(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 104079555 B
(45)授权公告日 2017.10.20

(21)申请号 201410214881.7

(22)申请日 2007.02.16

(65)同一申请的已公布的文献号
申请公布号 CN 104079555 A

(43)申请公布日 2014.10.01

(30)优先权数据
60/773,820 2006.02.16 US
11/591,802 2006.11.01 US

(62)分案原申请数据
200780013323.2 2007.02.16

(73)专利权人 技术卫士安全有限责任公司
地址 美国密苏里州

(72)发明人 D·E·梅斯塔斯 B·L·库珀

(74)专利代理机构 北京市中咨律师事务所 11247
代理人 杨博 杨晓光

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 21/55(2013.01)

(56)对比文件
US 2004015309 A1,2004.01.22,
US 6040834 A,2000.03.21,
CN 1736076 A,2006.02.15,
US 2004128355 A1,2004.07.01,
US 6754662 B1,2004.06.22,

审查员 孙丽

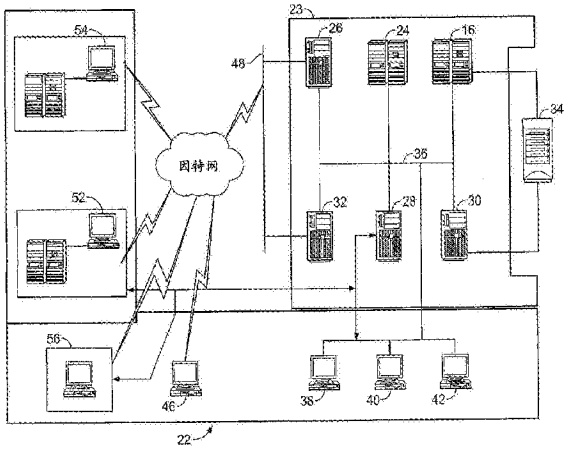
权利要求书1页 说明书13页 附图5页

(54)发明名称

用于确定数据流的系统和方法

(57)摘要

描述了一种用于确定数据流的方法。该方法包括:生成包括地图的图形用户接口;接收对所述地图上的点的选择;当接收到对所述点的选择时,显示多个结果;接收对所述结果之一的选择;以及向所述点分派所述结果之一。



CN 104079555 B

1.一种用于确定计算机网络中的数据流的方法,所述方法包括:

生成包括地图的图形用户接口;

接收对所述地图上的点的选择;

当接收到对所述点的选择时,显示多个结果;

接收对所述结果之一的选择,其中所述结果之一是以下三个选项中的一个:拒绝分组通过防火墙,允许分组通过所述防火墙,或者向分组分派优先级;以及

向所述点分派所述结果之一,其中所述向所述点分派所述结果之一包括:将所述结果之一应用于从所述点表示的物理位置接收的分组。

2.根据权利要求1所述的方法,其进一步包括显示世界地图。

用于确定数据流的系统和方法

[0001] 本申请为申请号200780013323.2、申请日2007年2月16日、名称为“用于确定数据流的系统和方法”的分案申请。

技术领域

[0002] 本发明一般地涉及计算机网络，并且更特别地，涉及用于确定数据流的系统和方法。

背景技术

[0003] 常规的基于规则的计算机安全防火墙基于变化复杂的规则集合或“规则库”。将进入这样的防火墙的数据分组与一个或多个规则库中的信息和规则进行比较，以便确定是否应当允许该数据分组通过防火墙。围绕逻辑比较的概念，例如布尔逻辑，以及通过规则列表的顺序规则流来构造规则库。随着规则库变得越来越复杂，其要求更多的系统和处理器开销。因此，使用防火墙的组织常常在规则库复杂性与所意识到的所需数据吞吐量之间进行折衷，牺牲某些安全性来支持性能。

发明内容

[0004] 在一个方面中，描述了一种用于确定数据流的方法。该方法包括：确定包括第一集合内第一数目的至少一个比特的分组是否基于所述第一集合内的所述至少一个比特而被分派分类值，以及当确定所述分组被分派所述分类值时，确定将要应用于所述分组的结果。该方法进一步包括：当确定所述分组不能够基于所述分组的所述第一数目的至少一个比特而被分派所述分类值时，通过处理器来分析所述分组的第二集合内第二数目的至少一个比特。

[0005] 在另一方面中，描述了一种处理器。所述处理器被配置以便确定包括第一集合内第一数目的至少一个比特的分组是否基于所述第一集合内的所述至少一个比特而被分派分类值，以及当确定所述分组被分派所述分类值时，确定将要应用于所述分组的结果。所述处理器进一步被配置以便当确定所述分组不能够基于所述分组的所述第一数目的至少一个比特而被分派所述分类值时，分析所述分组的第二集合内第二数目的至少一个比特。

[0006] 在又一方面中，描述了一种计算机可读介质。所述计算机可读介质被编码于计算机程序内，其被配置以便确定包括第一集合内第一数目的至少一个比特的分组是否基于所述第一集合内的所述至少一个比特而被分派分类值，当确定所述分组被分派所述分类值时确定将要应用于所述分组的结果，以及当确定所述分组不能够基于所述分组的所述第一数目的至少一个比特而被分派所述分类值时，分析所述分组的第二集合内第二数目的至少一个比特。

[0007] 在再一方面中，描述了一种用于确定数据流的方法。所述方法包括生成包括地图的图形用户接口，接收对所述地图上的点的选择，在接收到对所述点的选择时显示多个结果，接收对所述结果之一的选择，以及将所述结果之一分派给所述点。

附图说明

[0008] 图1是用于确定数据流的系统的一实施例的框图；

[0009] 图2是用于确定数据流的系统的一实施例的详细框图；

[0010] 图3是用于确定数据流的系统的另一实施例的框图；

[0011] 图4是由图3的系统的处理器接收的数据分组的一实施例的示图；

[0012] 图5是用于确定数据流的方法的一实施例的流程图；以及

[0013] 图6是用于创建多个表格的图形用户接口(GUI)的一实施例。

具体实施方式

[0014] 图1是用于确定数据流的系统10的一实施例的框图。系统10包括服务器系统12和连接到服务器系统12的多个用户设备14。如文中所使用的，术语“服务器”并不仅限于本领域中被称为计算机的那些集成电路，而是广泛地指代处理器、微控制器、微型计算机、可编程逻辑控制器、专用集成电路、任何其它的可编程电路，以及硬件和软件的任何组合，并且在文中可互换地使用这些术语。在一个实施例中，用户设备14是包括Web浏览器的计算机，并且服务器系统12经由网络(例如，局域网(LAN)和广域网(WAN))可访问用户设备14。LAN可以包括内联网并且WAN可以包括因特网。

[0015] 用户设备14通过很多接口(包括拨号连接、线缆调制解调器以及高速综合业务数字网(ISDN)线路)互连至网络。可选地，用户设备14包括基于Web的电话或其它基于Web的可连接设备，其能够互连至网络。服务器系统12包括连接到中央数据库18的数据库服务器16，中央数据库18包括用于确定数据流的方法。

[0016] 在一个实施例中，中央数据库18存储在数据库服务器16上，并且可以借助于通过用户设备14之一登录到服务器系统12，由用户设备14之一处的潜在用户来访问。在一个实施例中，远离服务器系统12来存储中央数据库18。

[0017] 图2是用于确定数据流的系统22的一实施例的详细框图。系统22包括服务器系统23。服务器系统23是服务器系统12的例子。服务器系统23包括数据库服务器16、应用服务器24、Web服务器26、传真服务器28、目录服务器30以及邮件服务器32。盘存储单元34(其是单个数据库)耦合于数据库服务器16和目录服务器30。

[0018] 服务器16、24、26、28、30和32耦合于局域网(LAN)36中。可选地，WAN可用于替代LAN36。另外，系统管理员工作站38、用户工作站40和监管工作站42耦合于LAN36。每个工作站38、40和42均是具有Web浏览器的个人计算机。

[0019] 服务器系统23在通信上耦合于由个人或职员操作的各种工作站52和54。个人或用户操作工作站52可以访问服务器系统23。工作站52和54是具有Web浏览器的个人计算机。工作站54位于远程位置。服务器系统23也经由因特网服务提供商(ISP)连接48在通信上耦合于工作站46。

[0020] 此外，传真服务器28通过电话链路与工作站52以及任何远程位置的用户系统(包括工作站56)进行通信。每个工作站38、40、42、46、52、54和56都是用户设备14的例子。传真服务器28也与其它工作站38、40和42通信。服务器系统23执行文中所描述的方法以便确定数据流。

[0021] 示例性实施例中的通信被描述为通过因特网来实现，然而，在其它实施例中可以利用任何其它的广域网(WAN)类型通信。用于确定数据流的系统和方法并不限于通过因特网来实施。在一个实施例中，用于确定数据流的方法被存储在盘存储单元34，其是计算机可读介质的例子，并且通过服务器16、24、26、28、30和32中的任何一个来执行。计算机可读介质的其它例子包括软盘、只读光盘存储器(CD-ROM)以及数字视频盘(DVD)。

[0022] 图3是用于确定数据流的系统100的一实施例的框图。系统100包括处理器102、存储设备104、输入设备106以及输出设备108。处理器102可以是操作Linux™操作系统的x86体系结构或操作Linux™操作系统的x86_64体系结构。x86体系结构可从Intel™公司获得，并且x86_64体系结构可从Advanced Micro Devices™(AMD)公司获得。存储设备104的例子包括随机访问存储器(RAM)和只读存储器(ROM)。输入设备106的例子包括鼠标和键盘。输出设备108的例子包括阴极射线管(CRT)和液晶显示器(LCD)。如文中所使用的，术语“处理器”并不仅限于本领域中被称为处理器的那些集成电路，而是广泛地指代计算机、微控制器、微型计算机、可编程逻辑控制器、专用集成电路以及任何其它的可编程电路。

[0023] 处理器102执行用于确定数据流的方法。在一个实施例中，处理器102是基于安全策略防止数据分组在两个网络(例如因特网和内联网)之间通信的防火墙。

[0024] 图4是通过处理器102接收的数据分组150的一实施例的示图。分组150包括版本152、网际协议(IP)网络地址以及数据156。版本152的例子包括IP网络地址的IPv4版本和IPv6版本。分组150的IP网络地址的例子包括源地址或目的地址。源地址是分组150的发送源(例如工作站52)的地址。目的地址包括分组150的接收方或目的地(例如工作站38或40)的地址。在一个实施例中，分组150还包括分组150的报头的报头长度、将要提供给分组150的服务类型、分组150的总长度、由处理器102用来确定报头的所有比特是否都有效的报头校验和、分组150的生存时间、用于确定是否对分组150进行分段的多个标志，以及由处理器102用来确定分组150是否是IP数据报的一部分的分段偏移。在一个实施例中，如果分组150的IP网络地址是源地址，则分组150进一步包括目的地址，并且如果分组150的IP网络地址是目的地址，则分组150包括源地址。

[0025] 图5是用于确定数据流的方法200的一实施例的流程图。处理器102接收202分组150，并且从分组150获得204或提取N个比特。N的例子包括3、4、6、8或10。N个比特的另一例子包括小于分组150的IP网络地址的32个比特。而N的其它例子包括小于分组150的IP网络地址的128个比特。N个比特的另外其它的例子包括除了分组150的IP网络地址的8个最高有效比特(MSB)中的3个最低有效比特(LSB)和3个MSB之外的2个比特。N的其它例子包括分组150的IP网络地址的8个MSB中的2个LSB。处理器102基于分组150的版本152确定分组150的IP网络地址位于分组150的比特β之前以及比特α之后，并且从分组150的IP网络地址中提取在比特α与比特β之间的N个比特。作为另一例子，处理器102基于分组150的版本152确定数据156位于分组150的比特η之前以及比特γ之后，并且从数据156中提取在γ和η比特之间的N个比特。作为又一例子，处理器102基于分组150的版本152确定端口地址位于分组150的比特ω之前以及比特σ之后，并且从端口地址中提取在σ和ω比特之间的N个比特。端口地址的例子包括由源执行的源计算机应用的源端口地址(例如，传输控制协议(TCP)或用户数据报协议(UDP)端口号)，以及由目的地执行的目的地计算机应用的目的端口地址(例如，TCP或UDP端口号)。作为另一例子，处理器102从分组150的IP网络地址中提取N个比特中的一些

并且从端口地址中提取N个比特的其余部分。

[0026] 处理器102基于分组150的N个比特确定206分组150是否可以被分类。处理器102通过将N个比特与经由输入设备106由用户提供给存储设备104的表I进行比较而确定206分组150是否可以被分类。

[0027]

行号	子范围	分类值	结果
1	R1-R2	C1	S1
2	R3-R4	C2	S2
3	R5-R6		
4	R7-R8		
5	R9-R10		
6	R11-R12		

[0028] 表I

[0029] 表I内的子范围R1-R2、R3-R4、R5-R6、R7-R8、R9-R10以及R11-R12形成了有限集合，例如端口地址的M个比特的集合、诸如用户名和口令的授权数据的M个比特的集合，IP网络地址的M个比特的集合，以及IP网络地址和端口地址组合的M个比特的集合。分类值C1和C2的例子包括标识多个国家的国家代码集合、标识多个子区域的子区域代码集合、标识多个计算机黑客的黑客代码集合、标识多个计算机垃圾邮件发送者的垃圾邮件发送者代码集合、标识多个计算机病毒的病毒代码集合、标识多个Trojan(木马病毒)的Trojan代码集合、标识多个计算机蠕虫(worm)的蠕虫代码集合、标识多个钓鱼者(phisher)的多个钓鱼代码、标识经由后门获得对连接至处理器102的计算机网络的访问的多个入侵者的入侵者代码集合、标识多个北大西洋公约组织(NATO)国家的NATO国家代码集合、标识多个公司的公司代码集合、标识多个政府机构的政府机构代码集合、标识多个因特网服务提供商(ISP)的ISP代码集合、标识多个产业部门的产业部门代码集合，以及标识多个国防部(DoD)的DoD代码集合。例如，C1是加拿大的国家代码，并且C2是美国(USA)的国家代码。产业部门的例子包括石油产业、飞机产业、计算机软件产业以及游戏和娱乐产业。

[0030] 结果或过程S1和S2的例子包括处理器102接受或拒绝分组150。结果S1和S2的其它例子包括向分组150分派优先级或不分派优先级。结果的其它例子包括向分组150分派服务质量(QoS)。QoS的例子包括在到达目的地时未丢弃分组150。QoS的其它例子包括在到达目的地时未延迟分组150。处理器102接受分组150包括允许分组150通过从一个计算机网络到另一个计算机网络的防火墙而到达目的地。处理器102拒绝分组150的例子包括由处理器102发送分组150，用于将过程之一应用于伪装成系统100来诱骗攻击者(例如黑客的垃圾邮件发送者)的honeypot(蜜罐)，以便确定攻击者的特征并向执法机构描述攻击者的特征。拒绝分组150的例子包括删除分组150以防止分组150进一步穿过网络。处理器102拒绝分组150的另一个例子包括不允许分组150穿过防火墙到达目的地。作为另一个例子，处理器102拒绝分组150包括由处理器102将分组150分流(shunting)到另一个处理器102，用于实现对分组150的“Whois”查询(域名查询)、美国国际号码注册机构(ARIN)查找中的至少一个，以及在计算机网络中跟踪分组150的路由，以便确定发送分组150的攻击者。一旦确定了攻击者，处理器102便向执行机构报告该攻击者。

[0031] 处理器102将分组150的N个比特与表I中的每个子范围R1-R2、R3-R4、R5-R6、R7-R8、R9-R10以及R11-R12的M个比特进行比较，以便确定子范围之一是否具有与这N个比特相匹配的M个比特。注意到M等于N。一旦确定了子范围之一，例如R1-R2，具有与这N个比特相匹配的M个比特，处理器102便向分组150分派对应的分类值之一，例如C1。举例来说，一旦确定这N个比特与子范围R3-R4的M个比特相匹配，处理器102便向分组150分派分类值C2。如果处理器102确定表I内的分类值中存在一个分类值对应于表I的子范围R1-R2、R3-R4、R5-R6、R7-R8、R9-R10和R11-R12中具有与这N个比特相匹配的M个比特的一个子范围，则处理器102确定分组150被分类。另一方面，如果处理器102确定表I内的分类值中不存在一个分类值对应于表I的子范围R1-R2、R3-R4、R5-R6、R7-R8、R9-R10和R11-R12中具有与这N个比特相匹配的M个比特的一个子范围，则处理器102确定分组150不能被分类。例如，一旦比较了M和N个比特，处理器102便确定分组150的N个比特与并不对应于分类值C1和C2之一的子范围R5-R6内的M个比特相匹配。在该例中，一旦处理器102确定这N个比特并不对应于分类值C1和C2之一，处理器102便确定分组150不能被分类。

[0032] 在确定了分组150被分类时，处理器102要么提供208对应于分类值之一的结果S1和S2之一或者过程，要么向将结果之一应用于分组150的另一处理器102(例如包括在工作站52内的处理器)发送分组150。举例来说，一旦确定分组150在分类值C1的情况下被分类，处理器102便将结果S1应用于分组150。作为另一例子，一旦处理器102确定分组150具有分类值C2，处理器102便向将结果S2应用于分组150的另一处理器(例如包括在工作站54内的处理器)发送分组150。一旦确定分组150被分类，处理器102便不检查分组150中除了N个比特之外的其它比特。

[0033] 下面提供的表II是表I的一例子。

[0034]

行号	IP 网络地址子范围	国家代码	国家	结果
1	0	148	保留	接受
2	1-2	199	未分派	拒绝
3	3-4	189	美国	接受
4	5-9	199	未分派	拒绝
5	10-22	148/189	保留，美国	接受
6	23	199	未分派	拒绝
7	24			

[0035]

8	25	188	英国	接受
9	…	…	…	…
10	43	88	日本	接受
11	…	…	…	…
12	47	36	加拿大	接受
13	…	…	…	…
14	53	66	德国	拒绝
15	54-56	189	美国	接受
16	57	61	法国	拒绝
17	…	…	…	…
18	80-88			
19	89-124	199	未分派	拒绝
20	…	…	…	…
21	216-223			
22	224-255	148	保留	接受

[0036] 表II

[0037] 表II的IP网络地址子范围是表I的子范围的例子，表II的国家代码是表I的分类值的例子，并且表II的结果是表I的结果的例子。例如，诸如54或57这样的每个IP网络地址子范围均是有限集合内IP网络地址的MSB。

[0038] 处理器102将分组150的N个比特与表II的每个IP网络地址子范围进行比较，并且确定IP网络地址子范围中具有与这N个比特相匹配的M个比特的一个IP网络地址子范围。例如，一旦确定表II的网络地址47.0.0.0－47.255.255.255与分组150的N个比特相匹配，处理器102便将表II的国家代码36分派给分组150，并且确定分组150是从加拿大发送的。一旦确定分组150是从加拿大发送的，处理器102便基于表II确定接受分组150。作为另一例子，一旦处理器102确定表II的IP网络地址子范围23的M个比特与分组150的N个比特相匹配，处理器102便向分组150分派表II的国家代码199，并且确定分组150是从未分派的区域发送的。一旦确定分组150是从未分派的区域发送的，处理器102便确定拒绝分组150，如表II所示。再举另一个例子，一旦处理器102确定表II的多个IP网络地址224.0.0.0－255.255.255.255的IP网络地址子范围227的M个比特与分组150的N个比特相匹配，处理器102便向分组150分派表II的国家代码148，并且确定分组150是从保留区域发送的。一旦确定分组150是从保留区域发送的，处理器102便基于表II确定接受分组150。再举另一个例子，一旦处理器102确定IP网络地址子范围216-223的M个比特与分组150的N个比特相匹配，处理器102便基于分类值确定分组150不能被分类。

[0039] 下面提供的表III是表I的另一个例子。

[0040]

IP网络地址子范围	结果
0-127	允许
128-160	拒绝
161-163	允许
164-167	拒绝
168-191	允许
192-207	拒绝
208-255	允许

[0041] 表III

[0042] 表III的IP网络地址子范围是8个MSB，其是表I的有限集合内IP网络地址子范围的M个比特的例子。另外，表III的结果是表I的结果的例子。

[0043] 处理器102接收分组150的N个比特，将这N个比特与表III的每个IP网络地址子范围的M个比特进行比较，以便确定IP网络地址子范围中具有与这N个比特相匹配的M个比特的一个IP网络地址子范围。一旦确定分组150的N个比特与IP网络地址子范围0-127、161-163、168-191和208-255中任何一个内的M个比特相匹配，处理器102便确定分组150被允许穿过防火墙。另一方面，一旦确定分组150的N个比特与IP网络地址子范围128-160、164-167和192-207中任何一个内的M个比特相匹配，处理器102便确定拒绝分组150通过防火墙。

[0044] 下面示出的表IV是表I的另一个例子。

[0045]

IP网络地址子范围	IP网络地址子范围的MSB	结果
0-127	0	允许
128-255	1	

[0046] 表IV

[0047] 表IV的IP网络地址子范围是表I的子范围的例子，并且表IV的结果是表I的结果的例子。

[0048] 处理器102将分组150的IP网络地址的MSB(其是N的一例子)与表IV的每个IP网络地址子范围的MSB(其是M的一例子)进行比较，以便确定分组150的MSB是匹配于比特1或比特0。一旦确定分组150的IP网络地址的MSB匹配于比特0(其是表IV的IP网络地址子范围0-127的MSB)，处理器102便基于表IV的结果确定允许分组150通过防火墙。另一方面，一旦确定分组150的IP网络地址的MSB匹配于比特1(其是表IV的IP网络地址子范围128-255的MSB)，处理器102便基于表IV的结果确定分组150不能被分类并且不向分组150提供结果。

[0049] 一旦确定分组150不能基于分组150的N个比特而被分类，处理器102便从分组150获得210除了这N个比特之外的G个比特。一旦确定不能通过将N个比特与表I的子范围的M个比特进行比较来分类分组150，处理器102便从分组150获得G个比特。举例来说，处理器102确定分组150是IPv4分组150，并且提取分组150的IP网络地址中顺序接着MSB的7个比特，其中MSB是分组150的IP网络地址中的第N个比特。再举另一个例子，处理器102确定分组150是IPv4分组150，并且提取分组150的IP网络地址的8个MSB中的3个MSB，其中除了IP网络地址的3个MSB和3个LSB之外的2个比特是分组150的IP网络地址的N个比特。再举另一个例子，处

理器102确定分组150是IPv6分组150，并且从分组150的IP网络地址的16个MSB中提取4个LSB，其中12个MSB是分组150的IP网络地址的N个比特。G的例子包括除了分组150的IP网络地址的8个MSB中的N个比特之外的比特。G的另一个例子包括连续接着分组150的IP网络地址的16个MSB的MSB的15个比特，其中MSB是分组150的IP网络地址的第N个比特。

[0050] 处理器102确定206分组150是否可以基于分组150的G个比特被分类。处理器102应用如下所示的由用户存储在存储设备104中的表V，以便确定分组150是否可以基于分组150的G个比特而被分类。

[0051]

子范围	分类值	结果
SR1-SR2	C3	S3
SR3-SR4	C4	S4
SR5-SR6		
SR7-SR8		

[0052] 表V

[0053] 表V内的子范围SR1-SR2、SR3-SR4、SR5-SR6和SR7-SR8形成了有限集合，例如端口地址的G个比特的集合、授权数据的G个比特的集合，IP网络地址的G个比特的集合，以及IP网络地址和端口地址组合的G个比特的集合。分类值C3和C4的例子包括标识多个国家的国家代码集合、标识多个子区域的子区域代码集合、标识多个计算机黑客的黑客代码集合、标识多个计算机垃圾邮件发送者的垃圾邮件发送者代码集合、标识多个计算机病毒的病毒代码集合、标识多个Trojan的Trojan代码集合、标识多个计算机蠕虫的蠕虫代码集合、标识多个钓鱼者的多个钓鱼代码、标识经由后门获得对连接至处理器102的计算机网络的访问的多个入侵者的入侵者代码集合、标识多个NATO国家的NATO国家代码集合、标识多个公司的公司代码集合、标识多个政府机构的政府机构代码集合、标识多个ISP的ISP代码集合、标识多个产业部门的产业部门代码集合，以及标识多个DoD的DoD代码集合。结果S3和S4的例子包括处理器102接受或拒绝分组150。结果S3和S4的其它例子包括向分组150分派优先级或不分派优先级。注意到G等于H。

[0054] 一旦确定表V的子范围SR1-SR2、SR3-SR4、SR5-SR6和SR7-SR8之一具有与分组150的G个比特相匹配的H个比特，处理器102便向分组150分派诸如C3和C4的对应分类值之一。举例来说，一旦确定G个比特与子范围SR3-SR4的H个比特相匹配，处理器102便向分组150分派分类值C4。如果处理器102确定表V内的分类值中存在一个分类值对应于表V的子范围中具有与分组150的G个比特相匹配的H个比特的一个子范围，则处理器102确定分组150被分类。另一方面，如果处理器102确定表V内的分类值中并不存在一个分类值对应于表V内的子范围中具有与分组150的G个比特(在处理器102将其与表V的子范围进行比较的情况下)相匹配的H个比特的一个子范围，则处理器102确定G个比特与并不对应于分类值C3和C4之一的子范围SR5-SR6内的H个比特相匹配。在该例中，一旦处理器102确定分组150的G个比特并不对应于分类值C3和C4之一，处理器102便确定分组150不能被分类。

[0055] 一旦确定分组150被分类，处理器102要么提供208对应于表V的分类值之一的结果S3和S4之一或过程，要么向将结果S3和S4之一提供208给分组150的另一处理器102(例如包括在工作站54内的处理器)发送分组150。举例来说，一旦确定分组150被分类为具有分类值

C3，处理器102便将结果S3应用于分组150。作为另一例子，一旦处理器102确定分组150具有分类值C2，处理器102便向将结果S2应用于分组150的另一处理器102发送分组150。一旦确定分组150被分类，处理器102便不提取分组150中除了这G和N个比特之外的其它比特来确定分组150是否可以被分类。

[0056] 下面示出的表VI是表V的例子。

[0057]

IP网络地址子范围	比特IP网络地址子范围	结果
128-160	00	拒绝
161-207	01-10	
168-255	11	允许

[0058] 表VI

[0059] 表VI的IP网络地址子范围的比特是表V的子范围的H个比特的例子。例如，作为H的例子，两比特00是表VI的IP网络地址子范围128-160内128的第二和第三MSB。再举另一个例子，表VI内的比特01是表VI的IP网络地址子范围161-207内161的第二和第三MSB。表VI的结果是表V的结果的例子。

[0060] 处理器102接收分组150的G个比特，将这G个比特与H个比特进行比较，以便确定分组150可以被分类。例如，一旦接收到G个比特，处理器102便确定G个比特与01相匹配以及确定分组150不能被分类，并且其并不基于表VI提供结果。另一方面，处理器102接收分组150的G个比特，将这G个比特与比特00进行比较，以便确定这G个比特是00，并且基于表VI拒绝分组150通过防火墙。此外，处理器102接收分组150的G个比特，将这G个比特与表VI内的比特11进行比较，以便确定这G个比特是11并且确定允许分组150通过防火墙，如表VI所示。

[0061] 一旦基于分组150的G和N个比特确定分组150不能被分类，处理器102便通过分析分组150的不同于这G和N个比特的A个比特来确定分组150是否可以被分类。表VII如下所示。

[0062]

IP网络地址子范围	比特IP网络地址子范围	结果

[0063]

192-207	0	拒绝
208-223	1	允许

[0064] 表VII

[0065] 处理器102接收A个比特(例如，分组150的IP网络地址的8个MSB的第5个LSB)，将这A个比特与B个比特(例如，具有表VII的IP网络地址子范围的每个IP网络地址的8个MSB的第5个LSB)进行比较，以便确定分组150是否可以被分类。例如，一旦接收到分组150的A个比特，处理器102便确定这A个比特匹配于0，其是IP网络地址193.0.0.0的IP网络地址子范围193的8个MSB的第5个LSB，确定分组150可以被分类，并且基于表VII拒绝分组150通过防火墙。再举一个例子，一旦接收到分组150的A个比特，处理器102便确定这A个比特匹配于比特1，其是IP网络地址210.1.1.1的IP网络地址子范围210的8个MSB的第5个LSB，确定分组150可以被分类，并且基于表VII允许分组150通过防火墙。注意到A等于B。

[0066] 下面示出的表VIII是表V的例子。

[0067]

IP网络地址子范围	比特IP网络地址子范围	结果
160-168	0	
191	1	允许

[0068] 表VIII

[0069] 表VIII的IP网络地址子范围是表V的子范围的另一个例子。表VI的IP网络地址子范围的比特是表V的子范围的H个比特的另一个例子。例如，比特0是具有范围从160到168且包括160和168的MSB的多个IP网络地址的8个MSB160-168中每一个的第5个LSB，并且160-168是子范围SR5-SR6的例子。作为另一个例子，比特1是具有MSB191的多个IP网络地址的8个MSB191的第5个LSB，并且191是IP网络地址子范围SR1-SR2。

[0070] 处理器102接收分组150的G个比特，将这G比特与表VIII的H个比特进行比较，以便确定分组150是否可以被分类。例如，一旦接收到分组150的G个比特，处理器102便确定这G个比特与表VIII的IP网络地址子范围160-168的0相匹配，确定这G个比特不能被分类，并且不向分组150提供结果。作为另一个例子，一旦接收到分组150的G个比特，处理器102便确定这G个比特与IP网络地址子范围191的1相匹配，以便确定分组150可以被分类，从而允许分组150穿过防火墙。

[0071] 一旦基于将分组150的G个比特与H个比特进行比较而确定分组150不能被分类，处理器102便确定是否可以基于将分组150的A个比特与B个比特进行比较来分类分组150。表IX如下所示。

[0072]

IP网络地址子范围	比特IP网络地址子范围	结果
160-167	0	
168	1	允许

[0073] 表IX

[0074] 处理器102接收分组150的A个比特，将这A个比特与B个比特(例如，多个IP网络地址160.0.0.0－167.255.255.255的8个MSB160-167中每一个的第4个LSB)进行比较，以便确定分组150是否可以被分类。例如，一旦接收到分组150的A个比特，处理器102便确定这A个比特匹配于比特0(其是8个MSB160-167中每一个的第4个LSB)，确定分组150不能被分类，并且不能被提供结果。作为另一个例子，一旦接收到分组150的A个比特，处理器102便确定这A个比特匹配于比特1(其是多个IP网络地址168.0.0.0－168.255.255.255的8个MSB168的第4个LSB)，确定分组150可以被分类，并且允许分组150通过防火墙。

[0075] 一旦基于分组150的N、G和A个比特确定分组150不可以被分类，处理器102便获得分组150的C个比特，并且基于这C个比特确定分组150是否可以被分类。表X如下所示。

[0076]

IP网络地址子范围	比特IP网络地址子范围	结果
160-163	0	
164-167	1	拒绝

[0077] 表X

[0078] 举例来说，分组150的C个比特包括分组150(其是IPv4分组150)的IP网络地址的8

个MSB的第3个LSB。另一个例子中，分组150的C个比特包括分组150(其是IPv6分组150)的IP网络地址的第4个LSB。

[0079] 处理器102接收分组150的C个比特，将这C个比特与D个比特(例如，多个IP网络地址160.0.0.0－163.255.255.255的8个MSB中每一个的第3个LSB)进行比较，以便确定分组150是否可以被分类。例如，处理器102将分组150的C个比特与比特0(其是8个MSB160-163中每一个的第3个LSB)进行比较，从而确定分组150不能被分类，并且不向分组150提供结果。作为另一个例子，处理器102将分组150的C个比特与比特1(其是多个IP网络地址164.0.0.0－167.255.255.255的8个MSB164-167中每一个的第3个LSB)进行比较，从而确定分组150可以被分类，并且拒绝分组150通过防火墙。注意到C等于D。

[0080] 一旦基于分组150的N、G、A和C个比特确定分组150不可以被分类，处理器102便获得分组150的E个比特，并且基于这E个比特确定分组150是否可以被分类。表XI如下所示。

[0081]

IP网络地址子范围	比特IP网络地址子范围	结果
160-161	0	
163	1	允许

[0082] 表XI

[0083] 举例来说，分组150的E个比特包括分组150(其是IPv4分组)的IP网络地址的8个MSB的第2个LSB。在另一个例子中，分组150的E个比特包括分组150(其是IPv6分组)的IP网络地址的8个MSB的第5个LSB。

[0084] 处理器102接收分组150的E个比特，将这E个比特与F个比特(例如，表XI的每个IP网络地址子范围的第2个LSB)进行比较，以便确定分组150是否可以被分类。例如，处理器102将分组150的E个比特与比特0(其是多个IP网络地址160.0.0.0－161.255.255.255的8个MSB160-161中每一个的第2个LSB)进行比较，以便确定分组150不能被分类。作为另一个例子，处理器102接收分组150的E个比特，将这E个比特与比特1(其是多个IP网络地址163.0.0.0－163.255.255.255的8个MSB163的第2个LSB)进行比较，以便确定分组150可以被分类，并且允许分组150通过防火墙。注意到E等于F。

[0085] 一旦基于分组150的N、G、A、C和E个比特确定分组150不可以被分类，处理器102便获得分组150的不同于这N、G、A、C和E个比特的I个比特，以便基于这I个比特确定分组150是否可以被分类。表XII如下所示。

[0086]

IP网络地址子范围	比特IP网络地址子范围	结果
160	0	拒绝
161	1	允许

[0087] 表XII

[0088] 举例来说，分组150的I个比特包括分组150(其是IPv4分组)的IP网络地址的8个MSB的LSB。在另一个例子中，分组150的I个比特包括分组150(其是IPv6分组)的IP网络地址的16个MSB的LSB。

[0089] 处理器102接收分组150的I个比特，将这I个比特与J个比特(例如，表XII的每个IP网络地址子范围的LSB)进行比较，以便确定分组150是否可以被分类。例如，处理器102将分

组150的I个比特与比特0(其是多个IP网络地址160.0.0.0－160.255.255.255中160的LSB)进行比较，以便确定分组150可以被分类并且拒绝分组150通过防火墙。作为另一个例子，一旦接收到分组150的I个比特，处理器102便将这I个比特与比特1(其是多个IP网络地址161.0.0.0－161.255.255.255中161的LSB)进行比较，以便确定分组150可以被分类，并且允许分组150通过防火墙。相应地，处理器102继续将分组150的另外的比特与诸如表V-XII的多个表格进行比较，直到分组150可以被分类。注意到I等于J。

[0090] 图6是用于创建表I-XII中任何一个的图形用户接口(GUI)250的实施例。处理器102在输出设备108上向用户显示GUI250。GUI250包括世界地图252。处理器102在地图252上将多个点254、256和258与子范围R1-R2、R3-R4、R5-R6、R7-R8、R9-R10和R11-R12之一相关联或链接。例如，处理器102将点254与表I的子范围R1-R2相关联，并且将点256与表I的IP网络地址子范围R5-R6相关联。作为另一个例子，处理器102将点254与位于美国内的计算机端口的端口地址相关联，并且将点256与位于加拿大内的计算机端口的端口地址相关联。

[0091] 当用户通过输入设备106在地图252上选择点的时候，处理器102向用户显示多个结果。例如，当用户选择点254的时候，处理器102显示多个选项，包括允许分组150(其具有与位于点254处的计算机的IP网络地址的子范围R1-R2、R3-R4、R5-R6、R7-R8、R9-R10和R11-R12之一的M个比特相匹配的N个比特)通过防火墙、拒绝分组150、向分组150提供优先级，以及不向分组150提供优先级。当用户选择其中一个选项的时候，处理器102将这其中一个选项与地图252上的点相关联。举例来说，当用户选择允许与点254相关联的分组150(其具有与子范围R1-R2、R3-R4、R5-R6、R7-R8、R9-R10和R11-R12之一的M个比特相匹配的N个比特)穿过防火墙时，处理器102在存储设备104内存储将要允许分组150(其具有与子范围R1-R2、R3-R4、R5-R6、R7-R8、R9-R10和R11-R12之一的M个比特相匹配的N个比特)穿过防火墙。作为另一个例子，当用户选择向与点258相关联的分组150(其具有与子范围R1-R2、R3-R4、R5-R6、R7-R8、R9-R10和R11-R12之一的M个比特相匹配的N个比特)提供优先级的时候，处理器102在存储设备104中存储将要向具有子范围之一的分组150提供优先级。

[0092] 在一个实施例中，当用户选择一次(例如通过单击鼠标、任何一个点以及选择一个结果)的时候，处理器102将地图252上的区域(例如国家、城市、州、公司以及计算机网络)内多个点与结果S1和S2之一相关联。例如，当用户在处于美国内的点254上点击一次并且选择允许分组150的时候，处理器102将地图252上处于美国内的所有点与允许由处理器102从美国接收分组150相关联。在该实施例中，当用户选择至少一个点之一达到一定的次数(例如两次)并且选择结果之一的时候，处理器102将子区域的至少一个点(例如，位于该区域内的城市、政府机构、ISP、公司、DoD、计算机、端口)与结果S1和S2之一相关联。例如，当用户双击表示美国内的城市的点254并且通过双击点254而选择无优先级的时候，处理器102将从该城市接收的分组150关联于无优先级。作为另一个例子，当用户双击表示加拿大内的计算机网络的点258并且通过双击点258而选择拒绝分组150通过的时候，处理器102将点258关联于拒绝从该计算机网络接收的分组150通过防火墙。

[0093] 注意到，在一个实施例中，图5和图6的方法以及表I-XII是在一组逻辑门和移位寄存器内实现的有限状态机(FSM)从而实现防火墙。在另一个实施例中，分组150被分派高优先级而不是分派优先级，并且分组150被分派低于该高优先级的低优先级而不是未分派优先级。注意到，图5和图6所说明的方法以及表I-XII在小型、微型或大型机硬件中实现。在又

一个实施例中，图5和图6所说明的方法以及表I-XII在现场可编程门阵列(FPGA)内实现。在此所描述的用于确定数据流的系统和方法提供了基于树的遍历结构，其允许对多个规则或访问控制列表(ACL)的指数执行(exponential execution)。例如，处理器102通过将分组150的IP地址的8个MSB与表II的行3中多个IP地址3.0.0.0-4.255.255.255的IP网络地址子范围3-4或者表II的行4中多个IP地址5.0.0.0-9.255.255.255的IP网络地址子范围5-9进行比较而得到结果，这不同于将分组150的所有比特与IP地址3.0.0.0-4.255.255.255和5.0.0.0-9.255.255.255进行比较。作为另一个例子，处理器102提供结果以指数方式快于通过将分组150的所有比特与一组比特进行比较来提供结果。在该例中，处理器102通过将分组150的IP地址的8个MSB的第2和第3个MSB与表VI内IP地址128.0.0.0-160.255.255.255的8个MSB128-160的第2和第3个MSB进行比较而以指数方式更快地提供结果。在此所描述的用于确定数据流的方法和系统并不需要执行浮点操作并且因此可以在内核空间中运行。

[0094] 在此所描述的系统和方法通过拒绝来自区域(例如国家)或可选地来自子区域的分组150而实现了经由防火墙连接的两个网络之间的隔离。此外，一旦确定分组150是从防火墙所处的国家的同盟国接收的，在此所描述的系统和方法便允许分组150通过防火墙。另外，在此所描述的系统和方法用于拒绝从不同于群内的多个组织的实体接收的分组150。

[0095] 通过降低未经请求的电子邮件或垃圾邮件的发生率来执行在此所描述的方法和系统，以便改进因特网吞吐量。例如，处理器102基于分组150的N个比特以及表II来确定分组150是否被分类在德国的国家代码66内。一旦确定分组150具有分类值66，处理器102便确定拒绝可能包括来自德国的垃圾邮件的分组150，并且通过减少通过到网络的防火墙的垃圾邮件来提高因特网的吞吐量。作为另一个例子，处理器102基于分组150的N个比特来确定分组150被分派不同于189的国家代码。一旦确定分组150被分派不同于189的国家代码，处理器102便拒绝分组150通过防火墙，并且该拒绝降低了通过耦合于防火墙的网络对来自于除了美国以外的国家的垃圾邮件的接收。此外，在该例中，通过降低对来自美国的垃圾邮件的接收，处理器102使得跟踪在美国的垃圾邮件发送者相当简单。在该例中，处理器102应用用于确定数据流的方法来处理从美国发送的分组150，其明显快于(例如十倍)光载体-192(OC-192)的9.6千兆比特每秒(Gbps)的通信速度。在此所描述的方法用于缓和各种计算机通信网络安全威胁，例如由攻击者发送的计算机病毒。该方法提供了可扩展性、可适应性以及用于适应安全问题的每种演进(every-evolving)范围的性能特征。可以在多种安全产品中实现在此所描述的方法，例如数据分路设备、网络仿真系统、生物统计分析系统、生物统计异常分析系统、安全体系结构设计系统、网络操作中心、虚拟专用网络(VPN)以及安全信息管理系统。

[0096] 虽然已经根据各种具体实施例描述了本发明，但是本领域的技术人员将认识到，本发明可以在权利要求的精神和范围内修改的情况下实施。

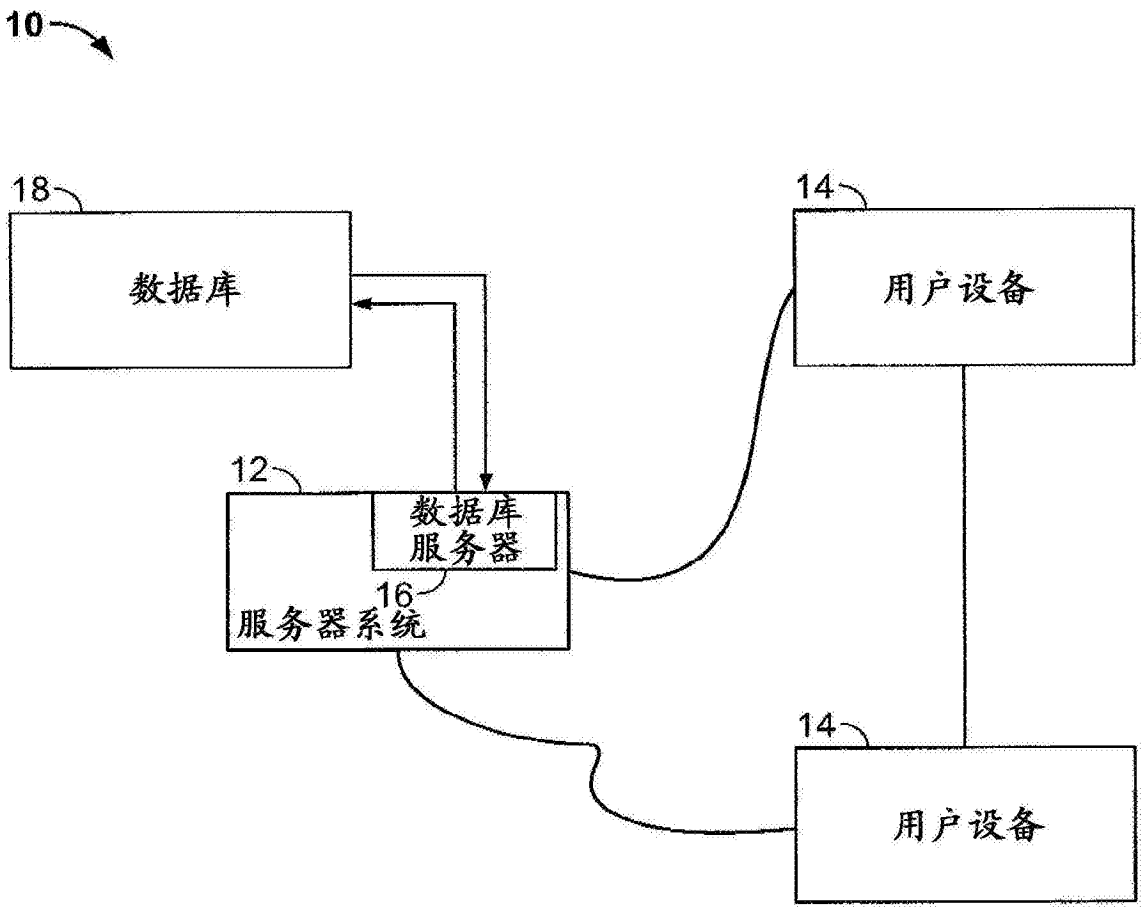


图1

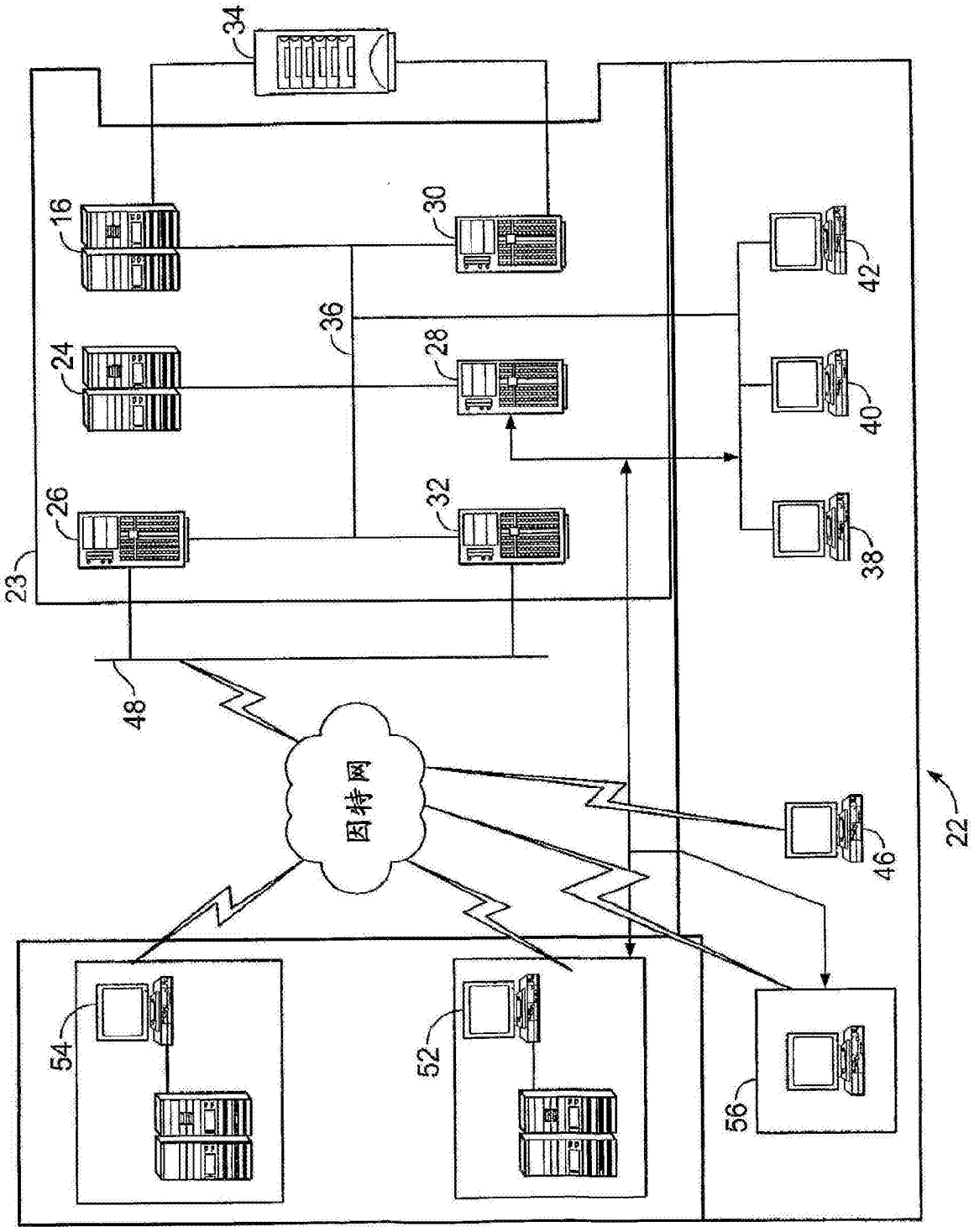


图2

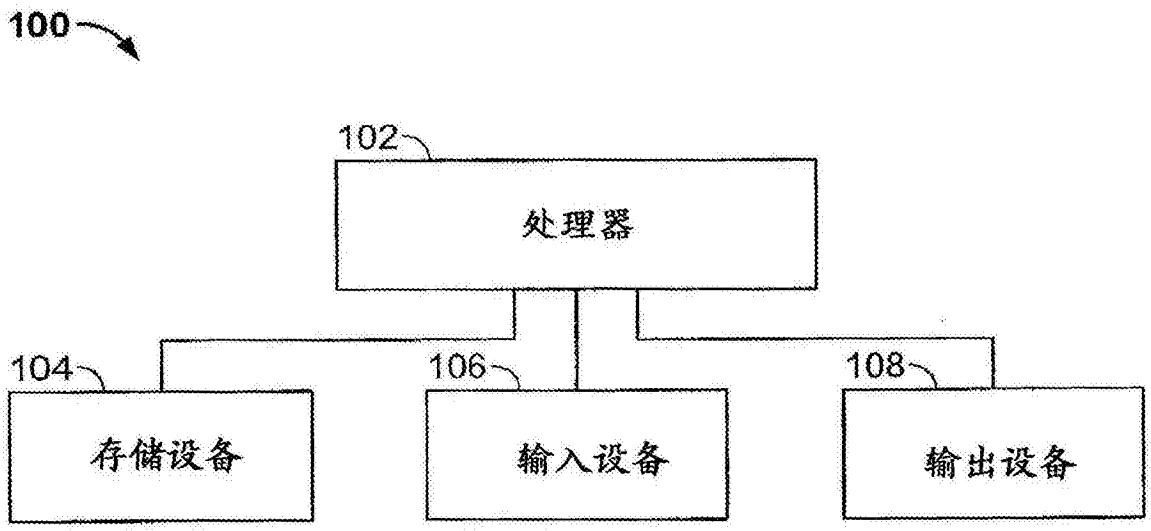

100
102
处理器
104
存储设备
106
输入设备
108
输出设备

图3

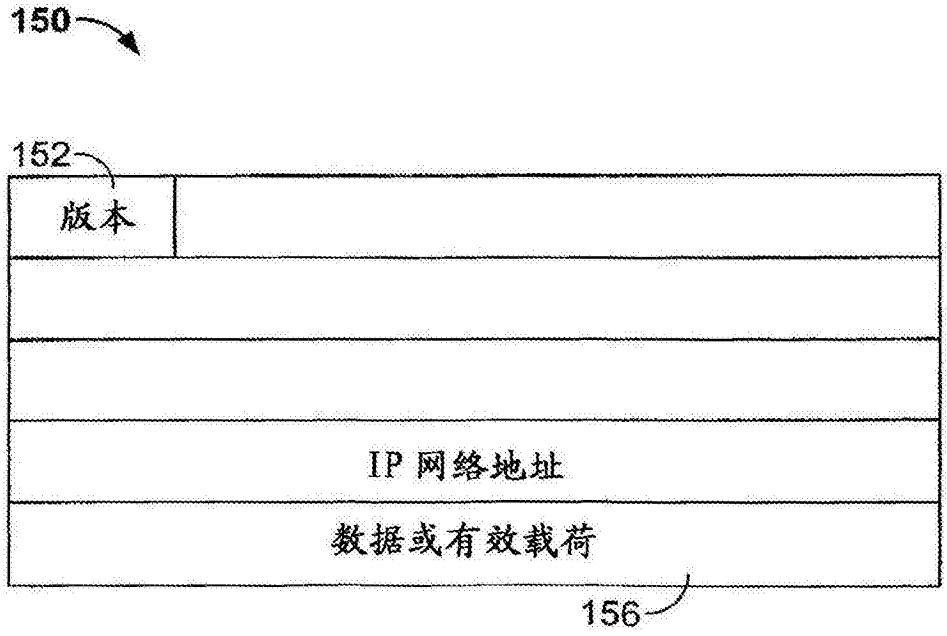

150
152
版本
IP 网络地址
数据或有效载荷
156

图4

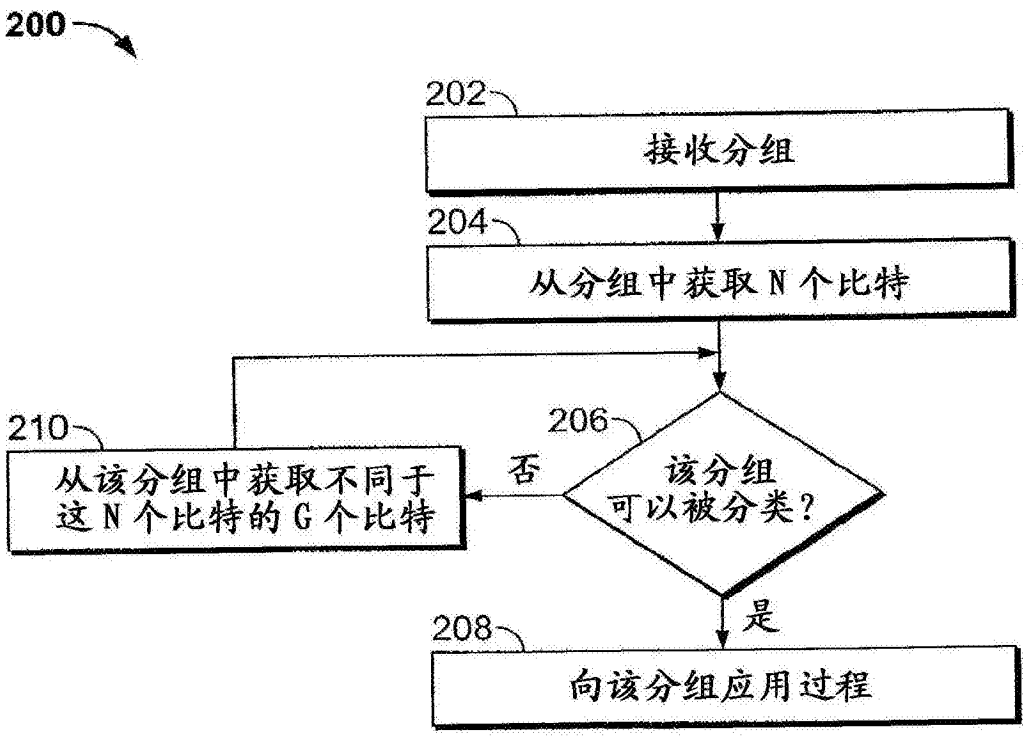

200
202
接收分组
204
从分组中获取 N 个比特
206
该分组
可以被分类？
否
210
从该分组中获取不同于
这 N 个比特的 G 个比特
是
208
向该分组应用过程

图5

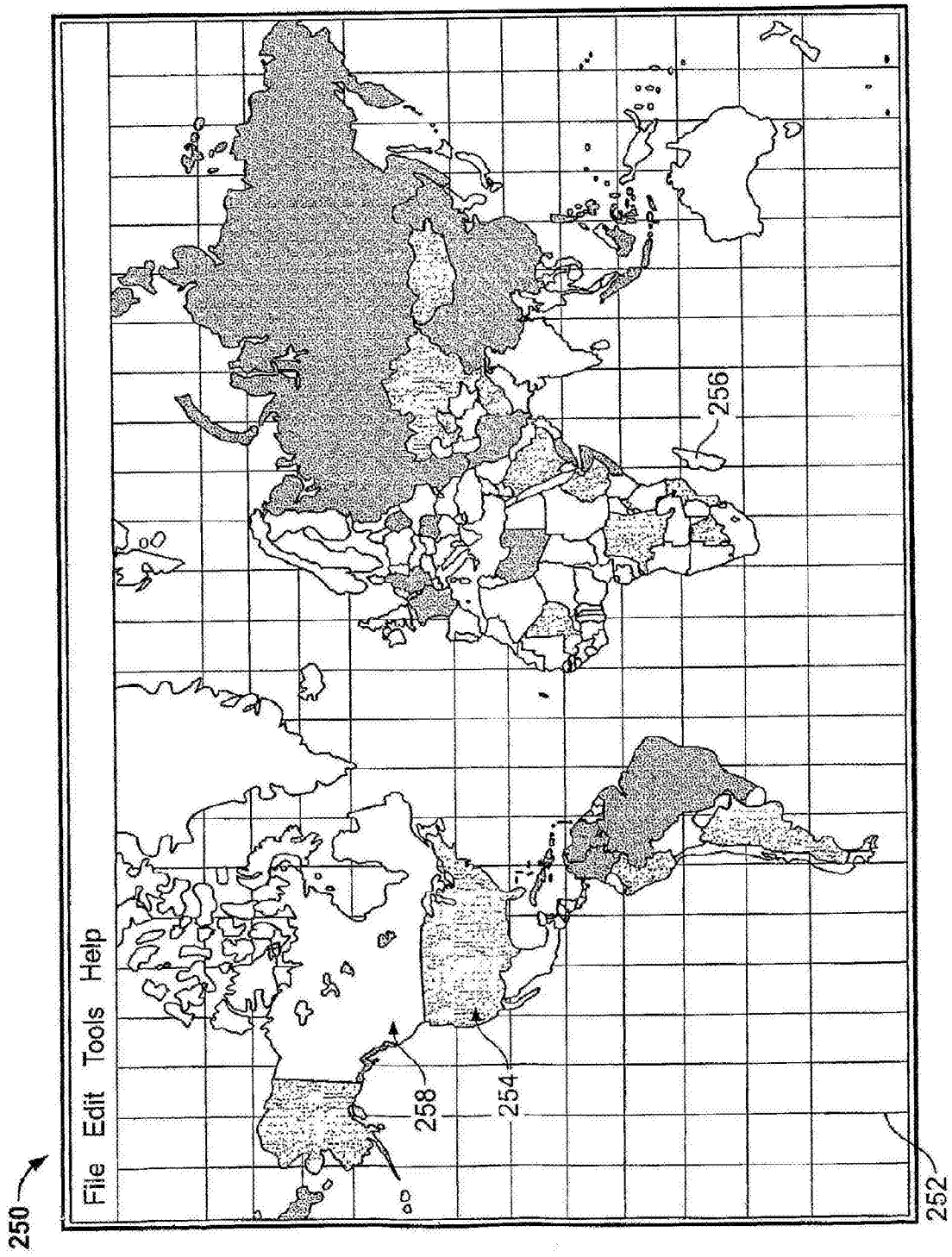


图6