(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 101841489 B
(45)授权公告日 2013.03.27

(21)申请号 200910208925.4
(22)申请日 2005.05.25
(30)优先权数据
60/574239 2004.05.25 US
(62)分案原申请数据
200580024599.1 2005.05.25
(73)专利权人 反射网络公司
地址 美国麻萨诸塞州
(72)发明人 J·麦伊萨克 M·达哈洛夫
B·塔塔斯基 R·瓦莱特
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 汤春龙 徐予红
(51)Int.Cl.
H04L 12/58(2006.01)
H04L 29/06(2006.01)
H04L 29/08(2006.01)
(56)对比文件
CN 1350247 A,2002.05.22,
US 6377993 B1,2002.04.23,
CN 1467670 A,2004.01.14,
审查员 郝政宇

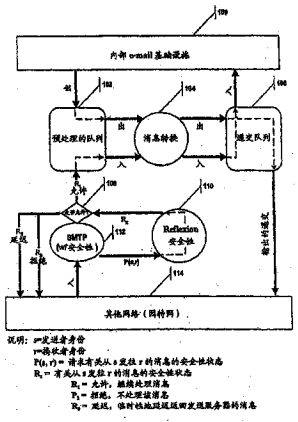
权利要求书 4 页 说明书 16 页 附图 13 页

(54)发明名称

用于控制对电子消息接收者的访问的系统和方法

(57)摘要

本发明提供了一种用于控制对电子消息接收者的访问的系统和方法。用于选择性地允许或拒绝对耦合到电子通信网络的用户的访问,包括通过电子通信网络从发送者接收入站消息的接收器。入站消息包括与发送者关联的标识符和与接收者关联的标识符。该系统还包括处理器,处理器用于确定与接收者关联的标识符是否是由用户先前生成的,以及是否是与接收者关联的多个代理标识符中所没有的。处理器还确定与入站消息关联的至少三个安全性状态的其中之一。第一安全性状态指示允许将入站消息递交至用户。第二安全性状态指示拒绝将入站消息递交至用户。第三安全性状态指示有条件地允许将该消息递交至用户。这三个安全性状态的每一个状态与入站消息中所含的发送者标识和接收者标识符关联。



CN 101841489 B

1. 一种用于选择性地允许或拒绝由耦合到电子通信网络的其它用户对耦合到所述电子通信网络的用户的通信访问的方法，包括：

通过所述电子通信网络从发送者接收入站消息，其中所述入站消息包含与发送者关联的标识符和与接收者关联的标识符；

确定与所述入站消息关联的至少三个安全性状态的其中之一，其中：

第一安全性状态指示允许将所述入站消息递交到所述用户，

第二安全性状态指示拒绝将所述入站消息递交到所述用户，

第三安全性状态指示有条件地允许将所述消息递交到所述用户，

所述至少三个安全性状态的每一个与所述入站消息中包含的与所述发送者关联的标识符和与所述接收者关联的标识符相关联；以及

如果允许递交，则向所述入站消息添加用户界面，其中所述用户界面配置为允许所述用户控制对所述用户的所述通信访问。

2. 如权利要求 1 所述的方法，其特征在于，所述用户界面包括所述入站消息中所含的信息。

3. 如权利要求 1 所述的方法，其特征在于，所述用户界面包括表示与所述入站消息关联的安全性状态的信息。

4. 如权利要求 1 所述的方法，其特征在于，所述用户界面是可调整的，用于更新所述用户界面表示的信息。

5. 如权利要求 1 所述的方法，其特征在于，所述用户界面的内容由所述用户调整。

6. 如权利要求 1 所述的方法，其特征在于，基于所确定的安全性状态，延迟所述入站消息的递交。

7. 如权利要求 1 所述的方法，还包括：

确定与所述接收者关联的标识符是否是由用户先前生成的以及是否是与所述接收者关联的多个代理标识符中所没有的。

8. 如权利要求 7 所述的方法，还包括：

在已确定与所述接收者关联的标识符是即时名称且所述即时名称被创建的情况下，将与所述接收者关联的标识符添加到所述多个代理标识符。

9. 如权利要求 7 所述的方法，其特征在于，确定与所述接收者关联的标识符是由用户先前生成的步骤包括将与所述接收者关联的标识符的一部分分离，以确定所述多个代理标识符中是否包含此部分。

10. 如权利要求 7 所述的方法，还包括：

如果所述第一安全性状态与所述入站消息关联，则从所述入站消息中移除与所述接收者关联的标识符。

11. 如权利要求 1 所述的方法，还包括：

确定所述入站消息是否豁免于所述安全性状态；以及

如果豁免，则基于所述安全性豁免递交所述入站消息。

12. 如权利要求 11 所述的方法，其特征在于，所述安全性豁免基于与所述发送者关联的所述标识符。

13. 如权利要求 11 所述的方法，其特征在于，所述安全性豁免基于和标识符关联的域，

所述标识符与所述接收者相关联。

14. 如权利要求 11 所述的方法，其特征在于，所述安全性豁免基于包括本地递交的本地邮件的地址中的相似域的与所述发送者关联的标识符和与所述接收者关联的标识符。

15. 如权利要求 11 所述的方法，其特征在于，所述安全性豁免基于所述入站消息，所述入站消息是对发送到豁免和非豁免接收者的第二消息的回复消息。

16. 如权利要求 11 所述的方法，其特征在于，所述安全性豁免在一段时间间隔内有效。

17. 如权利要求 11 所述的方法，还包括：

存储表示所述入站消息的递交的数据。

18. 如权利要求 1 所述的方法，其中确定所述安全性状态的步骤包括确定何时接收到包含与所述发送者关联的标识符和与所述接收者关联的标识符的先前消息。

19. 如权利要求 18 所述的方法，还包括：

在所述入站消息与所述先前消息的接收之间的时间间隔小于预定义的时间的情况下递交所述入站消息。

20. 如权利要求 1 所述的方法，还包括确定是否已提升与所述入站消息关联的安全性状态。

21. 如权利要求 20 所述的方法，还包括：

如果提升所述安全性状态且所述入站消息与所述第一安全性状态关联，则将所述第二安全性状态与所述入站消息关联以取代所述第一安全性状态。

22. 如权利要求 20 所述的方法，还包括：

如果提升所述安全性状态且所述入站消息与所述第一安全性状态关联，则将所述第三安全性状态与所述入站消息关联以取代所述第一安全性状态。

23. 如权利要求 20 所述的方法，其特征在于，所述安全性状态提升是在预定义的时间间隔内进行。

24. 如权利要求 20 所述的方法，其特征在于，确定是否已提升所述安全性状态的步骤包括检测预定义的条件。

25. 如权利要求 20 所述的方法，其特征在于，确定是否已提升所述安全性状态的步骤包括从系统管理员处接收指令。

26. 如权利要求 1 所述的方法，其中所述用户界面是所述入站消息中的注脚。

27. 如权利要求 1 所述的方法，其中所述用户界面配置为允许所述用户控制所述至少三个安全性状态。

28. 如权利要求 1 所述的方法，其中所述用户界面包括到外部用户界面的链接，所述外部用户界面配置为允许用户控制对所述用户的通信访问。

29. 如权利要求 28 所述的方法，其中所述外部用户界面配置为允许所述用户控制至所述少三个安全性状态。

30. 如权利要求 1 所述的方法，其中所述用户界面包括与所述入站消息相关联的信息。

31. 如权利要求 1 所述的方法，其中所述入站消息包括电子邮件消息。

32. 一种用于选择性地允许或拒绝由耦合到电子通信网络的其它用户对耦合到所述电子通信网络的用户的通信访问的系统，包括：

接收器，配置为通过所述电子通信网络从发送者接收入站消息，其中所述入站消息包

含与发送者关联的标识符和与接收者关联的标识符；以及

处理器，配置为确定与所述入站消息关联的至少三个安全性状态的其中之一，其中第一安全性状态指示允许将所述入站消息递交到所述用户，第二安全性状态指示拒绝将所述入站消息递交到所述用户，第三安全性状态指示有条件地允许将所述消息递交到所述用户，所述至少三个安全性状态的每一个与所述入站消息中包含的与所述发送者关联的标识符和与所述接收者关联的标识符相关联，

其中如果允许递交，则所述处理器还配置为向所述入站消息添加用户界面，其中所述用户界面配置为允许所述用户控制对所述用户的通信访问。

33. 如权利要求 32 所述的系统，其特征在于，所述用户界面包含所述入站消息中所含的信息。

34. 如权利要求 32 所述的系统，其特征在于，所述用户界面包含表示与所述入站消息关联的安全性状态的信息。

35. 如权利要求 32 所述的系统，其特征在于，所述处理器还配置为调整所述用户界面，用于更新所述用户界面表示的信息。

36. 如权利要求 32 所述的系统，其特征在于，所述处理器还配置为调整所述用户界面，用于更新由所述用户界面表示的信息，其中所述用户启动所述调整。

37. 如权利要求 32 所述的系统，其特征在于，基于所确定的安全性状态，所述处理器还配置为延迟所述入站消息的递交。

38. 如权利要求 32 所述的系统，其中所述处理器还配置为确定与所述接收者关联的标识符是否是由用户先前生成的以及是否是与所述接收者关联的多个代理标识符中所没有的。

39. 如权利要求 38 所述的系统，其特征在于，所述处理器还配置为将与所述接收者关联的标识符添加到所述多个代理标识符中。

40. 如权利要求 38 所述的系统，其特征在于，确定与所述接收者关联的标识符是由用户先前生成的步骤包括将与所述接收者关联的标识符的一部分分离，以确定所述多个代理标识符中是否包含此部分。

41. 如权利要求 38 所述的系统，其特征在于，如果所述第一安全性状态与所述入站消息关联，则所述处理器还配置为从所述入站消息中移除与所述接收者关联的标识符。

42. 如权利要求 32 所述的系统，其中所述处理器还配置为确定所述入站消息是否豁免于所述安全性状态，并基于安全性豁免递交所述入站消息。

43. 如权利要求 32 所述的系统，其中确定所述安全性状态的步骤包括确定何时接收到包含与所述发送者关联的标识符和与所述接收者关联的标识符的先前消息。

44. 如权利要求 43 所述的系统，其特征在于，所述处理器还配置为在所述入站消息与所述先前消息的接收之间的时间间隔小于预定义的时间的情况下递交所述入站消息。

45. 如权利要求 32 所述的系统，其中所述处理器还配置为确定是否已提升与所述入站消息关联的安全性状态。

46. 如权利要求 45 所述的系统，其特征在于，如果提升所述安全性状态且所述入站消息与所述第一安全性状态关联，则所述处理器还配置为将所述第二安全性状态与所述入站消息关联，以取代所述第一安全性状态。

47. 如权利要求 45 所述的系统，其特征在于，如果提升所述安全性状态且所述入站消息与所述第一安全性状态关联，则所述处理器还配置为将所述第三安全性状态与所述入站消息关联以取代所述第一安全性状态。

48. 如权利要求 45 所述的系统，其特征在于，所述安全性状态提升是在预定义的时间间隔内进行。

49. 如权利要求 45 所述的系统，其特征在于，确定是否已提升所述安全性状态的步骤包括检测预定义的条件。

50. 如权利要求 45 所述的系统，其特征在于，确定是否已提升所述安全性状态的步骤包括从系统管理员处接收指令。

用于控制对电子消息接收者的访问的系统和方法

[0001] 相关申请

[0002] 本申请要求 2004 年 5 月 25 日提交的美国临时申请号 60/574239、标题为“用于使用多个代理标识符控制对电子消息接收者的访问的系统和方法”(Systems and Methods for Controlling Access to anElectronic Message Recipient through the use of a Plurality of ProxyIdentities) 的优先权。

技术领域

[0003] 本公开内容涉及计算机网络，更确切来说涉及用于控制对多种形式的电子通信（例如“电子邮件”、“即时消息传送”）的访问控制的系统和方法，其中使用发送者和接收者标识符在参与者之间传导消息。

背景技术

[0004] 电子邮件（“e-mail”）的强大之处在于定义 e-mail 消息的内容和递交的通用标准协议。遗憾的是，这些标准协议不认证发送者标识，从而对 e-mail 的访问控制难以提出。在最近几年，对 e-mail 缺乏访问控制已经导致商业广告和其他非期望的消息（“垃圾邮件”）的数量泛滥地增加。

[0005] 十多年间，已经有数以百计的尝试要创建对 e-mail 收件箱的控制访问的软件系统。

[0006] 在提交本申请时，全面地来看确信现有反垃圾邮件技术无法解决 e-mail 中的垃圾邮件问题，甚至有预言垃圾邮件已经将媒体置于变得不可使用的危机。

[0007] 最常见的方法是通称为“垃圾邮件过滤”的一种方法。垃圾邮件过滤尝试基于对其内容、发送者的标识符或消息的某些其他特征的评估来确定消息是否是所想要的。

[0008] 过滤器往往存在一个或多个常见的缺陷。过滤器频繁地漏检垃圾邮件消息，并允许它们递交，而且还不正确地将合法的消息标识为垃圾邮件（“误肯定”）。足够漏检大量垃圾邮件但是阻挡合法消息的问题对于大多数用户来说完全是不可容忍的，尤其是在被过滤的消息属于至关重要的公司里。

[0009] 因为过滤器据以识别垃圾邮件的属性通常在发送者的控制下（例如发送者的标识符、主题、消息内容），所以容易绕开过滤器。

[0010] 基于规则的过滤器要求用户和管理员进行规则的持续维护。过滤器可能在计算方面成本高昂，因为每个消息均通过所有规则处理，从而导致消息递交的延迟。

[0011] 限制对电子通信的访问的第二种方法是拒绝所有来自非认证的源的访问，一种技术通常称为“白名单”。这是一种允许“仅被邀请”的消息到达的系统。

[0012] 当将消息发送到白名单保护的 e-mail 地址时，该消息仅在发送者的标识符出现在该白名单上的情况下才被递交。来自白名单上没有的发送者的消息则被拒绝，作为可疑垃圾邮件被隔离或最常见地被质询。每次拒绝行为导致自身的工作负荷，以及合法通信的干扰。

[0013] 因为大多数垃圾邮件发送者不想接收回复消息，所以白名单是有效的，由此基于消息的质询多数只会到达合法消息发送者。

[0014] 更改底层 e-mail 协议不会缓解问题。IETF（定义和支持 RFC e-mail 标准的实体）已经在 1999 年定义了对标准 e-mail 通信的认证扩充，称为 ESMTP。尽管 ESMTP 已经伴随我们四年，但是罕有邮件主机要求发送者使用 ESMTP，因为这样做将会拒绝主要多数的采用通用非认证标准 (SMTP) 发送的消息。所以在每个人都这样做之前，没有人会转移到 ESMTP 标准，从而导致对 SMTP 的持续且永久性依赖。

[0015] 尝试对 email 设置收费控制系统（例如每个消息付费的 e-mail 和捆绑的 e-mail）或尝试从法律方面的知识产权保护（例如在消息头中的商标诗）的商业方案要求太多的设置以及后续工作才够为大多数用户所接受。

[0016] 促成本发明的关键理念一直接受如下事实，即使并非不可能，设计一种将混合在一个集合中的所有期望的消息与非期望的消息分离的系统也是非常困难的。这样做的多种多样的尝试并未达到针对垃圾邮件的完全保护而且不阻挡合法消息。

[0017] 解决方案存在于这样一种系统或方法中，可以由用户或企业单方面采用该系统或方法，以防止期望的消息和非期望的消息混合在同一个集合中。

发明内容

[0018] 根据本公开内容的一个方面，一种用于选择性地允许或拒绝对耦合到电子通信网络的用户的访问的系统，包括通过电子通信网络从发送者接收入站消息的接收器。该入站消息包含与发送者关联的标识符和与接收者关联的标识符。该系统还包括处理器，该处理器用于确定与接收者关联的标识符是否是由用户先前生成的以及是否是与接收者关联的多个代理标识符中所没有的。处理器还确定与入站消息关联的至少三个安全性状态的其中之一。第一安全性状态指示允许将入站消息递交到用户。第二安全性状态指示拒绝将入站消息递交到用户。第三安全性状态指示有条件地允许将该消息递交到用户。这三个安全性状态的每一个状态与入站消息中包含的发送者标识符和接收者标识符关联。

[0019] 在一个实施例中，该处理器可以配置为将与接收者关联的标识符添加到多个代理标识符中。确定接收者标识是由该用户先前生成的步骤可以包括将接收者标识符的一部分分离，以确定多个代理标识符中是否包含该部分。如果第一安全性状态与入站消息关联，则该处理器可以从入站消息中移除接收者标识符。

[0020] 根据本公开内容的另一个方面，一种用于选择性地允许或拒绝对耦合到电子通信网络的用户的访问的系统，包括通过电子通信网络从发送者接收入站消息的接收器。该入站消息包含与发送者关联的标识符和与接收者关联的标识符。该系统还包括处理器，该处理器配置为确定与入站消息关联的至少三个安全性状态的其中之一。第一安全性状态指示允许将入站消息递交到用户。第二安全性状态指示拒绝将入站消息递交到用户。第三安全性状态指示有条件地允许将该消息递交到用户。至少三个安全性状态的每一个状态与入站消息中包含的发送者标识符和接收者标识符关联。如果允许递交，则处理器还配置为向入站消息添加注脚。该注脚配置为用作用户的界面。

[0021] 在一个实施例中，注脚可以包含入站消息中所含的信息。在一个实施例中，注脚可以包括表示与入站消息关联的安全性状态的信息。该处理器可以配置为调整注脚，用于更

新注脚表示的信息。该处理器还可以配置为调整注脚，用于更新注脚表示的信息，其中用户发起该调整。基于所确定的安全性状态，该处理器可以延迟入站消息的递交。

[0022] 根据本公开内容的另一个方面，一种用于选择性地允许或拒绝对耦合到电子通信网络的用户的访问的系统，包括通过电子通信网络从发送者接收入站消息的接收器。该入站消息包含与发送者关联的标识符和与接收者关联的标识符。该系统还包括处理器，该处理器配置为确定与入站消息关联的至少三个安全性状态的其中之一。第一安全性状态指示允许将入站消息递交到用户。第二安全性状态指示拒绝将入站消息递交到用户。第三安全性状态指示有条件地允许将该消息递交到用户。至少三个安全性状态的每一个状态与入站消息中包含的发送者标识符和接收者标识符关联。该处理器还配置为确定入站消息是否豁免于安全性状态并基于安全性豁免 (exemption) 递交入站消息。

[0023] 在一个实施例中，安全性豁免可以基于与发送者关联的标识符。安全性豁免可以基于与接收者标识符关联的域。安全性豁免可以基于包含相似域的接收者标识符和发送者标识符。安全性豁免可以基于入站消息，该入站消息是对发送到豁免和非豁免接收者的另一个消息的回复消息。安全性豁免可以在一段时间间隔内有效。该处理器还可以配置为存储表示入站消息的递交的数据。

[0024] 根据本公开内容的另一个方面，一种用于选择性地允许或拒绝对耦合到电子通信网络的用户的访问的系统，包括配置为通过电子通信网络从发送者接收入站消息的接收器。该入站消息包含与发送者关联的标识符和与接收者关联的标识符。该系统还包括处理器，该处理器配置为确定与入站消息关联的至少三个安全性状态的其中之一。第一安全性状态指示允许将入站消息递交到用户。第二安全性状态指示拒绝将入站消息递交到用户。第三安全性状态指示有条件地允许将该消息递交到用户。至少三个安全性状态的每一个状态与入站消息中包含的发送者标识符和接收者标识符关联。确定安全性状态的步骤包括确定何时接收到包含与发送者关联的标识符和与接收者关联的标识符的先前消息。

[0025] 在一个实施例中，该处理器还可以配置为在入站消息与先前消息的接收之间的时间间隔小于预定义的时间的情况下递交入站消息。

[0026] 根据本公开内容的另一个方面，一种用于选择性地允许或拒绝对耦合到电子通信网络的用户的访问的系统，包括通过电子通信网络从发送者接收入站消息的接收器。该入站消息包含与发送者关联的标识符和与接收者关联的标识符。该系统还包括处理器，该处理器配置为确定与入站消息关联的至少三个安全性状态的其中之一。第一安全性状态指示允许将入站消息递交到用户。第二安全性状态指示拒绝将入站消息递交到用户。第三安全性状态指示有条件地允许将该消息递交到用户。至少三个安全性状态的每一个状态与入站消息中包含的发送者标识符和接收者标识符关联。该处理器还确定是否已经提升与该入站消息关联的安全性状态。

[0027] 在一个实施例中，如果提升安全性状态并且入站消息与第一安全性状态关联，则处理器可以将第二安全性状态与该入站消息关联以取代第一安全性状态。如果提升安全性状态并且入站消息与第一安全性状态关联，则处理器可以将第三安全性状态与该入站消息关联以取代第一安全性状态。安全性状态提升可以在一段预定义的时间间隔内发生。确定是否已提升安全性状态的步骤可以包括检测预定义的条件。确定是否已提升安全性状态的步骤可以包括从系统管理员处接收指令。

[0028] 从下文详细描述中，本领域技术人员将容易地显见到本发明公开内容的其他优点和方面，其中仅通过说明实现本发明而构想的最佳实施方式来图示并描述了本发明的实施例。例如，公开内容中结合描述系统来描述方法和计算机产品实现。如将描述的，在未背离本发明公开内容的精神的前提下，本发明公开内容能够实现其他和不同的实施例，它的许多细节可容易地在显见的方面进行修改。因此，这些附图和描述本质上视为说明性的，而非限定性的。

附图说明

[0029] 图 1 是表示电子通信系统的体系结构的框图。

[0030] 图 2 是表示 e-mail 通信量如何填充数据库以及在安全性模块的实施之前所遵循的其他初始步骤的流程图。

[0031] 图 3 是表示以实施模式工作的产品的安全性模块的逻辑和行为的流程图。

[0032] 图 4 是表示产品以标记模式工作时安全性模块的逻辑和行为的流程图。

[0033] 图 5 是表示根据消息场景（即谁在发送该消息，使用什么代理以及发给谁）和多种安全性设置的多种地址转换结果的公式表。

[0034] 图 6 是表示仅隐含安全性豁免的操作的流程图。

[0035] 图 7 是包括登录页面的图形用户界面。

[0036] 图 8 是包括联系人列表的图形用户界面。

[0037] 图 9 是包括联系人详情页面的图形用户界面。

[0038] 图 10 是包括 Reflexion 用户选项页面的图形用户界面。

[0039] 图 11 是包括管理员添加全局豁免页面的图形用户界面。

[0040] 图 12 是包括管理员创建新用户页面的图形用户界面。

[0041] 图 13 是表示即时名称 (Name-on-the-Fly) 的地址创建的操作的流程图。

[0042] 图 14 是表示将注脚添加到入站消息的操作的流程图。

[0043] 图 15 是表示从出站消息中移除注脚的操作的流程图。

[0044] 图 16 是表示接收消息时安全性实施的操作的流程图。

[0045] 图 17 是表示冷联系人防病毒的流程图。

[0046] 图 18 是表示抵御病毒和基于容量的攻击的禁闭防范的流程图。

具体实施方式

[0047] 本发明（“产品”）提供用于控制电子通信（例如“电子邮件”、“即时消息传送”）形式的访问的系统和方法，其中通过创建和管理用作受保护的原始标识符（“始发者”）的替换的多个代理标识符（“代理”），使用发送者和接收者标识符在参与者之间递交消息，这些代理的每一个具有定义访问权的离散安全性状态，这些访问权对应于据以与始发者（“联系人”）通信的消息传送群体 (community) 的部分。

[0048] 通常，至少有三个安全性状态，在许多实施例中有多于三个安全性状态，这些安全性状态控制代理标识符（例如 e-mail 地址）在消息递交期间作为对目的地标识符访问的限制、创建代理标识符（例如 e-mail 地址）和将代理标识符（例如 e-mail 地址）替换用于对消息中的源标识符的引用的方式。

[0049] 该系统可以支持总体上彼此相互作用的多个（即，多于三个）安全性设置，从而得到离散的安全性状态和相应行为的矩阵。本实施例中安全性状态的多样性提供比例如允许或禁止访问的二进制状态系统更精确的系统行为。在本实施例和其他实施例中，可以允许某些群体的用户访问其他用户不能访问的地方，即使是在发送到相同目的地标识符的消息中。为了实现访问控制，可以拒绝、质询、隔离或接受消息，并且每个具有不同的变化。

[0050] 能以多种方式定义代理 e-mail 地址，包括在通过系统处理消息时由本产品自动创建和指定、由企业或个人用户显式地创建和指定以及遵循预先确定源 e-mail 地址和初始安全性状态的命名约定的隐含创建。

[0051] 对代理 e-mail 地址的引用可以转换成或不转换成对应的源地址，具体取决于安全性状态。例如，在整个消息中，以源标识符替换对产品自动创建的代理标识符的引用。不以源标识符替换显式地创建的或通过命名约定定义的代理地址（并因此对于用户是已知的）。

[0052] 本产品由三个系统构成：Reflexion 邮件服务器 (RMS)、管理 Web 网站 (AWS) 和数据库服务器。

[0053] 三个系统可以驻留在一个服务器中或以多种配置集群在多个服务器上。

[0054] 通常，往返于始发者的大多数外部消息均通过本产品。从始发者到外部接收者（“联系人”）的消息本文称为“出站消息”；从外部发送者（也称为“联系人”）到始发者的消息本文称为“入站消息”。

[0055] Reflexion 邮件服务器（“RMS”）采用两个存储队列，在一个队列中驻留入站通信消息直到安全性模块处理它们（“预处理队列”）为止，而另一个队列中放置处理的消息和退回消息以便进行最后递交（“递交队列”）。

[0056] SMTP 递交的传输封装中指定的发送者和接收者 e-mail 地址是安全性模块的关键。安全性模块基于如下文定义的交互安全性状态的组合来确定是否应该将该消息递交到预期的接收者。如果确证的话，可以向发送者回送多种错误消息和告警。

[0057] 递交的消息通常具有由 RMS 附着于消息底部的注脚连同至 Reflexion 向导的链接，Reflexion 向导是用作用户与本产品的主界面的多态浏览器界面。

[0058] Reflexion 邮件服务器也管理作为本发明的核心安全性设备的代理标识符阵列的创建和使用。

[0059] 代理地址

[0060] 为每个联系人指定一个或多个代理地址，每个代理地址是 RFC- 相容 e-mail 地址（即与大多数常见 e-mail 协议的命名约定兼容的地址；有关 e-mail 协议的更多信息，参见 http://www.ietf.org/rfx.html）。在本申请的上下文中，“代理标识符”与“代理地址”是同义的。

[0061] 在第一参考上为每个联系人指定它自己的代理地址作为传送通过 RMS 的消息中的发送者或接收者。本产品基于作为属性存储在每个安全性代码上的企业和用户偏好和缺省值来控制对基础结构的访问。

[0062] 如下是从始发者到外部联系人的消息：

[0063] 1. 通过主机企业的现有 e-mail 底层设施处理出站消息，并到达实施本发明的本产品。

[0064] 2. 本产品自动指定并记录唯一的代理地址，如将其登记以供联系人使用。如果代理地址先前已指定给该联系人，则将重复使用它。

[0065] 3. 将对出站消息的消息头和消息体中的始发者地址的所有引用更改为对应的代理地址。例如，来自始发者地址的消息：

[0066] From :ssmith@company.com

[0067] 发送到外部联系人。因为该消息通过本产品，所以对始发者地址 ssmith@company.com 的所有引用被更改为对应于接收者的代理地址，本示例中为：

[0068] From :ssmith.123@company.com

[0069] 当该消息到达联系人的收件箱中时，消息看上去像是始发于地址 ssmith.123@company.com（重点在于“.123”），而非来自 ssmith@company.com。

[0070] 在该实例中，代理地址保持始发者身份的个性化，局部仍具有“ssmith”并且域仍为“company.com”。在其他实施例中，代理地址可以容易地不保持来自始发者地址的可见出处。例如，如 123@company.com 的地址可以指定为 ssmith@company.com 的代理地址。在再一个示例中，如 123@321.com 的地址可以指定为 ssmith@company.com 的代理地址。通常每个代理地址相对于其他代理地址是唯一的，以便每个代理地址可以与其他代理地址区分开。

[0071] 4. 在将始发者地址的引用变更为代理地址之后，该消息如同未作任何处理的 e-mail 消息一样被递交。

[0072] 如下是经由代理地址从外部联系人向始发者发回消息：

[0073] 1. 外部联系人将出站消息发送到代理地址，最终到达 RMS。

[0074] 2.RMS 安全性模块基于包含的地址的安全性状态确定消息的递交安排，地址的安全性状态包括但不限于：

[0075] a. 消息递交被拒绝，消息不向发送者提供任何追索。结束处理。

[0076] b. 消息递交被拒绝，消息向发送者提供新代理。结束处理。

[0077] c. 消息递交被接受，消息被标记为“可疑”。进行到步骤 3。

[0078] d. 消息递交无保留地被接受。进行到步骤 3。

[0079] 3. 对于授权用于递交的消息，将入站消息的消息头和消息体中的代理地址的所有引用更改为对应的始发者地址。接续本示例，至代理地址的消息：

[0080] To :ssmith.123@company.com

[0081] 当该消息到达联系人的收件箱中时，消息看上去像是已从外部联系人发送到始发者的地址 ssmith@company.com。

[0082] 以此方式，在最终递交时未暴露入站消息的代理地址，从而使访问控制协议的机制对用户透明。

[0083] 用户可以禁用或限制使用一个安全性代码而不影响任何其他安全性代码。

[0084] 访问控制难以被绕开，这是因为驻留在 e-mail 地址本身上的安全性设置所致，因此发送者说他们是谁或他们在消息中放置了什么都无关紧要，因为地址本身一旦被废弃将不再有效。

[0085] 关于管理 Web 网站

[0086] 管理 Web 网站（“AWS”）提供对代理阵列、安全性设置和通信历史的完全控制、完

全公开界面。

[0087] AWS 构建在三层体系结构上：

[0088] 1. Java 服务器页面和 Servlets

[0089] 2. 数据服务器

[0090] 3. 应用服务器

[0091] 服务器页面定义应用接口，从数据库服务器更新和请求数据，并构造供应用服务器服务于用户浏览器的结果页面和表单。

[0092] 在服务器页面和 servlet 定义的界面内，有许多专用于应用的对象。

[0093] 用户

[0094] 对整个 AWS 的访问要求用户证书的成功认证。在优选实施例中，AWS 要求使用用户 ID 和对应的密码来成功登录。

[0095] 对 AWS 内的每个页面加强了认证和证书要求。

[0096] AWS 中支持的有三个级别的用户，每个级别具有不同的访问特权：

[0097] 1. 超级管理员－完全访问且可以访问服务器配置和控制方法的唯一用户类型。对整个通信历史细节和概要的访问。

[0098] 2. 域组管理员 (DGA)－对域组本身的完全访问，域组的用户，DGA 指定的域组的通信历史。

[0099] 3. 用户－对用户自己选项、代理地址和个人历史的访问。

[0100]

属性	描述
登录 ID	登录到管理 Web 网站期间使用的名称或 e-mail 地址
密码模式	登录到管理 Web 网站 Reflexion 期间使用的密码具有不同的总安全性模式： 1. 实施－当消息无法递交时向发送者发送拒绝和质询消息 2. 标记－保证所有消息递交到接收者。在实施模式会被拒绝或质询的消息被“标记”(即提供可见指示符，以指示该消息在实施模式中不会被递交。) 3. 通过－至接收者的消息将完全跳过安全性模块并直接递交。 4. 逆向－用于消除代理地址的相关性，表面上准备移除本产品。卸下所有安全性，并且至代理地址的任何消息导致向发送者发送请求消息，以请求基于原始地址向接收者再发送消息。对于发送到代理地址的消息，标记消息。

注脚	因为消息通过本产品，所以 RMS 将注脚附着于每个消息的底部。有三种类型的注脚可提供给每个用户： 1. 标准注脚 - 包含连接到 Reflexion 向导的单个链接。 2. 高级注脚 - 包含标准注脚中没有的大量附加信息和链接。 3. 无注脚 - 注脚不是必需的；此类型将其关闭。
消息存储自动豁免	保存被拒绝或质询的消息的副本的选项。当用户回复来自联系人的被标记消息时自动豁免联系人的选项。

[0101]

[0102] 服务器

[0103] 服务器对象包含专用于本产品的全部安装的属性和方法。服务器对象仅可供具有“超级管理员”特权的用户使用。

[0104] 大多数属性与作为通用邮件服务器的本产品的属性相关。它们包括队列有效期的设置、管理 Web 网站的 IP 地址、数据库备份时间表等。

[0105] 域组

[0106] 每个 Reflexion 安装可以支持任何数量的企业。在本产品上企业作为域组来管理。域组可以具有任何数量受管理的域、任何数量具有地址在这些域的用户、以及任何数量管理域组的域组管理员 (DGA)。

[0107] 联系人

[0108] Reflexion 将向用户发送或从用户接收消息的所有外部联系人编目。联系人是具有安全性设置的代理地址，也是该代理地址登记到的该联系人的安全性简介信息。

[0109] 属性 描述

[0110] 联系人名称 联系人的代理地址登记到的联系人的名称。从来自

[0111] 联系人的入站消息中分析联系人名称来。

[0112] 真实地址 联系人的 e-mail 地址（不要与指定给用户的代理地址

[0113] 混淆）。

[0114] 代理地址 由 RMS 指定给联系人的 Reflexion 代理地址。

[0115] 安全性状态 每个代理地址具有如下安全性状态的其中之一：

[0116] 1. 公用 - 此代理可以被任何人使用和共享，并且发往它的消息将被递交。

[0117] 2. 受保护 - 仅“适合”的联系人可以使用此代理地址，不适合的联系人将被质询（实施模式）或他们的消息将被标记（标记模式）。

[0118] 3. 不共享 - 仅“适合”的联系人可以使用此代理地址，不适合的联系人将被拒绝（实施模式）或他们的消息将被标记（标记模式）。

[0119] 4. 禁用 - 发往该代理地址的任何邮件将不会被递交（对于豁免发送者除外）。

[0120] 消息存储 保存被拒绝或质询的消息的副本的选项。

[0121] 自动豁免 当用户回复来自联系人的被标记消息时自动豁免联

[0122] 系人的选项。

[0123] 即时名称 如果被启用，则允许“即时地”定义新代理地址（即

[0124] (NOTF) 无需与本产品进行任何交互），该新代理地址是由此
[0125] 联系人的代理地址派生的。例如，如果此联系人的
[0126] 代理地址是：
[0127] proxy@company.com
[0128] 以及 NOTF 已启用，则用户可以创造如下形式的任何
[0129] 新代理地址：
[0130] proxy.new@company.com
[0131] 其中“new”是用户希望的任何内容。该 NOTF 代理
[0132] 将被指定给使用它的第一个联系人（参见图 13）。
[0133] 有效期限 可以对代理地址赋予限定的有效期限。当代理“过
[0134] 期”时，将安全性状态设为禁用。

[0135] 豁免

[0136] Reflexion 支持用于标识不应受安全性实施影响的发送者地址的数据项。Reflexion 的个人用户或企业用户可以设置四种显式豁免。包括 e-mail 的豁免，但是该技术可以应用于任何形式的电子通信：

[0137] 1. 豁免单个 Reflexion 用户的单个发送者标识符 (e-mail 地址）。

[0138] 2. 豁免单个 Reflexion 用户的整个主机和域（例如“company.com”）。

[0139] 3. 豁免企业内的所有用户的单个发送者标识 (e-mail 地址）。

[0140] 4. 豁免企业内的所有用户的整个主机和域（例如“company.com”）。

[0141] 对于远程通信方发送或接收的每个消息（即，其地址对于受保护的企业不是本地的发送者），只要与具有上文列出的四种对应豁免分类的任何一种的发送者地址匹配，则将使该通信方作为“豁免”对待。

[0142] 豁免发送者不受 Reflexion 安全性影响，这意味着通过作为豁免，来自豁免发送者的所有消息都将递交。发往豁免接收者的消息将禁止使用 Reflexion 地址。

[0143] Reflexion 中的显式豁免的主要用途是，使已经取决于原始地址的远程通信方无需更改它们的行为或用于到达 Reflexion 用户的 e-mail 地址，尤其是当 Reflexion 用户开始使用具有已存在垃圾邮件问题的应用程序时。

[0144] 如下是 Reflexion 用户停止已存在的垃圾邮件问题的过程：

[0145] 1. 提升原始 e-mail 地址的安全性，通常将安全性状态从“公共”提高到“受保护”。

[0146] 2. 豁免已知 e-mail 地址和合法联系人的域，从而允许那些联系人未降低地继续使用原始地址。

[0147] 3. 将安全性实施设为“标记模式”以保证所有消息到达用户。

[0148] 4. 用户将不在豁免列表上的合法联系人（即其消息以“已标记”方式到达）添加到豁免列表。

[0149] 5. 当 Reflexion 用户确信所有合法联系人在豁免列表上，且所有标记的消息都是非期望的时，他们可以选择以将安全性实施更改为“实施模式”，在之后的时间将很少需要将地址和主机和域添加到豁免列表。

[0150] 系统还允许用户取消豁免的联系人。作为选项，每个用户或企业可以指示 Reflexion 向豁免联系人发送礼貌请求：他们应该将他们发往该用户的 e-mail 地址更改为

唯一的代理地址，该操作由来自该豁免联系人的消息的到达被触发。当消息到达推荐的代理地址时，对该联系人清除豁免状态。

[0151] 有 Reflexion 支持的隐含联系人。如果任何 Reflexion 用户发送到两个或两个以上外部联系人的消息，其中这些联系人的至少其中一个是豁免的而这些联系人的其中一个不是豁免的，则非豁免联系人将具有应用为他们的地址记录的仅隐含安全性豁免。该隐含豁免允许非豁免用户绕开有关入站消息的安全性（但是将不禁止对发往他们的出站消息使用唯一的代理地址）。有关应用程序中为什么和如何支持仅隐含安全性豁免的示例，参见图 6。

[0152] 历史

[0153] 本产品记录有关向企业内或企业外发送的每个消息的描述性信息。个体消息历史项目被合并到一起以用于历史概要报告，并在保留在线可配置的时间长度之后被丢弃。

[0154] 参考图 1，Reflexion 邮件服务器采用 2 个 e-mail 队列，一个队列 102 用于入站业务，消息驻留在其中直到安全性模块处理它们（“预处理的队列”）为止，而第二个队列 106，其中放置已处理消息和退回消息用于最终递交（“递交队列”）。

[0155] 接收入站消息（来自企业 100 的邮件服务器或外部联系人 114 的邮件服务器）并将其存储在入站队列 102 中。来自外部源 114 的入站消息受本产品的安全性影响。

[0156] 在使用 SMTP 协议 112 接收入站消息期间，发生安全性实施。一旦接收到传输封装发送者和接收者地址，则 SMTP 协议处理程序向 Reflexion 安全性模块 110 发送请求以获取该消息 116 的安全性安排。使该入站消息的余下部分的后续处理依据从 Reflexion 安全性模块 108 返回的安全性响应 118 来判定。

[0157] 如果可以递交该消息，则将其存放在预处理队列 102 中。如果该消息无法递交，则将延迟或拒绝 120 回送到发送服务器 114。

[0158] 受延期影响的消息仅延迟某个时间（通常 30 至 60 分钟）。这是测试，检验发送服务器 114 是否“行为良好”。发送垃圾邮件的许多服务器不处理被延期的消息，因此延迟的消息将不会被此类消息源重发。

[0159] 使用典型的队列调度器，由本产品的消息转换模块 104 处理每个入站消息，以在递交队列 106 中存放：

[0160] 1. 按消息“原样”，或

[0161] 2. 具有添加、修改或其他转换级别的消息，下文将对此予以描述。

[0162] 递交队列 106 将入站消息递交到企业的内部 e-mail 基础设施 100 或外部目的地 114。递交队列可以使用标准目的地查询机制以解析递交位置（例如域名服务 DNS）或将邮件发送到已知内部域直到内部 e-mail 基础设施 100 和将每个邮件发送到因特网 114 的路由选择表。

[0163] 参考图 2，描述入站消息准备。当本产品处理邮件时，它利用新代理地址、容量统计和历史跟踪更新数据库。图 2 详细描述优选实施例中接收入站消息期间所做的数据库准备。

[0164] 入站消息准备在对给定消息返回安全性安排之前进行。

[0165] 通常，对入站消息检查的第一件事是接收者地址是否在 Reflexion 保护的域中 200。

[0166] 注意，到达 Reflexion 的消息必须发送到其域正被 Reflexion 保护的地址（“入站”）或从此类地址发送（“出站”）。本地邮件应该以本地方式递交；因此 Reflexion 应该从不查看在同一个域中的地址之间往返的 e-mail。

[0167] 邮件要从一个企业发送到另一个企业且两个企业的域都寄放在一个 Reflexion 安装上是可能的。在此情况中，首先将消息作为来自第一个企业的出站消息处理，然后将其作为发往第二个企业的入站消息处理。

[0168] 如果 Reflexion 的此安装从未遇到过该发送者的地址 202，则将其添加到“真实地址”的数据库表中 204。

[0169] 接下来，本产品搜索数据库以查看该接收者地址是否是已签发的代理地址 206。

[0170] 如果不存在别名，则通过公知为“即时名称”(NOTF) 的命名约定来创建地址 210 仍是可能的，在此情况中应该基于从命名约定中提取的信息创建代理地址并将其登记到受保护的用户 212。如果对于未知的代理地址不允许 NOTF，则拒绝该消息 208（有关 NOTF 的更多信息，参见图 13）。

[0171] 在这一点上，数据库中存在代理地址。启动跟踪历史系统的消息结果 220。

[0172] 为了发现代理替换的用户，在优选实施例中需要首先导航到用户的原始地址 218，再从这里到用户记录 216。在其他实施例中，可以使用多个其他策略来实现此目的，但是必须掌握有该用户的身份才能进行。

[0173] 如果未将代理地址登记到任何给定用户 214，则将其登记到当前发送者 222。该情况可以因两个可能的情况而发生。第一，刚使用 NOTF 创建了代理地址，因此不被拥有。第二，可以在使用之前以显式方式创建代理地址，在此情况中它在第一次使用之前是未被拥有的，其中与刚刚 NOTF 代理一样它得以登记到第一个用户 222。

[0174] 然后检查 224 发送者的豁免状态以向 Reflexion 安全性模块以及还有地址转换模块提供信息。豁免发送者不受访问控制的影响，往返于豁免联系人的所有邮件均在受保护用户的原始内部地址下进行。

[0175] 参考图 3，描述安全性实施。一旦完成入站消息准备，则 Reflexion 将确定该消息的安全性安排。

[0176] 有两个活动安全性模式可供 Reflexion 用户使用：实施模式和标记模式。

[0177] 图 3 详细描述对于发送到采用实施模式的用户的消息优选实施例安全性模型所遵循的逻辑。

[0178] 通过定义，发往 Reflexion 保护的域的所有入站邮件都是代理标识符，即使接收者地址与原始内部地址是不可区分的。每个原始内部地址具有含相同地址的代理地址，以便允许对原始地址本身设置安全性。

[0179] 首先调查接收者地址的安全性状态。

[0180] 发往公共代理的消息

[0181] 如果接收者代理地址具有“公共”的安全性状态 300，则检查发送者的豁免状态 302。如果发送者是豁免的，则绕开安全性，并将该消息传递到后续消息转换阶段并将其递交 338。

[0182] 如果登记到发送者的代理地址与用作该消息的接收者地址的代理地址不同（在附图中未明确地说明此情况，但是存在这种情况），则本产品将在允许递交之前检查发送者

的代理上设置的安全性。

[0183] 如果指定给发送者的代理是公共的 312 或是受保护的 320，则允许该消息通过安全性 338。如果登记到发送者的代理是受保护的，则向发送者发送提示消息以便在将来使用他们自己的代理地址 322。

[0184] 如果发送者的代理是“不共享”328，则不允许递交该消息。而是向发送者回送请求，以请求发送者使用登记到该发送者的代理地址重发消息（与该消息中的接收者所用的代理相反）。

[0185] 所以即使将消息发送到公共代理地址，发送者的代理地址的安全性状态仍可以更改或禁止该消息的递交。

[0186] 发往受保护代理的消息

[0187] 如果接收者代理地址具有“受保护”的安全性状态 304，则检查是否允许发送者向该代理地址发送邮件。

[0188] 目前，有三种方式发送者可以被授权使用受保护代理。第一，如果发送者是豁免的 314，则绕开安全性，并将消息传递到后续消息转换阶段并将其递交 338。其次，如果发送者是登记到代理地址的通信方 324，则授权并完成递交 338。最后，如果发送者来自与登记到代理地址的联系人相同的域，且该域不是例如 AOL、Yahoo、Hotmail 等（可配置的列表）的主要 ISP 的其中之一，并且该代理上启用允许域级共享的安全性属性 332，则授权该消息递交 338。

[0189] 向未获授权使用受保护代理的发送者发送如下请求：向允许发送者使用的代理地址重发消息 316。该消息实质上告知“代理地址 x 已经更改为发送者的代理地址 y。请将您的消息重发送到 y”。

[0190] 受保护地址用于防止不具有有效返回地址的垃圾邮件，但是向合法联系人提供允许递交消息的重发机制。

[0191] 发往非共享代理的消息

[0192] 如果接收者代理地址具有“非共享”的安全性状态 306，则检查是否允许发送者向该代理地址发送邮件。

[0193] 目前，有三种方式发送者可以被授权使用受保护代理。第一，如果发送者是豁免的 314，则绕开安全性，并将消息传递到后续消息转换阶段并将其递交 338。其次，如果发送者是登记到代理地址的通信方 324，则授权并完成递交 338。最后，如果发送者来自与登记到代理地址的联系人相同的域，且该域不是例如 AOL、Yahoo、Hotmail 等（可配置的列表）的主要 ISP 的其中之一，并且该代理上启用允许域级共享的安全性属性 332，则授权该消息递交 338。

[0194] 向未获授权使用受保护代理的发送者发送不提供重发该消息的任何追索的递交消息的拒绝 316。未获授权使用受保护地址与未获授权使用非共享地址之间的差异在于受保护代理拒绝提供成功重发消息的方式，而非共享拒绝不提供。

[0195] 就非共享代理来说，成功发送 e-mail 消息的要求从仅知道接收者地址提升到要同时知道接收者和对应的登记到代理的发送者地址。非共享代理为有安全性意识的机构提供非常有效但是轻量级保护以防止公知的“目录获取攻击”。目录获取攻击是一种用于通过向目标域中的大量不同地址发送消息来获取有用的 e-mail 地址的技术。无论如何，只要地

址不导致“无此用户”,即假定为有效的。

[0196] 就非共享代理来说,直接获取将不会成功,除非发送者知道每次尝试时假冒正确发送者的地址。

[0197] 发往已禁用代理的消息

[0198] 如果接收者代理地址具有“禁用”的安全性状态 308,则检查发送者是否是豁免的,这是用户采用实施模式安全性的情况下发往禁用代理的消息可以被递交的唯一方式。

[0199] 参考图 4,描述标记安全性。具体来说,详细描述优选实施例安全性模型用于将消息发送到采取标记模式的用户所遵循的逻辑。

[0200] 标记模式确保所有入站消息将被递交到用户的收件箱。

[0201] 该逻辑几乎与图 3 描述的相同,唯一实质差异在于,在标记模式中,无论如何只要确定发送者未获授权向接收者代理发送消息,并不向实施模式中那样发送拒绝或重试消息,而是本产品将只利用前缀标记主题行,以指示该发送者未获授权将该消息发送到选定的代理地址 422/426。

[0202] 重点要注意的是,主题行标记仅在主机企业内是可见的 ;对标记的消息的回复在离开该企业的途中由 Reflexion 移除其中的标记。

[0203] 标记模式服务三个重要的产品要求 :

[0204] 1. 为新用户提供平滑地迁移到使用 Reflexion 的操作模式,从而确保将不会因 Reflexion 加重外部联系人的工作负荷 (“过渡”)。在新用户的过渡期间,清除已存在的垃圾邮件问题。

[0205] 2. 向很少或不容许合法但未预料的消息被阻挡的用户提供保证将所有邮件递交到用户的收件箱。标志模式对于角色为销售、商业开发或主管位置的那些人来说是理想的,这些人派发大量的名片,未预料的消息的价值和频率高。

[0206] 不更改或无法更改他们的 e-mail 行为的用户将永久以标记模式操作本产品。这些用户 (或他们的管理员) 还可以禁止一起使用多个代理地址,从而使用户能够继续如常地使用他们的一个且仅一个地址,仍接收垃圾邮件免除。

[0207] 停止已存在的垃圾邮件问题

[0208] 具有已存在的垃圾邮件且开始使用本产品的新用户能以如下方式结束正发送到现有地址的垃圾邮件 :

[0209] 1. 将整个安全性实施配置为标记模式。

[0210] 2. 使用多种豁免方法的实施例的任何一种豁免所有已知的联系人。豁免联系人允许已经与原始内部地址相关联的合法联系人继续不废弃地使用它。

[0211] 3. 提高具有与原始内部地址相同地址的代理上的安全性。这将导致发送到该代理的任何邮件被标记,除非该联系人在豁免列表上。这是非激进形式的“白名单”,这是在阻挡垃圾邮件时非常有效的常用技术,但是有限制了尤其是公司之间的广泛采用的缺点。

[0212] Reflexion 仅采用这种白名单来停止已存在的垃圾邮件问题。如果新用户开始时没有垃圾邮件问题,则并不一定需要白名单。

[0213] 参考图 5,描述地址转换。一旦已成功清理入站消息以进行递交,则将对代理地址的大多数引用转换成对应的原始内部地址。优选实施例中有一些安全性状态禁止转换代理地址,尤其是即时名称代理 (有关 NOTF 的更多信息,参见图 13)。

[0214] NOTF 代理是由用户定义的，因此驻留在用户的名称空间中。NOTF 代理地址在登录序列中或以 NOTF 代理地址为关键字的其他过程中多次使用。通过禁止转换 e-mail 消息体内的NOTF（与消息头相对，必须转换才能确保消息在现有 e-mail 基础设施内递交），指定使用 NOTF 代理的确认消息会是准确的（即，转换会使信息不正确）。

[0215] 当考虑地址转换时，首先理解仅个体 Reflexion 安装保护的域中的代理地址是转换的候选。而非受保护域中的地址从不转换。

[0216] Reflexion 在数据库内保存一个“真实”地址的目录。受保护域的外部地址和内部原始地址都存储在该真实地址目录 500 中。通过搜索本身作为关键字的代理地址（例如 proxy.123@company.com）或搜索指定给外部联系人以使用对内部原始地址的替换的代理来查找代理地址 502。

[0217] 给定发送者和接收者的真实地址的情况下，可以在出站消息中检索对应的代理，并在消息内替换为对原始内部地址的任何且所有引用。

[0218] 给定代理地址的情况下，可以在入站消息中检索对应的内部原始地址，并在消息内替换为对代理地址的任何且所有引用。

[0219] 当本产品还同时为入站和出站消息转换可能存在或可能不存在但是如果需要会创建的同事的代理地址时，地址转换可能变得更复杂。

[0220] 豁免状态添加了另一个级别的复杂性，因为往返于豁免联系人的 e-mail 导致禁止地址转换。

[0221] 此外，一些外部联系人与第三方代理相关，所以发往这些联系人的消息应该接着使用预期的代理（即在从用户发往该联系人的所有消息中对相同的联系人提供相同的代理）。

[0222] 为了理解图 5，满足语法是有所帮助的。

[0223] 将 504 解读为“取某个地址‘a’并返回它的正确转换的转换方法”。

[0224] 将 506 解读为“返回外部联系人想要看到的代理地址的方法”，这不总是与指定给该联系人的代理地址相同。

[0225] 参考图 13，描述“即时名称”。具体来说，即时名称 (NOTF) 是一种允许创建新的且唯一的代理 e-mail 地址而不使用任何启用设备或软件应用程序的命名技术。就NOTF 而言，Reflexion 用户可以仅遵循预定的命名方案来创建代理地址。

[0226] 通常，命名机制包括：当将消息发送到受 Reflexion 保护的域中的地址而发现尚未在应用程序中创建该地址时，则该未知地址的某些特征可以解析为一个且仅一个 Reflexion 用户。如果该地址未解析为一个且仅一个 Reflexion 用户，且该用户允许创建 NOTF 地址，则 Reflexion 将创建此前未知的代理地址，并将其置于应用程序的管理之下，将它作为代理地址指定给用户，并且根据符合安全性安排的情况递交或拒绝消息。

[0227] 例如，Reflexion 未在已知代理地址的表中发现 702 发送到代理地址 jsmith.hello@company.com 的消息 700。在将该消息作为发送到不存在的用户来处理 708 之前，Reflexion（在本示例中）将本地部分“jsmith”隔离 706，并搜索拥有代理地址 jsmith@.company.com 的用户 712。如果发现，则查看用户 712 是否允许创建 NOTF 代理地址（这能以多种方式实现，下文示例中是优选方法）714。如果允许，则创建新代理地址 jsmith.hello@company.com 720，并如同发送到现有代理 722 一样继续处理该消息，否则作为发送到不存

在用户来处理该消息 716。

[0228] 在主题、用于 NOTF 地址引用的消息的 SMTP 头和体中抑制 Reflexion 地址转换（其中将对代理地址的引用转换成用户的原始地址）。由于两个原因，Reflexion 抑制 NOTF 地址。第一，NOTF 地址最可能是由用户定义的，因此在发送到 NOTF 地址的消息中是已知且预期的。其次，NOTF 地址的公开可以用于登录和密码序列，所以如果将这些类型的序列通过 e-mail 报告给用户（例如“我忘记密码”类型消息），则保留准确的地址是重要的。

[0229] 参考图 14 和 15，描述往消息中添加和从消息中移除注脚。具体来说，附带于每个入站消息底部的是注脚，注脚包含用作与 Reflexion 的安全性模型交互并控制它的主用户界面的有效控件（“注脚”）。

[0230] 对于入站消息 1400，当 Reflexion 处理该消息时收集有关该消息的信息 1402。该信息包括传输封装地址、日期和时间、主题、大小、附件和安全性通过的分辨率（允许、不允许、标记等）。

[0231] 在构造注脚 1404 时根据情况提供并使用所有这些信息。有多种可能的呈示方式可用于实现。在一个实施例中，为有利于用户的目的，注脚可以呈示或给出最相关的操作。例如，如果正在标记消息，则对于用户来说最相关的操作是停止标记消息，使得该操作比其他可能性更突出。在其他实施例中，可以呈示更宽范围的选项，或许与标准注脚结构相符或向用户提供最大选择度和便利。

[0232] 无论注脚是如何构建的，注脚中所含的有效控件支持的操作从它所附的消息中提取上下文。

[0233] Reflexion 构造注脚并将其附于消息 1406，之后才将其递交。可以将注脚附于文档中任何位置，或它可以是文档中至例如浏览器或其他应用程序的外部查看器的链接。

[0234] 在一个实施例中，Reflexion 构造注脚的文本和 HTML 版本，其中使用 HTML 注脚是企业或用户的选项。Reflexion 将入站消息从它们包含的任何原始形式转换成适合的 MIME（多目的因特网邮件扩充，参见 http://www.ietf.org/rfc/rfc2045.txt？ number ＝ 2045）格式，以便可以根据所选的选项查看注脚的文本或 HTML 版本。

[0235] 对于出站消息 1500，Reflexion 首先标识任何和所有注脚的位置 1502，并从消息 1504 中移除它们。移除注脚并非必需的，但是这是本优选实施例中处理消息的方式。

[0236] 参考图 16，描述有关接收消息的安全性实施。具体来说，在最快可能的时间实施安全性。对于 e-mail 通信，安全性实施在接收消息的途中发生，通常使用 SMTP（简单邮件传输协议，参见 http://www.ietf.org/rfc/rfc0821.txt？ number ＝ 821）协议。

[0237] 在消息的 SMTP 递交开始时 1600，在实际的消息本身之前递交传输封装。Reflexion 从传输封装收集发送者和接收者 e-mail 地址 1602，并立即解析该地址的安全性安排，之后才接收消息本身的任何部分（参见图 1 以查看系统体系结构的更多信息）。有三种可能的安全性安排 1606，使消息能够递交，阻止消息被递交（参见图 3）或将消息作为可疑消息来处理。

[0238] 如果消息被拒绝 1614，则可以根据环境向发送者发送消息不可递交的通知、应该将消息重发到新 Reflexion 地址的通知或完全不发送通知。

[0239] 如果允许消息 1610，则 Reflexion 将接受用于递交的消息并完成 SMTP 对话。

[0240] 如果消息的安全性安排为“标记的”，则怀疑该消息为非期望的。不会自动标记和

递交可疑的消息。相反，Reflexion 通过将可疑邮件延迟某个时间来测试发送者的邮件服务器（即邮件传输代理）的行为。

[0241] 第一次接收到新可疑消息时，Reflexion 开始跟踪递交尝试次数和自第一次尝试起递交的总时间 1620。每次尝试递交可疑消息时，Reflexion 检查以查看是否满足或超过测试阈值 1622。如果满足阈值，则接受、标记和递交该消息 1624，否则通知发送者稍后再试 1626。

[0242] 该延迟策略测试可疑（即“标记的”）消息的发送者的邮件服务器（邮件传输代理）是否行为良好。许多垃圾邮件发送者不重试被延迟的消息，因此增加了 Reflexion 的性能并节省已标记消息的递交。

[0243] 参考图 17，描述有关冷联系人防病毒保护的安全性实施。一般来说，“冷联系人”是一种针对潜在的新 e-mail（或其他电子通信媒介）携带的病毒的简单但有效的早期警报系统。签发多个代理地址的 Reflexion 范例使冷联系人成为可能。主机企业设置的任何代理地址处于不活动状态一段时间 1704，则将视为“冷联系人”，其中一个或多个保护性行为在此判断之后被触发，例如可能将原始消息隔离以“安全的”替代项替换 1706。

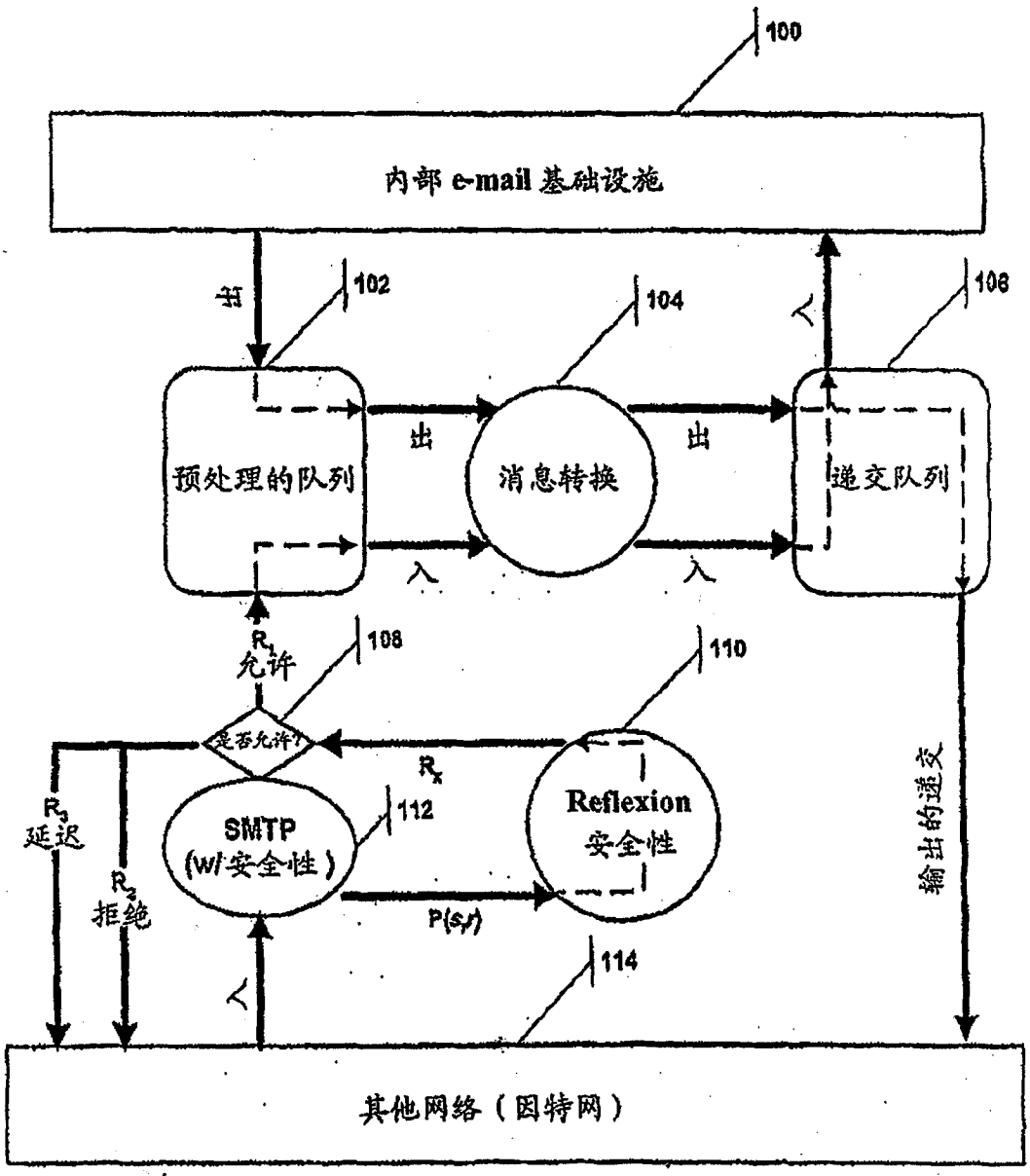
[0244] 冷联系人帮助抵御从合法联系人的地址发送到正确 Reflexion 代理地址而含有病毒扫描器无法检测到的病毒。

[0245] 参考图 18，描述针对病毒和基于容量的攻击的禁闭防范 (lockdown defense)。一般来说，“禁闭”是企业中抵御基于容量的攻击和利用假冒发送者地址散布的 e-mail 携带的病毒的另一种简单但有效的防御。禁闭是企业范围的及安全性上的临时实施，并具有可由 Reflexion 识别的条件自动触发或由系统管理员以显式方式触发的可选行为。

[0246] 当入站消息到达以进行处理 1800 时，Reflexion 如常地检索有关接收者代理地址的安全性状态 1802。对于具有“公共”安全性状态的地址，检查禁闭是否处于生效状态 1804。如果禁闭被启用，则临时将该代理地址上的安全性从“公共”提高到禁闭特征中设置的安全性状态选项，“受保护”或“非共享”1806。使用临时提高的安全性状态并拒绝或允许消息的递交 1808。

[0247] 用于禁闭的一些选项是对“公共”代理实施的临时安全性状态，抑制回送到发送者的不可递交或质询响应消息的选项，以及以图 17 描述的相同方式对冷联系人和含有潜在病毒附件或脚本的消息的隔离的选项。

[0248] 上文已描述一些实现。然而将理解到可以实施多种修改。因此，其他实现属于所附权利要求的范围内。



说明：s=发送者身份

r=接收者身份

P(s, r) = 请求有关从 s 发往 r 的消息的安全性状态

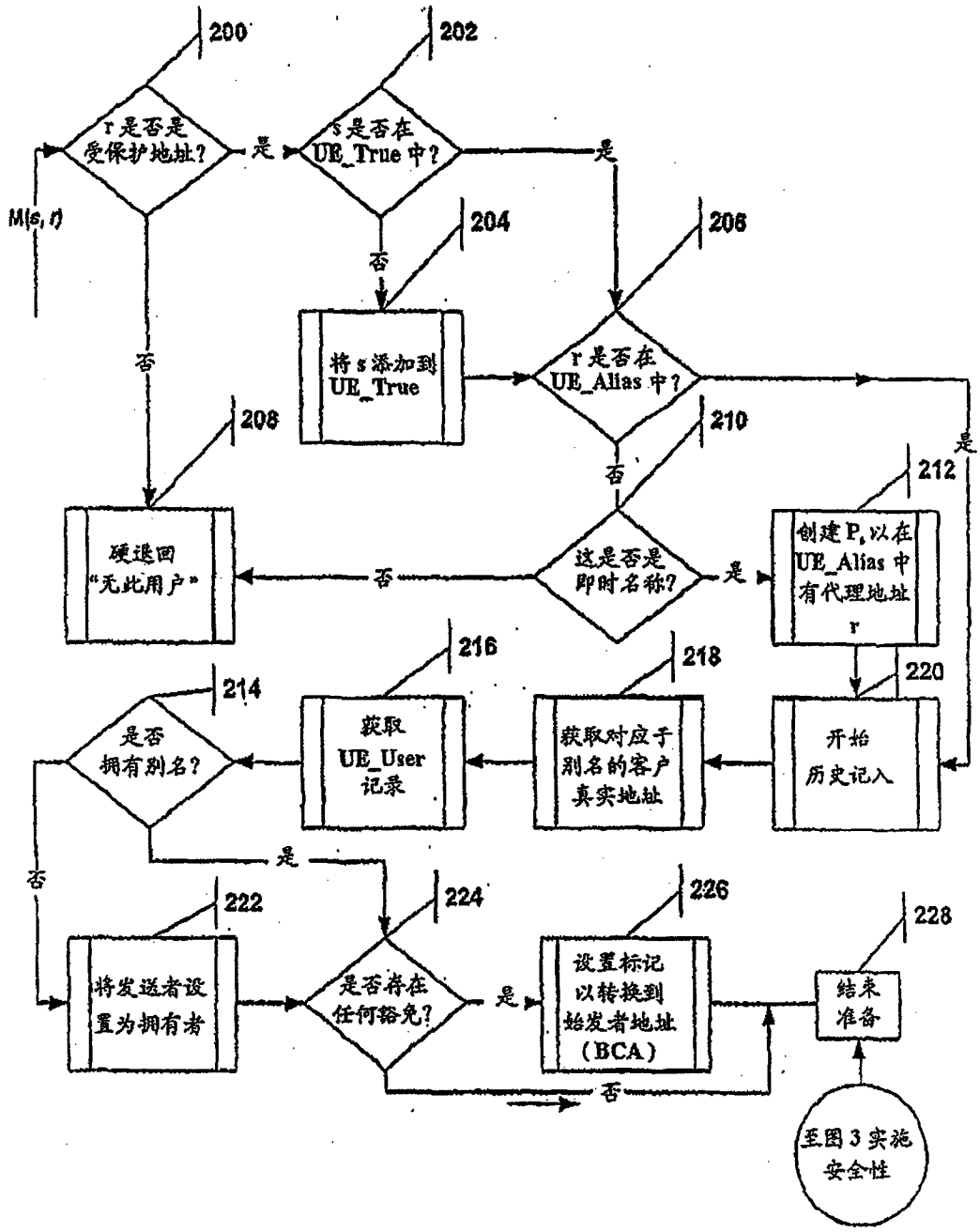
R_x = 有关从 s 发往 r 的消息的安全性状态

R_1 = 允许，继续处理消息

P_2 = 拒绝，不处理该消息

R_3 = 延迟，临时性地延迟返回发送服务器的消息

图 1



说明：s=发送者身份
r=接收者身份
M(s,r)= 从s发往r的消息
UE_TRUE是包含"真实"（即非代理）地址的数据库表
UE_ALIAS是包含代理地址的数据库表
UE_User是包含用户信息的数据库表
BCA= "名片地址"，内部邮件传输代理（即邮件服务器）管理的始发者地址
P_r是对于用户登记到s的代理地址的安全性设置，其中该用户拥有代理r替代的始发者地址

图2

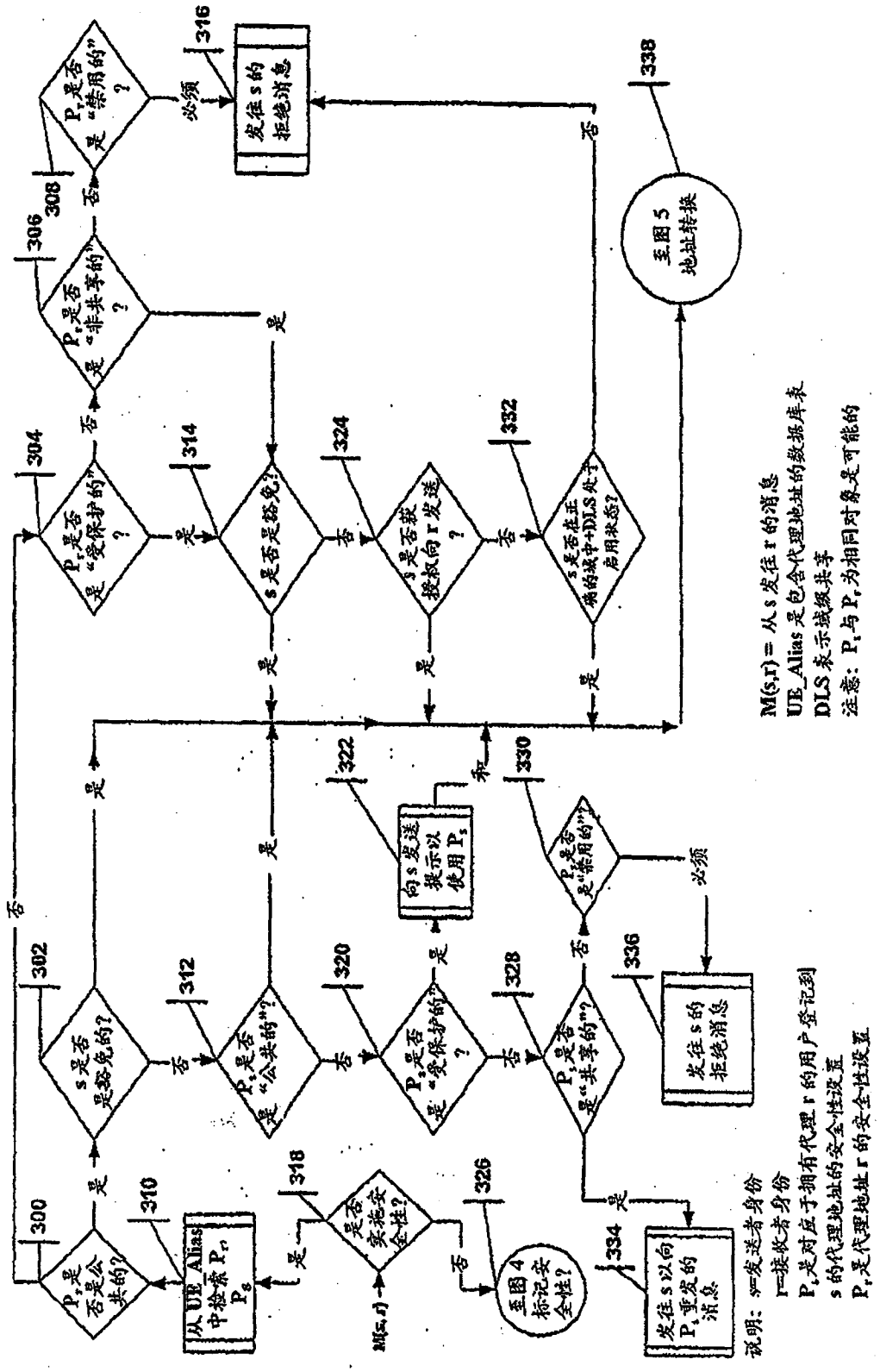

300
302
304
306
308
310
312
314
316
318
320
322
324
326
328
330
332
334
336
338
P1是否公共的?
s是否是豁免的?
P1是否受保护的?
P1是否“非共享的”?
P1是否“禁用的”?
从UE_Alias中检索P1,Ps
P1,是否是“公共的”?
P2是否受保护的?
P1是否是“共享的”?
是否实施安全性?
向s发送提示以使用Ps
s是否是豁免?
s是否在正确的域中+DLS处于启用状态?
s是否获授权向r发送?
P1是否“禁用的”?
发往s的拒绝消息
发往s的拒绝消息
发往s以向P1重发的消息
至图4标记安全性?
至图5地址排挨
是
否
必须
M(s,r)= 从s发往r的消息
UE_Alias是包含代理地址的数据库表
DLS表示域级共享
注意:P1与P1为相同对象是可能的
说明:s=发送者身份
r=接收者身份
P1是对应于拥有代理r的用户登记到s的代理地址的安全性设置
P1是代理地址r的安全性设置

图 3

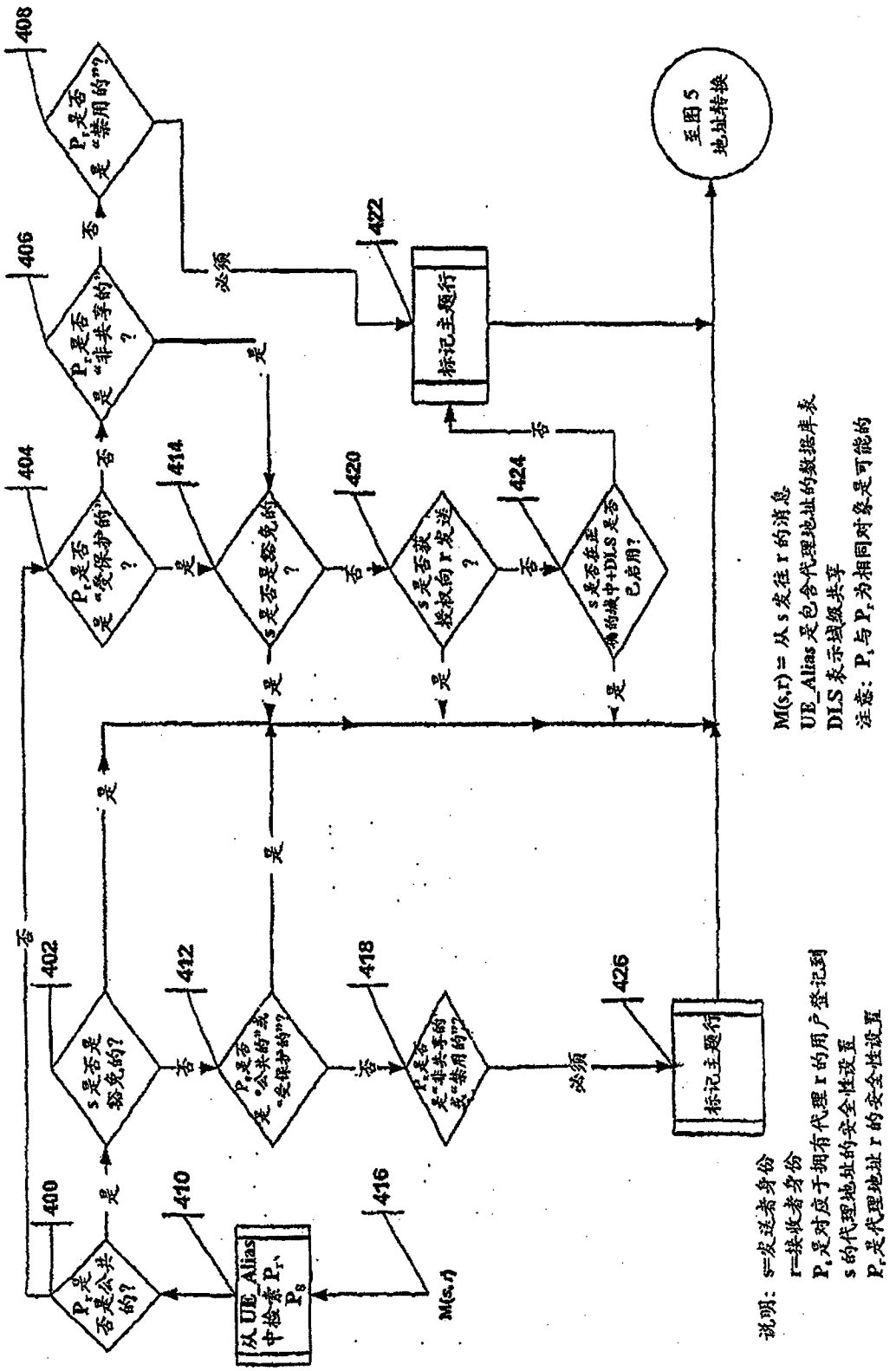

400
402
404
406
408
410
412
414
416
418
420
422
424
426
P_r是否是公共的?
s是否是豁免的?
P_r是否是"受保护的"?
P_r是否是"非共享的"?
P_r是否是"禁用的"?
从UE_Alias中检索P_r、P_s
P_r是否是"公共的"或"受保护的"?
s是否是豁免的?
s是否获授权向r发送?
s是否在正确的域中+DLS是否已启用?
P_r是否是"非共享的"或"禁用的"?
M(s,r)
标记主题行
标记主题行
必须
必须
是
否
至图5 地址转换
说明: s=发送者身份
r=接收者身份
P_s是对应于拥有代理r的用户登记到s的代理地址的安全性设置
P_r是代理地址r的安全性设置
M(s,r)=从s发往r的消息
UE_Alias是包含代理地址的数据库表
DLS表示域级共享
注意: P_r与P_s为相同对象是可能的

图4

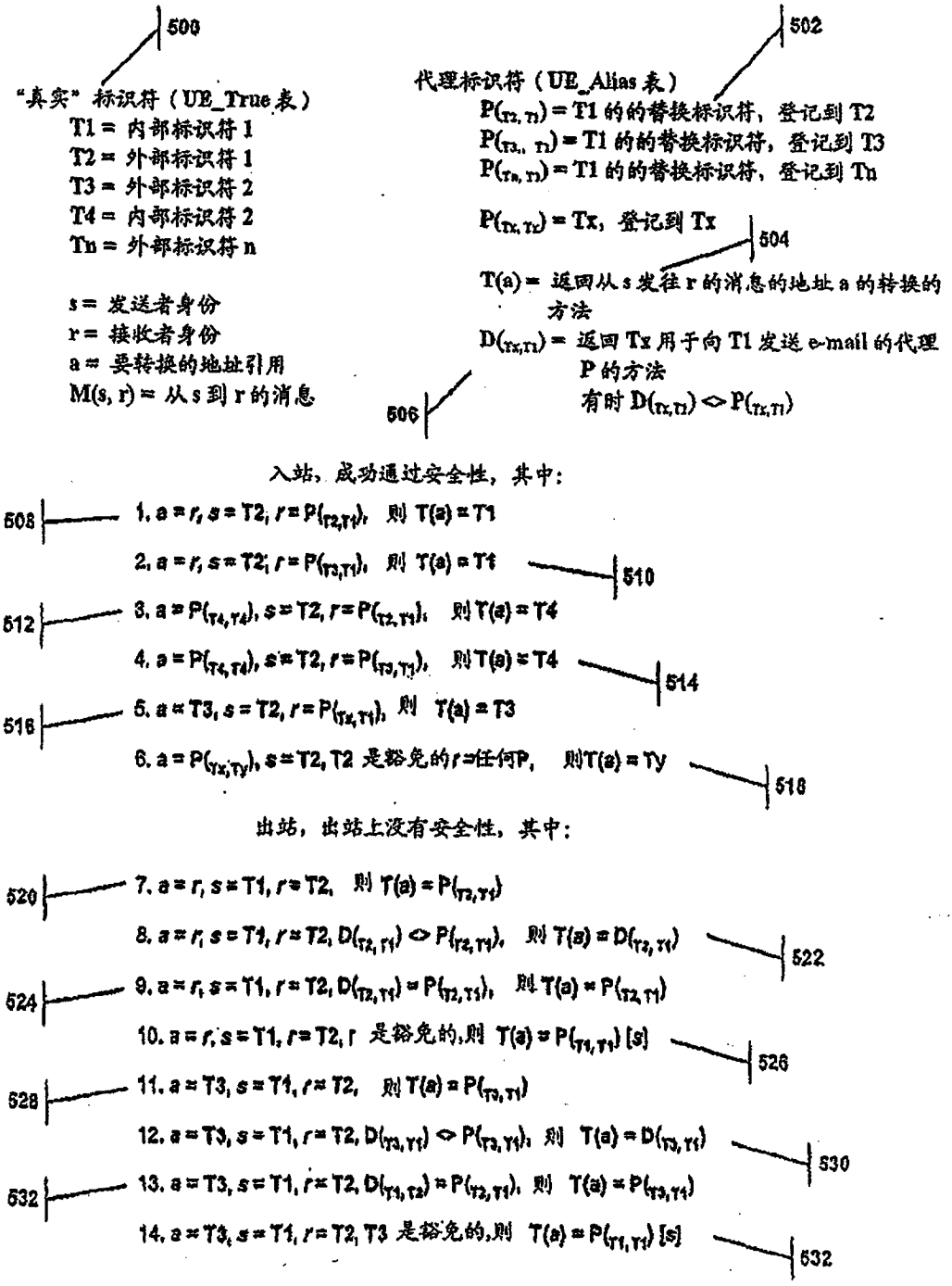

500
"真实"标识符（UE_True表）
T1 = 内部标识符 1
T2 = 外部标识符 1
T3 = 外部标识符 2
T4 = 内部标识符 2
Tn = 外部标识符 n
s = 发送者身份
r = 接收者身份
a = 要转换的地址引用
M(s, r) = 从 s 到 r 的消息
502
代理标识符（UE_Alias 表）
P(T2, T1) = T1 的的替换标识符，登记到 T2
P(T3, T1) = T1 的的替换标识符，登记到 T3
P(Tn, T1) = T1 的的替换标识符，登记到 Tn
P(Tx, Tx) = Tx，登记到 Tx
504
T(a) = 返回从 s 发往 r 的消息的地址 a 的转换的方法
D(Tx,T1) = 返回 Tx 用于向 T1 发送 e-mail 的代理 P 的方法
有时 D(Tx,T1) <> P(Tx,T1)
506
入站，成功通过安全性，其中：
508
1. a = r, s = T2, r = P(T2,T1)，则 T(a) = T1
2. a = r, s = T2, r = P(T3,T1)，则 T(a) = T1
510
512
3. a = P(T4,T4), s = T2, r = P(T2,T1)，则 T(a) = T4
4. a = P(T4,T4), s = T2, r = P(T3,T1)，则 T(a) = T4
514
516
5. a = T3, s = T2, r = P(Tx,T1)，则 T(a) = T3
6. a = P(Tx,Ty), s = T2, T2 是豁免的 r = 任何P，则T(a) = Ty
518
出站，出站上没有安全性，其中：
520
7. a = r, s = T1, r = T2，则 T(a) = P(T2,T1)
8. a = r, s = T1, r = T2, D(T2,T1) <> P(T2,T1)，则 T(a) = D(T2,T1)
522
524
9. a = r, s = T1, r = T2, D(T2,T1) = P(T2,T1)，则 T(a) = P(T2,T1)
10. a = r, s = T1, r = T2, r 是豁免的，则 T(a) = P(T1,T1)[s]
526
528
11. a = T3, s = T1, r = T2，则 T(a) = P(T3,T1)
12. a = T3, s = T1, r = T2, D(T3,T1) <> P(T3,T1)，则 T(a) = D(T3,T1)
530
532
13. a = T3, s = T1, r = T2, D(T1,T2) = P(T2,T1)，则 T(a) = P(T3,T1)
14. a = T3, s = T1, r = T2, T3 是豁免的，则 T(a) = P(T1,T1)[s]
532

图 5

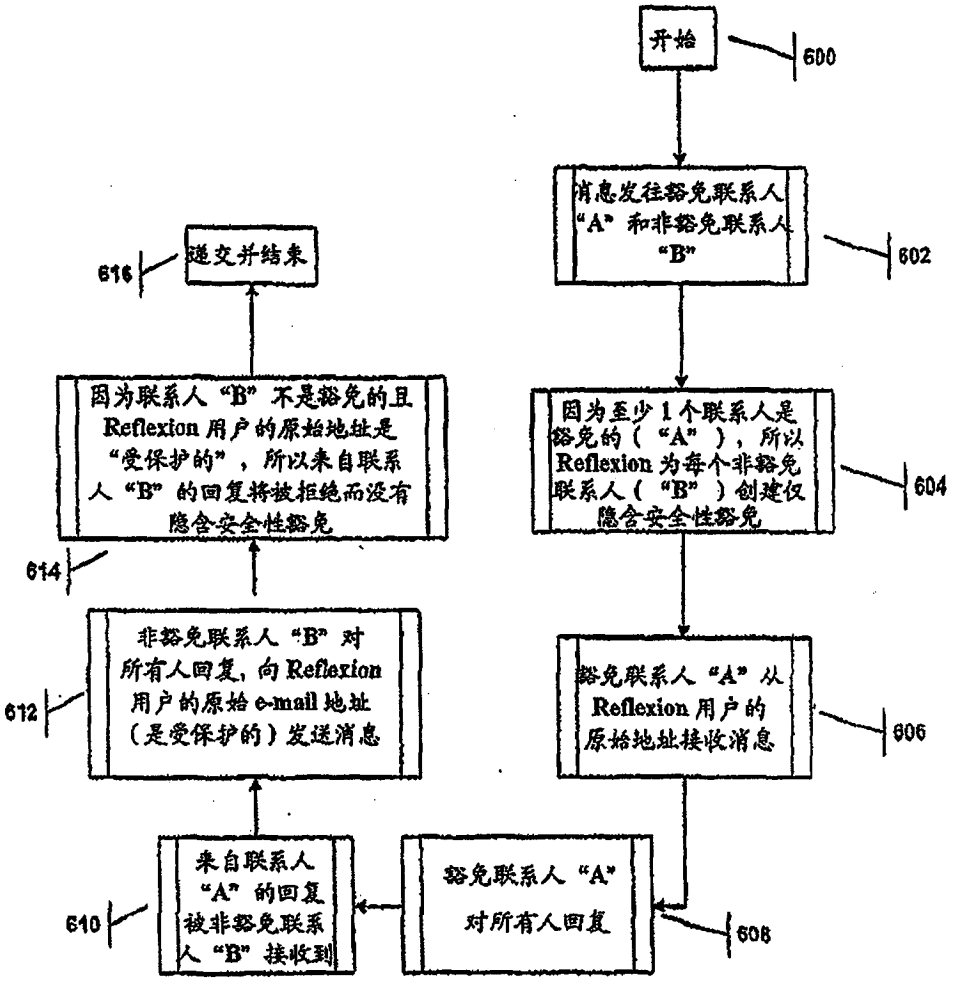

开始
600
消息发往豁免联系人“A”和非豁免联系人“B”
602
因为至少1个联系人是豁免的（“A”），所以Reflexion为每个非豁免联系人（“B”）创建仅隐含安全性豁免
604
豁免联系人“A”从Reflexion用户的原始地址接收消息
606
豁免联系人“A”对所有人回复
608
来自联系人“A”的回复被非豁免联系人“B”接收到
610
非豁免联系人“B”对所有人回复，向Reflexion用户的原始e-mail地址（是受保护的）发送消息
612
因为联系人“B”不是豁免的且Reflexion用户的原始地址是“受保护的”，所以来自联系人“B”的回复将被拒绝而没有隐含安全性豁免
614
递交并结束
616

图 6

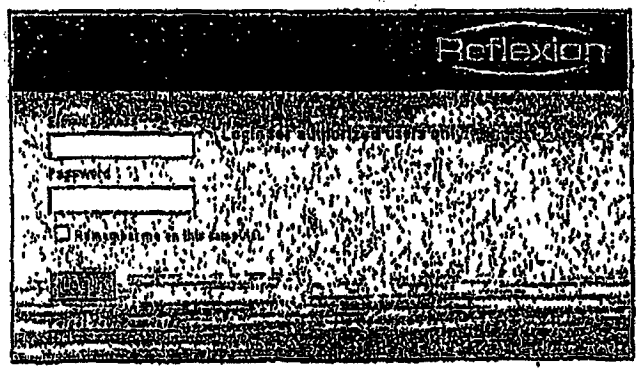

Reflexion

图 7

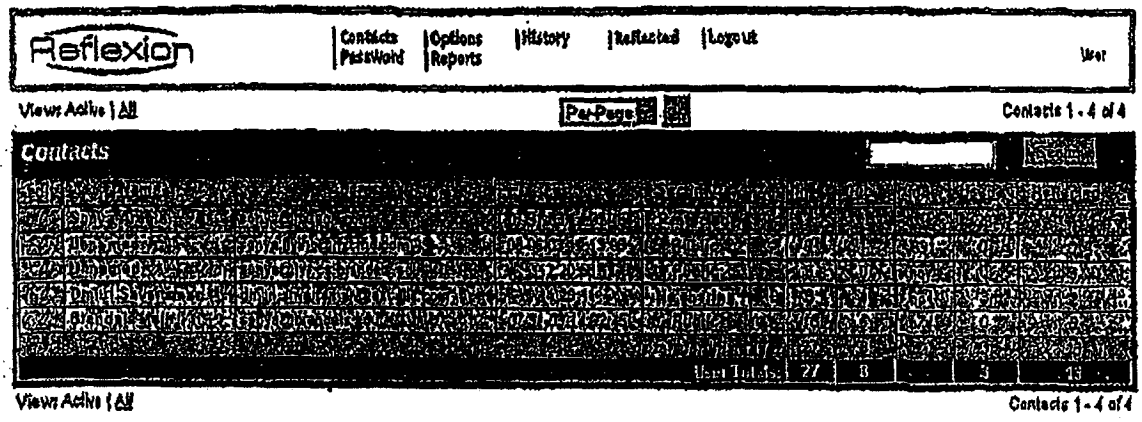

Reflexion
Contacts
Options
History
Logout
Contacts
Contacts 1 - 4 of 4
Views: Active | All

图 8

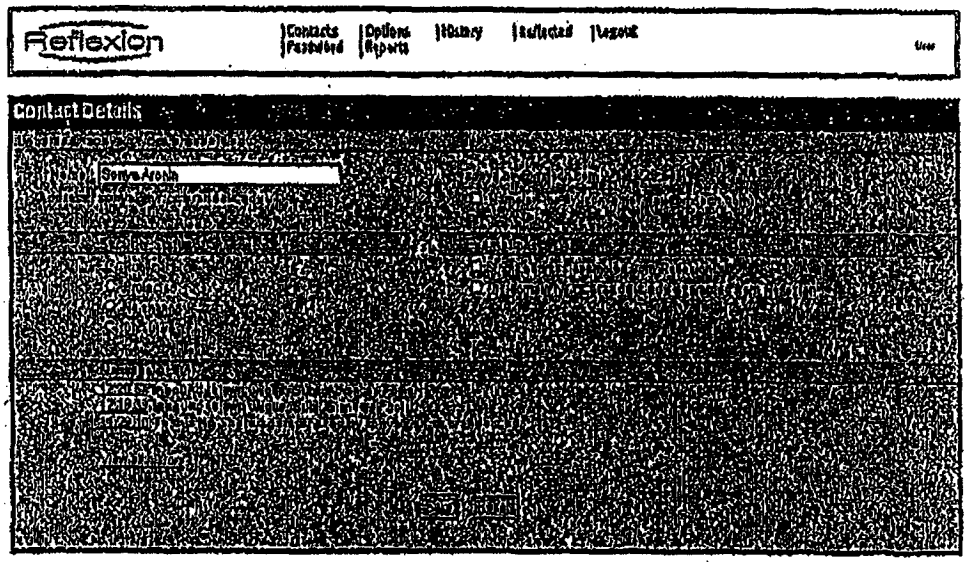

Reflexion
Contact Details

图 9

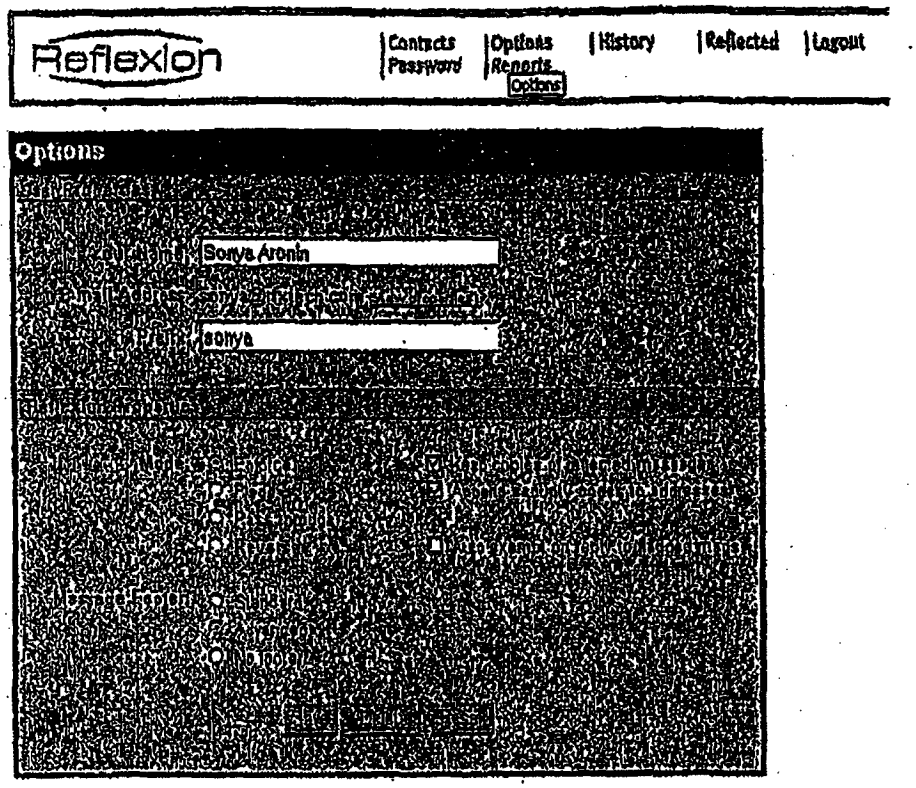

Reflexion
Contacts
Password
Options
Reports
History
Reflected
Logout
Options
Sonya Aronin
sonya

图 10

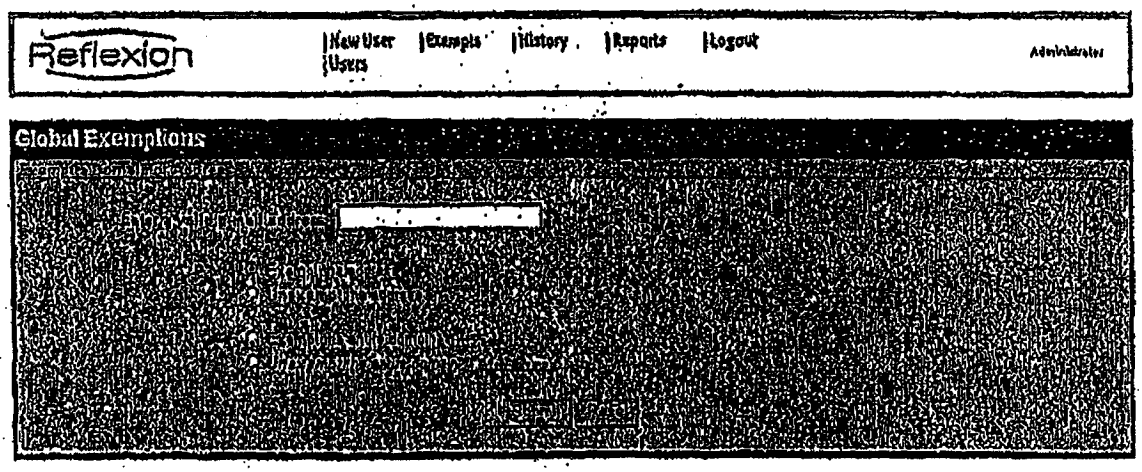

Reflexion
New User
Users
Exempts
History
Reports
Logout
Global Exemptions

图 11

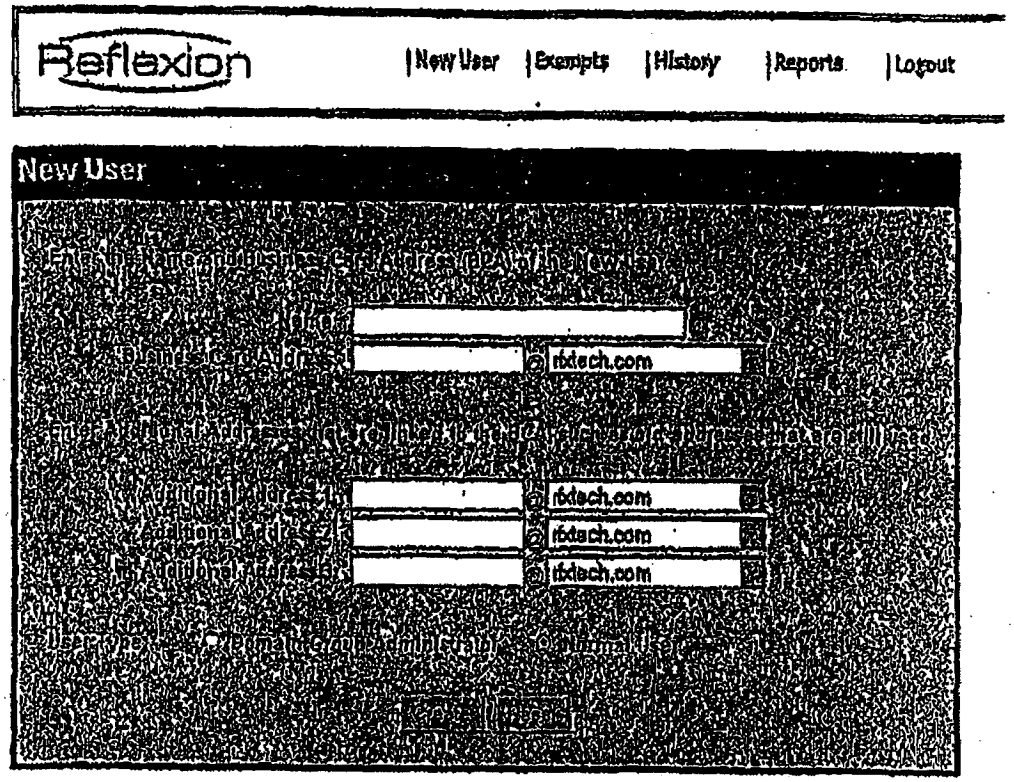

Reflexion
New User
Exempts
History
Reports
Logout
New User
rbtech.com
rbtech.com
rbtech.com
rbtech.com

图 12

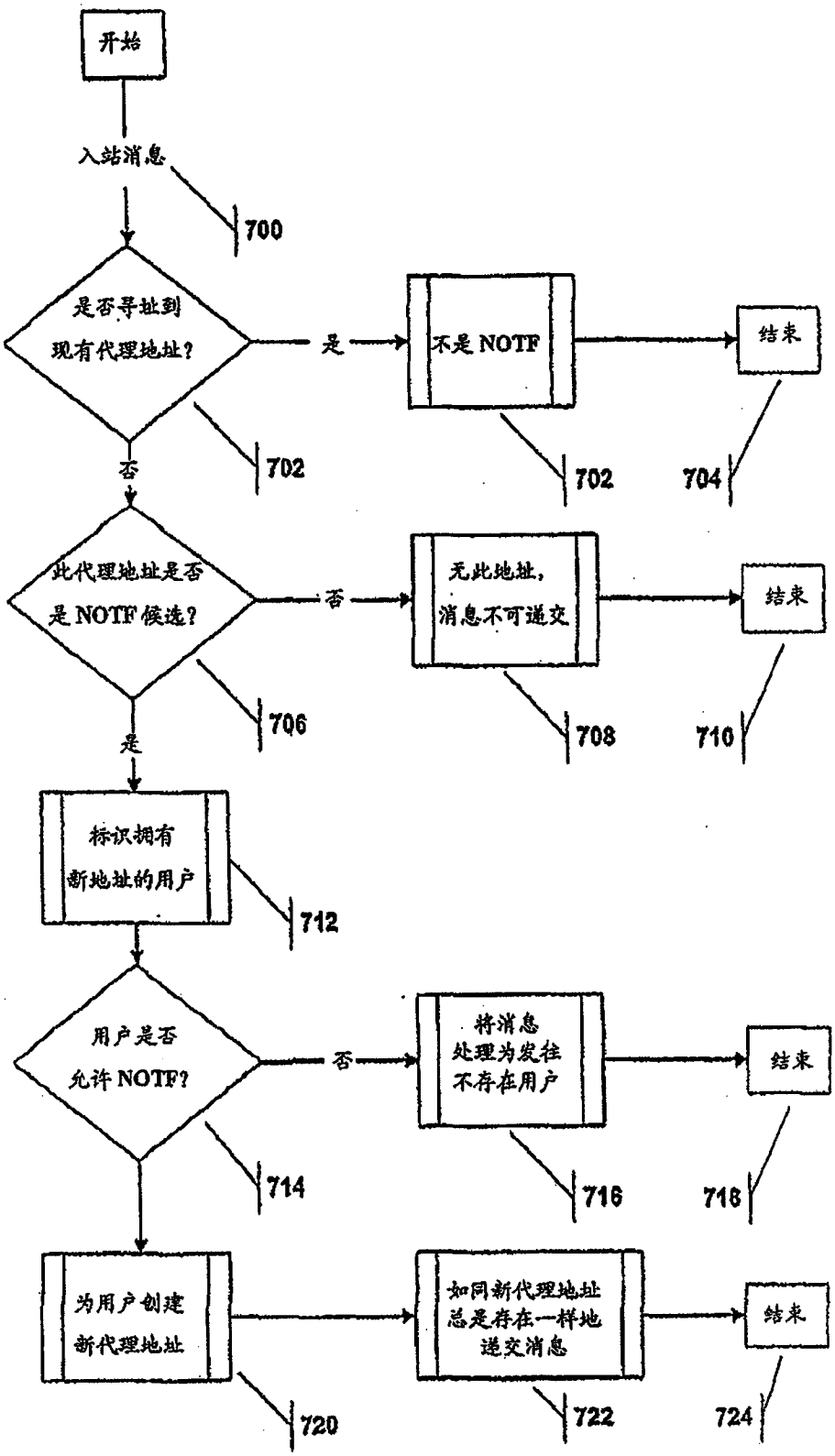

开始
入站消息
700
是否寻址到现有代理地址?
是
不是 NOTF
结束
702
702
704
否
此代理地址是否是 NOTF 候选?
否
无此地址，消息不可递交
结束
706
708
710
是
标识拥有新地址的用户
712
用户是否允许 NOTF?
否
将消息处理为发往不存在用户
结束
714
716
718
为用户创建新代理地址
如同新代理地址总是存在一样地递交消息
结束
720
722
724

图 13

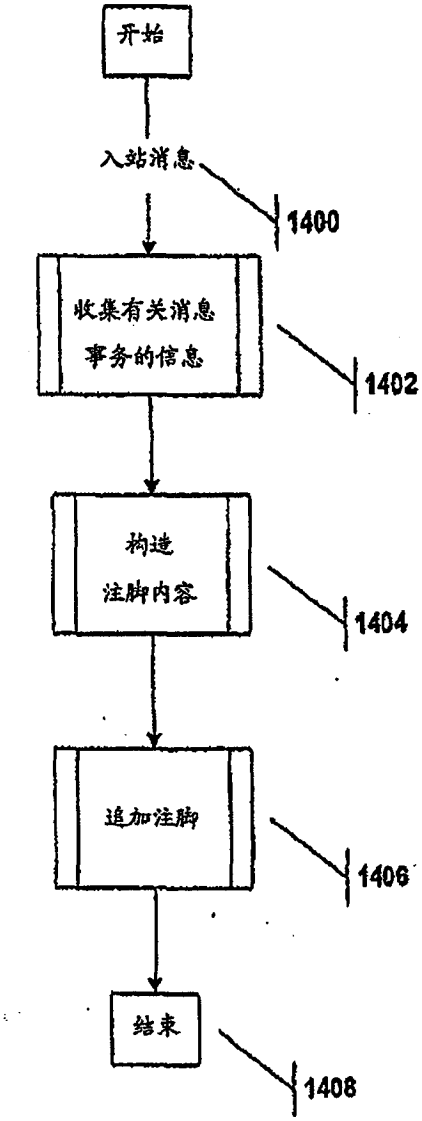

开始
入站消息
1400
收集有关消息事务的信息
1402
构造注脚内容
1404
追加注脚
1406
结束
1408

图 14

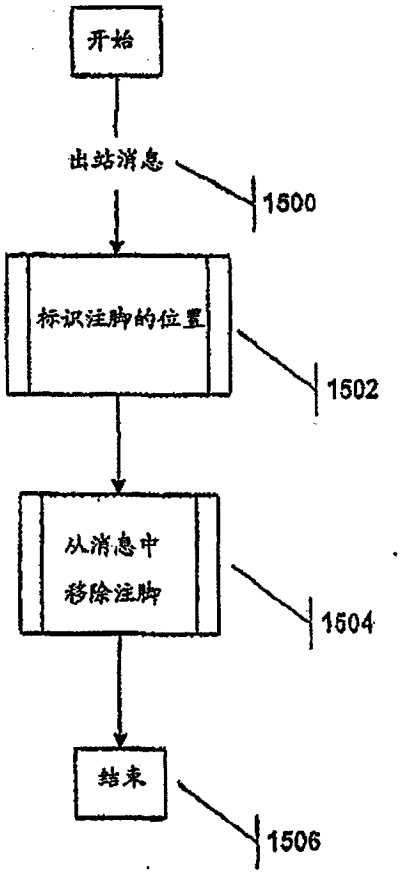

开始
出站消息
1500
标识注脚的位置
1502
从消息中移除注脚
1504
结束
1506

图 15

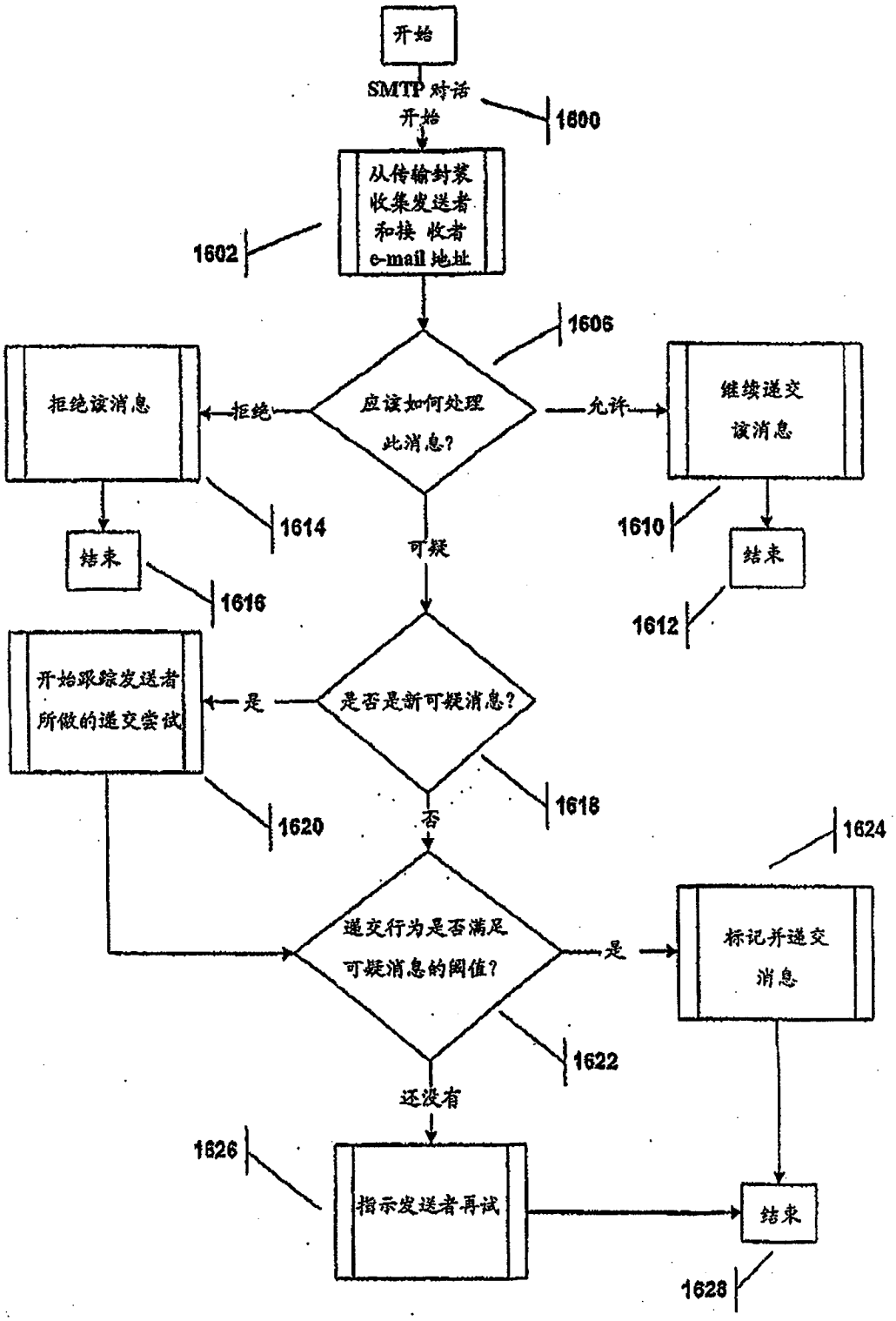

开始
SMTP 对话开始
1600
从传输封装收集发送者和接 收者 e-mail 地址
1602
1606
应该如何处理此消息?
拒绝
允许
拒绝该消息
继续递交该消息
1614
1610
结束
结束
1616
1612
可疑
是否是新可疑消息?
是
开始跟踪发送者所做的递交尝试
1618
1620
否
1624
递交行为是否满足可疑消息的阈值?
是
标记并递交消息
1622
还没有
1626
指示发送者再试
结束
1628

图 16

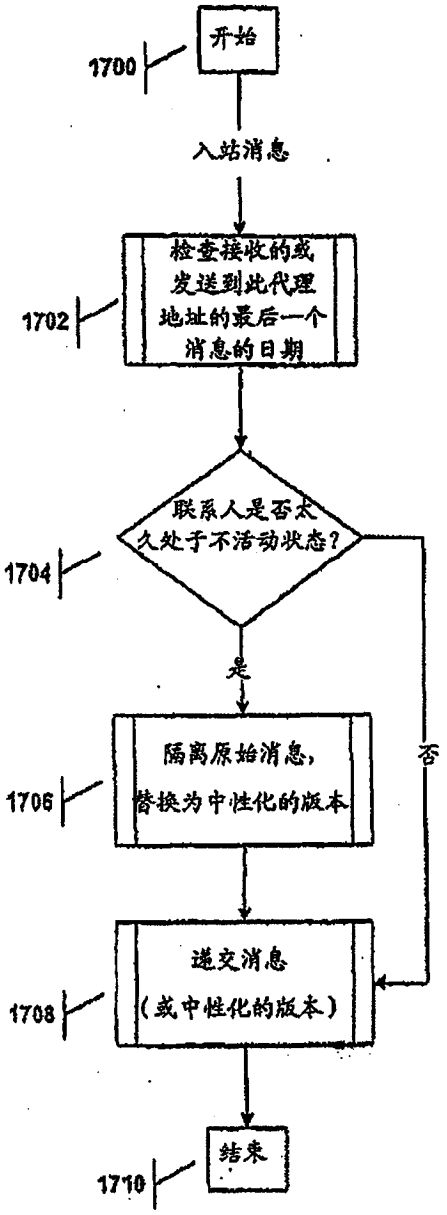

开始
1700
入站消息
检查接收的或发送到此代理地址的最后一个消息的日期
1702
联系人是否太久处于不活动状态？
1704
是
否
隔离原始消息，替换为中性化的版本
1706
递交消息（或中性化的版本）
1708
结束
1710

图 17

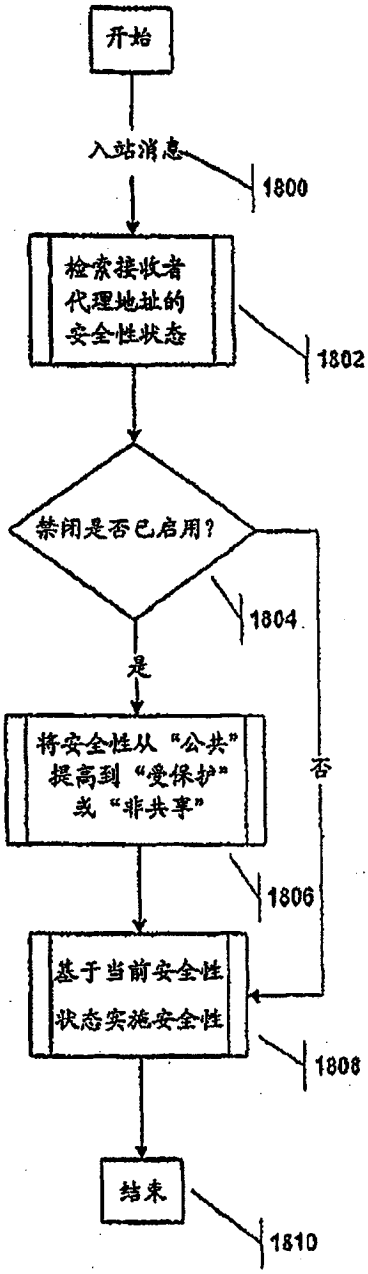

开始
入站消息
1800
检索接收者代理地址的安全性状态
1802
禁闭是否已启用？
1804
是
否
将安全性从“公共”提高到“受保护”或“非共享”
1806
基于当前安全性状态实施安全性
1808
结束
1810

图 18