统管理者的对此信息的用户询问而执行。

另外，预过滤模块 30 也可优选地设置至少一个，而优选地为多个网络接口，如图示的 MAC（媒体存取控制）40，它是发送及接收来自物理网络（未图示）的分组的硬件。预过滤模块 30 更优选地设有一个防火墙接口 42，以向防火墙发送分组并从防火墙（未图示）接收分组。

操作流程优选地如下列所述。分组可选地从标为“MAC1”的 MAC40 接收，然后被传送给分类引擎 38。在从存储器 36 内的数据库 32 中取得的信息和指令的协助下，分类引擎 38 然后就分析每个分组中的信息的至少一部分，并判定该分组是否被允许。如果该分组被允许，那么就传送给修改器 34，以根据来自防火墙（未图示）的至少一个指令选择性地修改，使得如果不修改，则防火墙就不发出该至少一个相关的指令。

防火墙可选地能够判定应向其发送一个分组的接口，如一个特定的 MAC40。但是，应注意的是，虽然防火墙可指令预过滤模块 30 将分组转发给一个特定接口，但是如果支持路由选择，则该路由选择应被用于路由选择该分组的路径，而不是路由选择来自防火墙（未图示）的指令的路径。

另选地，分组可选且优选地被转发给防火墙。还有另选地是，在下述更加详细描述的特定条件中，分组可被放弃，特别是从防火墙接口 42 接收的分组（其可选地被类似地分析）。为了避免放弃可能不是 IP 分组的分组，可选并优选的是，关于一个或多个“错误”分组类型的信息可被存储在数据库 32 中，以便如果这些信息没有被存储于在数据库 32 中，则分组就被确定为“不被允许的”。该“错误”分组类型的一个例子是一个 ARP (address resolution protocol 地址解析协议) 分组。

从如图 2 所示的预过滤模块 30 的实现中可看到，分组可选地从一个外部源例如 MAC40 到达预过滤模块 30，或者也可从防火墙接口 42 接收分组。如果分组从防火墙接口 42 接收，它可能已经由防火墙本身生成，或者也可能已经由主机的 IP 堆栈生成并转发。因此，可选并更优选的是，对于这样通过防火墙接口 42 所接收的分组，如果它们不被允许则预过滤模块 30 能够放弃它们，而不是将其转发给防火墙。因此，可选且优选地，至少部分地根据接收分组所通过的接口，执行预过滤模块 30 是放弃还是传送分组的判定。

当然，预过滤模块 30 也有包含在本发明的范围内的其他实现方法。

图 3 是用于操作本发明的一个示例方法的流程图。在步骤 1，一个分组被预过滤模块接收。在步骤 2，至少该分组的一个参数被该预过滤模块取得；在步骤 3，至少一个参数被用于检查已知的连接，优选地通过在这些已知的连接表中进行查找来执行。

在步骤 4a，如果找到该分组的一个入口，则该预过滤模块执行一个或多个为该连接所设定的动作；在步骤 5a，该分组被转发给其目的地；如果该分组有特定的路控制字段值（如一组使分组经过 IP 网络被传递的 SYN/FIN/RST 标志），则将不执行步骤 4a 和 5a，这种情况下，该分组被优选地转发给防火墙进行处理。该话路控制字段值标明携带的连接状态的信息的分组，因此为了判定该连接的状态，该话路控制字段值对于防火墙的接收及分析有重要意义。

可选地，如果该预过滤模块不能执行某些功能，比如本发明的关于 IP 网

络，特别是关于 TCP/IP 通信的 IP 网络的实施例中的虚拟合片功能，则分片分组也被转发给防火墙。在 IP 分组变得太大而不能被传输，分组被分成多个较小的分组（叫做分片）之后，将执行虚拟合片功能。虚拟合片是将所有接收的分片重新组装成原先的大分组的过程。

为防止各种由分片所带来的攻击，优选地，本发明的预过滤模块，或者防火墙，放弃重复的分组分片。换句话说，如果一个先前接收的分片被再次接收，则该分片被放弃。

再回到图 3 的流程图，另选地，在步骤 4b 中，如果在连接表中未找到分组入口，那么该分组被转发给防火墙进行处理。在步骤 5b 中，如果防火墙判定该分组所属的连接被允许，则可选地防火墙发送带有关于新连接信息的消息给预过滤模块。该消息优选地包括一个标识新连接的关键字、及关于地址转换的信息和可选地关于加密的信息，二者均为包括该分组本身修改的程序。标识新连接的关键字优选地包括信息诸如：源 IP 地址及端口、目的 IP 地址及端口、协议字段、及可选地一个分组被预定通过其接收以进行防欺骗保护的接口。地址转换信息包括所转换的源 IP 地址及端口、和目的 IP 地址及端口。

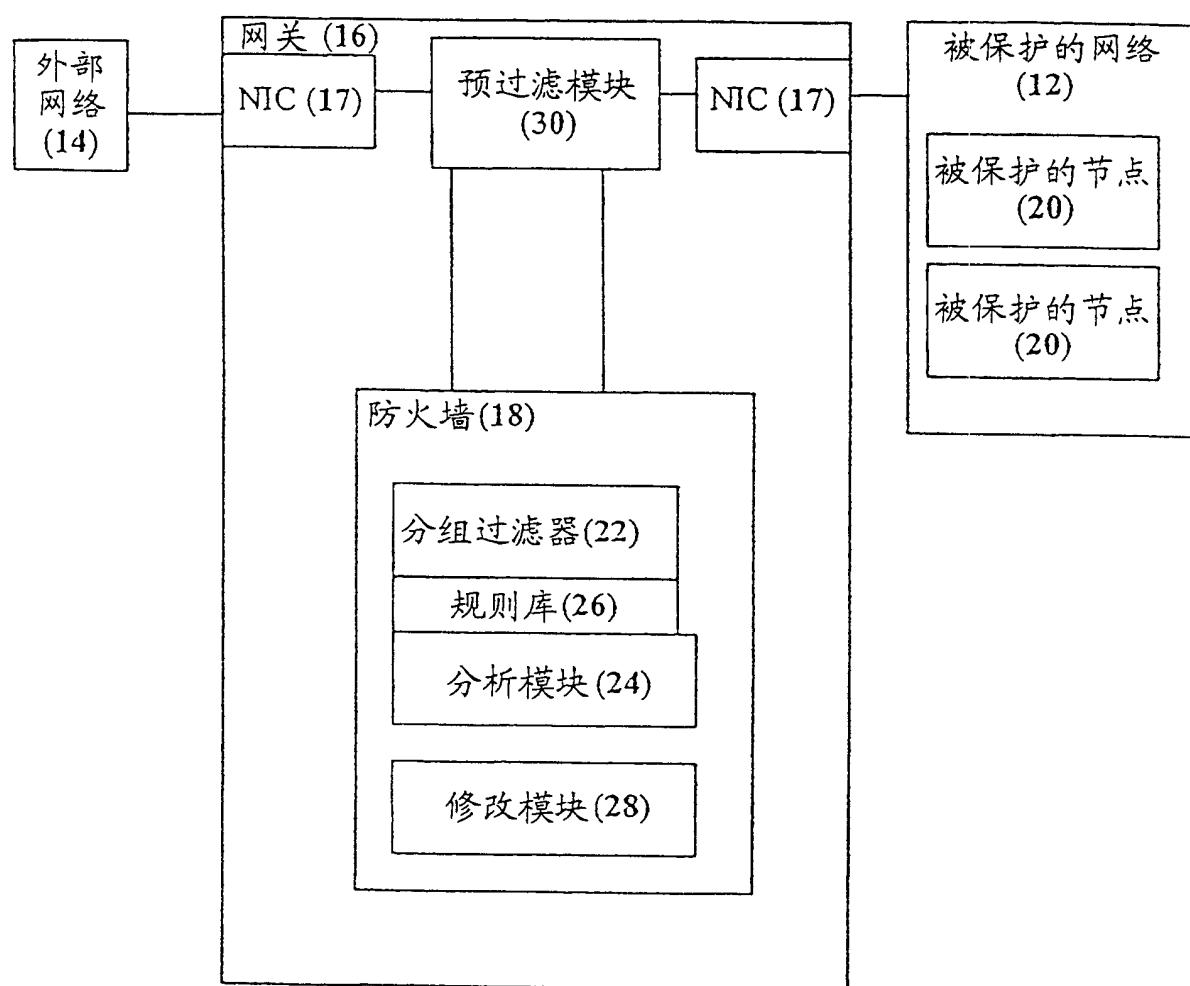
根据本发明的优选实施例，一旦防火墙将该消息发送给该预过滤模块，则连接就会被“卸载”给预过滤模块，这样防火墙将不再接收该连接的任何分组。优选地，防火墙不再接收任何其他的分组，直到接收到该连接的一个带有特定话路控制字段值（表明话路结束，如在 IP 网络实施例中的 FIN/RST 标志）的分组为止。

更加优选的是，当在一个特定时间段内未接收到一个特定连接的分组时，就会发生超时。因为防火墙没看到该卸载的连接的任何分组，所以防火墙就会询问预过滤模块接收到该连接的分组的上一次时间，根据接收到的答复，防火墙再决定保留还是删除该连接。如果防火墙删除该连接，则优选地从预过滤模块的该表中删除该连接。

根据本发明的其他优选实施例，防火墙以规则时间间隔从预过滤模块接收

修改的计数信息，该信息可选并优选地被预过滤模块发给防火墙，而不是使防火墙轮询预过滤模块。计数信息优选地包括：从计数信息最后一次被修改，以及从一个特定连接的分组被预过滤模块最后一次接收以来，预过滤模块所接收的该特定连接的分组及字节的数目。该信息然后在预过滤模块内被复位，可选且更优选地，如果预过滤模块删除该连接，则预过滤模块将该连接的上一次的计数信息发给防火墙。

应该理解的是上述说明仅仅用作例子，在本发明的精神和范围内还有许多其他的实施例。



10

图 1

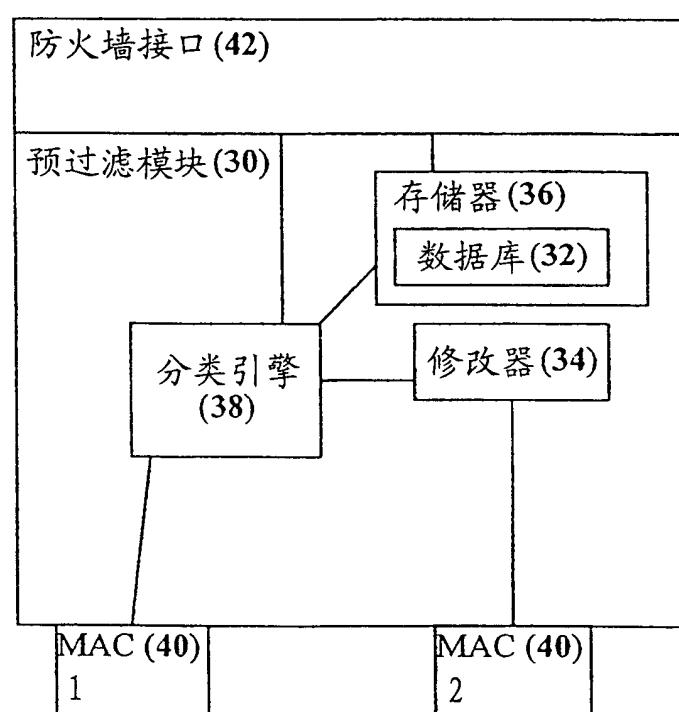


图 2

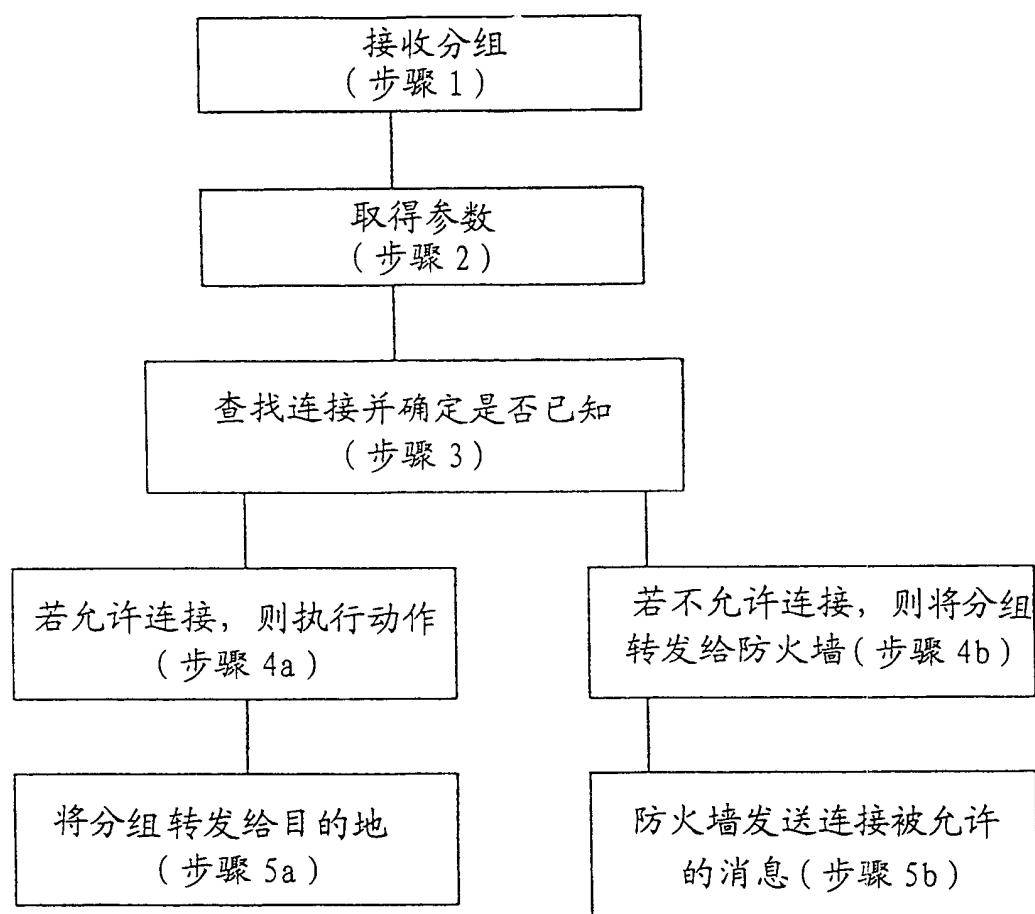


图 3