



(12) 发明专利申请

(10) 申请公布号 CN 104106094 A

(43) 申请公布日 2014. 10. 15

(21) 申请号 201380004584. 3

(74) 专利代理机构 永新专利商标代理有限公司

(22) 申请日 2013. 07. 15

72002

代理人 张扬 王英

(30) 优先权数据

(51) Int. Cl.

61/672, 222 2012. 07. 16 US

G06Q 50/32(2006. 01)

13/683, 976 2012. 11. 21 US

(85) PCT国际申请进入国家阶段日

2014. 06. 27

(86) PCT国际申请的申请数据

PCT/US2013/050573 2013. 07. 15

(87) PCT国际申请的公布数据

W02014/014848 EN 2014. 01. 23

(71) 申请人 迈克菲公司

地址 美国加利福尼亚

(72) 发明人 N·利布曼 P·尼尔 M·G·毕晓普

J·克拉金 M·德里斯科尔

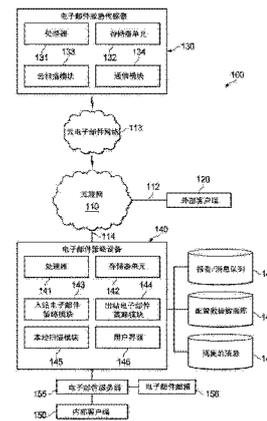
权利要求书4页 说明书21页 附图7页

(54) 发明名称

在网络环境下使用本地策略应用进行云电子邮件消息扫描

(57) 摘要

一种用于向电子邮件消息应用策略的方法包括:由受保护网络中的入站策略模块接收电子邮件消息的消息元数据。该方法还包括:基于该消息元数据,确定在受保护网络中接收该电子邮件消息是否被至少一个元数据策略禁止。该方法还包括:如果在受保护网络中接收该电子邮件消息被元数据策略禁止,则阻止将该电子邮件消息转发到受保护网络。在特定的实施例中,该方法包括:如果在受保护网络中接收该电子邮件消息未被一个或多个元数据策略禁止,则请求针对该电子邮件消息的扫描结果数据。在另外的实施例中,该方法包括:如果在受保护网络中接收该电子邮件消息未被一个或多个扫描策略禁止,则接收扫描结果数据,并请求该电子邮件消息。



CN 104106094 A

1. 至少一种机器可读存储介质,其具有存储在其上的用于向电子邮件消息应用策略的指令,当所述指令由处理器执行时,使得所述处理器执行以下操作:

由受保护网络中的进站策略模块接收电子邮件消息的消息元数据;

基于所述消息元数据,确定在所述受保护网络中接收所述电子邮件消息是否被一个或多个元数据策略中的至少一个元数据策略禁止;以及

如果在所述受保护网络中接收所述电子邮件消息被所述至少一个元数据策略禁止,则阻止将所述电子邮件消息转发到所述受保护网络。

2. 根据权利要求 1 所述的至少一种机器可读存储介质,还包括当由所述处理器执行时,使得所述处理器执行以下操作的指令:

向云网络中的电子邮件威胁传感器发送响应码,以阻止将所述电子邮件消息转发到所述受保护网络,其中,所述电子邮件威胁传感器从另一个网络中的发送客户端接收到所述电子邮件消息。

3. 根据权利要求 1 所述的至少一种机器可读存储介质,还包括当由所述处理器执行时,使得所述处理器执行以下操作的指令:

如果在所述受保护网络中接收所述电子邮件消息未被所述一个或多个元数据策略禁止,则请求针对所述电子邮件消息的扫描结果数据。

4. 根据权利要求 3 所述的至少一种机器可读存储介质,还包括当由所述处理器执行时,使得所述处理器执行以下操作的指令:

由所述受保护网络中的所述进站策略模块接收所述扫描结果数据;

基于所述扫描结果数据,确定在所述受保护网络中接收所述电子邮件消息是否被一个或多个扫描策略中的至少一个扫描策略禁止;以及

如果在所述受保护网络中接收所述电子邮件消息被所述至少一个扫描策略禁止,则阻止将所述电子邮件消息转发到所述受保护网络。

5. 根据权利要求 4 所述的至少一种机器可读存储介质,还包括当由所述处理器执行时,使得所述处理器执行以下操作的指令:

如果在所述受保护网络中接收所述电子邮件消息未被所述一个或多个扫描策略禁止,则请求所述电子邮件消息。

6. 根据权利要求 1、3、4 和 5 中的任一项权利要求所述的至少一种机器可读存储介质,还包括当由所述处理器执行时,使得所述处理器执行以下操作的指令:

当所述电子邮件消息被请求时,由所述受保护网络中的所述进站策略模块接收所述电子邮件消息;以及

将所述电子邮件消息转发到所述受保护网络中的邮件服务器,其中,所述邮件服务器将所述电子邮件消息传送给所述电子邮件消息的预期接收方。

7. 根据权利要求 1、3、4 和 5 中的任一项权利要求所述的至少一种机器可读存储介质,还包括当由所述处理器执行时,使得所述处理器执行以下操作的指令:

当所述电子邮件消息被请求时,由所述受保护网络中的所述进站策略模块接收所述电子邮件消息;

针对被一个或多个本地扫描策略所禁止的内容,对所接收的电子邮件消息进行扫描;以及

响应于在所述扫描期间发现至少一些禁止的内容,对所述电子邮件消息进行隔离。

8. 根据权利要求 1、3、4 和 5 中的任一项权利要求所述的至少一种机器可读存储介质,还包括当由所述处理器执行时,使得所述处理器执行以下操作的指令:

当所述电子邮件消息被请求时,由所述受保护网络中的所述进站策略模块接收所述电子邮件消息;

针对被一个或多个本地扫描策略所禁止的内容,对所接收的电子邮件消息进行扫描;以及

响应于在所述扫描期间发现至少一些禁止的内容,阻止将所述电子邮件消息传送给所述电子邮件消息的预期接收方。

9. 根据权利要求 8 所述的至少一种机器可读存储介质,还包括当由所述处理器执行时,使得所述处理器执行以下操作的指令:

响应于在所述扫描期间没有发现任何禁止的内容,将所述电子邮件消息转发给所述受保护网络中的邮件服务器,其中,所述邮件服务器配置为:将所述电子邮件消息传送给所述电子邮件消息的预期接收方。

10. 一种用于向电子邮件消息应用策略的方法,包括:

由受保护网络中的进站策略模块接收电子邮件消息的消息元数据;

基于所述消息元数据,确定在所述受保护网络中接收所述电子邮件消息是否被一个或多个元数据策略中的至少一个元数据策略禁止;以及

如果在所述受保护网络中接收所述电子邮件消息被所述至少一个元数据策略禁止,则阻止将所述电子邮件消息转发到所述受保护网络。

11. 根据权利要求 10 所述的方法,还包括:

如果在所述受保护网络中接收所述电子邮件消息未被所述一个或多个元数据策略禁止,则请求针对所述电子邮件消息的扫描结果数据。

12. 根据权利要求 11 所述的方法,还包括:

由所述受保护网络中的所述进站策略模块接收所述扫描结果数据;

基于所述扫描结果数据,确定在所述受保护网络中接收所述电子邮件消息是否被一个或多个扫描策略中的至少一个扫描策略禁止;以及

如果在所述受保护网络中接收所述电子邮件消息被所述至少一个扫描策略禁止,则阻止将所述电子邮件消息转发到所述受保护网络。

13. 根据权利要求 12 所述的方法,还包括:

如果在所述受保护网络中接收所述电子邮件消息未被所述一个或多个扫描策略禁止,则请求所述电子邮件消息。

14. 一种用于向电子邮件消息应用策略的装置,包括:

受保护网络中的处理器;以及

在所述处理器上执行的进站策略模块,所述进站策略模块配置为:

接收电子邮件消息的消息元数据;

基于所述消息元数据,确定在所述受保护网络中接收所述电子邮件消息是否被一个或多个元数据策略中的至少一个元数据策略禁止;以及

如果在所述受保护网络中接收所述电子邮件消息被所述至少一个元数据策略禁止,则

阻止将所述电子邮件消息转发到所述受保护网络。

15. 根据权利要求 14 所述的装置,其中,所述进站策略模块还配置为:

向云网络中的电子邮件威胁传感器发送响应码,以阻止将所述电子邮件消息转发到所述受保护网络,其中,所述电子邮件威胁传感器从另一个网络中的发送客户端接收到所述电子邮件消息。

16. 根据权利要求 14 所述的装置,其中,所述进站策略模块还配置为:

如果在所述受保护网络中接收所述电子邮件消息未被所述一个或多个元数据策略禁止,则请求针对所述电子邮件消息的扫描结果数据。

17. 根据权利要求 16 所述的装置,其中,所述进站策略模块还配置为:

接收所述扫描结果数据;

基于所述扫描结果数据,确定在所述受保护网络中接收所述电子邮件消息是否被一个或多个扫描策略中的至少一个扫描策略禁止;以及

如果在所述受保护网络中接收所述电子邮件消息被所述至少一个扫描策略禁止,则阻止将所述电子邮件消息转发到所述受保护网络。

18. 根据权利要求 17 所述的装置,其中,所述进站策略模块还配置为:

如果在所述受保护网络中接收所述电子邮件消息未被所述一个或多个扫描策略禁止,则请求所述电子邮件消息。

19. 根据权利要求 14、16、17 和 18 中的任一项权利要求所述的装置,其中,所述进站策略模块还配置为:

当所述电子邮件消息被请求时,接收所述电子邮件消息;以及

将所述电子邮件消息转发到所述受保护网络中的邮件服务器,其中,所述邮件服务器将所述电子邮件消息传送给所述电子邮件消息的预期接收方。

20. 根据权利要求 14、16、17 和 18 中的任一项权利要求所述的装置,其中,所述进站策略模块还配置为:

当所述电子邮件消息被请求时,接收所述电子邮件消息;

针对被本地扫描策略所禁止的内容,对所接收的电子邮件消息进行扫描;以及

响应于在扫描所述电子邮件消息时发现至少一些禁止的内容,对所述电子邮件消息进行隔离。

21. 根据权利要求 14、16、17 和 18 中的任一项权利要求所述的装置,其中,所述进站策略模块还配置为:

当所述电子邮件消息被请求时,接收所述电子邮件消息;

针对被本地扫描策略所禁止的内容,对所接收的电子邮件消息进行扫描;以及

响应于在所述扫描期间发现至少一些禁止的内容,阻止将所述电子邮件消息传送给所述电子邮件消息的预期接收方。

22. 根据权利要求 21 所述的装置,其中,所述进站策略模块还配置为:

响应于在所述扫描期间没有发现任何禁止的内容,将所述电子邮件消息转发给所述受保护网络中的邮件服务器,其中,所述邮件服务器配置为:将所述电子邮件消息传送给所述电子邮件消息的预期接收方。

23. 至少一种机器可读存储介质,其具有存储在其上的用于向电子邮件消息应用策略

的指令,当所述指令由处理器执行时,使得所述处理器执行以下操作:

接收具有接收方电子邮件地址的电子邮件消息,所述接收方电子邮件地址标识受保护网络中的预期接收方;

向所述受保护网络中的进站邮件策略模块发送所述电子邮件消息的消息元数据;以及

如果在所述受保护网络中接收所述电子邮件消息被一个或多个元数据策略中的至少一个元数据策略禁止,则阻止将所述电子邮件消息转发到所述受保护网络。

24. 根据权利要求 28 所述的至少一种机器可读存储介质,还包括当由所述处理器执行时,使得所述处理器执行以下操作的指令:

针对一个或多个威胁,对所述电子邮件消息进行扫描;以及

如果在所述受保护网络中接收所述电子邮件消息未被所述一个或多个元数据策略禁止,则向所述受保护网络中的所述进站邮件策略模块发送扫描结果数据。

25. 根据权利要求 23 和 24 中的任一项权利要求所述的至少一种机器可读存储介质,还包括当由所述处理器执行时,使得所述处理器执行以下操作的指令:

如果在所述受保护网络中接收所述电子邮件消息未被所述一个或多个扫描策略禁止,则向所述受保护网络中的所述进站邮件策略模块发送所述电子邮件消息。

在网络环境下使用本地策略应用进行云电子邮件消息扫描

[0001] 相关申请

[0002] 本申请根据 35U. S. C. § 119(e), 要求享受由 Nicholas Liebmann 等人于 2012 年 7 月 16 日提交的、题目为“MECHANISM FOR CLOUD EMAIL SCANNING WITH GATEWAY POLICY APPLICATION”的美国临时申请 No. 61/672, 222 的优先权的权益。

技术领域

[0003] 概括地说, 本发明涉及信息安全领域, 更具体地说, 涉及在网络环境下使用本地策略应用进行云电子邮件消息扫描。

背景技术

[0004] 网络安全领域在今日社会变得越来越重要。互联网实现了世界各地的不同计算机网络的互联。具体而言, 互联网提供了用于通过各种类型的客户端设备, 在连接到不同的计算机网络的不同用户之间交换电子邮件(email)的媒介。虽然 email 的使用改变了企业和个人通信, 但其同时也被恶意操作者使用成用于获得对于计算机和计算机网络的未授权访问, 以及敏感信息的有意或无意泄露的媒介物。

[0005] 感染主机的恶意软件 (“malware”) 能够执行任意数量的恶意动作, 例如, 从该主机发送出垃圾邮件或者恶意的电子邮件, 从与该主机关联的企业或者个人盗取敏感信息, 传播给其它主机, 和 / 或帮助分布式拒绝服务攻击, 举例而言。一些组织机构通常使用某种类型的电子邮件保护设备来过滤潜在有害邮件, 保护它们的计算机网络免受入站邮件威胁。云服务可以提供入站邮件过滤 (例如, 垃圾邮件、恶意软件), 帮助节省网络的带宽。但是, 通常使用其它机制来监测出站邮件, 以防止敏感信息或者机密信息的丢失。因此, 为了保护计算机和计算机网络免受通过入站和出站邮件而进行的恶意和无意利用, 仍然存在显著的管理挑战。

附图说明

[0006] 为了提供本发明以及其特征和优点的更完整理解, 可结合附图来参考下面的描述, 其中相同的附图标记表示相同的部件, 其中:

[0007] 图 1 是根据本发明的一个实施例, 用于在网络环境下进行云电子邮件消息扫描和本地策略应用的通信系统的简化框图;

[0008] 图 2 是示出根据一个实施例, 与电子邮件威胁传感器和电子邮件策略设备相关联的潜在操作的简化交互图;

[0009] 图 3 是示出根据一个实施例, 与通信系统相关联的潜在操作的简化流程图;

[0010] 图 4A 和图 4B 示出了根据一个实施例, 用于示出与通信系统相关联的其它潜在操作的简化流程图;

[0011] 图 5 是示出根据一个实施例, 以点对点配置进行布置的示例性计算系统的框图;

[0012] 图 6 是示出根据一个实施例的示例性处理器内核的框图。

具体实施方式

[0013] 示例性实施例

[0014] 图 1 是用于在网络环境下进行云电子邮件消息扫描和本地策略应用的通信系统 100 的简化框图。云电子邮件网络 113 中的电子邮件威胁传感器 130 和受保护网络 114 中的电子邮件策略设备 140 可以分别提供云电子邮件消息扫描和本地策略应用。此外,图 1 还提供了外部网络 112 中的外部客户端 120、受保护网络 114 中的邮件服务器 155 和内部客户端 150、以及互联网 110。互联网 110 有助于外部网络 112、云电子邮件网络 113 和受保护网络 114 的网络节点之间的网络通信,其包括电子邮件消息交换。电子邮件威胁传感器 130 可以包括处理器 131、存储器单元 132、云扫描模块 133 和通信模块 134。电子邮件策略设备 140 可以包括处理器 141、存储器单元 142、进站邮件策略模块 143、出站邮件策略模块 144、本地扫描模块 145 和用户界面 146。此外,在图 1 中还提供了用于报告和 / 或消息队列 147、配置数据数据库 148 和隔离的消息 149 的存储单元。这些存储单元可以与电子邮件策略设备 140 集成在一起,也可以由电子邮件策略设备 140 进行电子访问。

[0015] 图 1 的模块可以通过使用任何适当的连接(有线或无线)的一个或多个接口,来彼此相耦接,其中这些连接为网络通信提供可行的途径。另外,可以基于具体的配置需求,对图 1 的这些单元中的任何一个或多个进行组合,或者从该体系结构中删除这些单元中的任何一个或多个。通信系统 100 可以包括:能够传输控制协议 / 互联网协议(TCP/IP)通信,以便在网络中传输或者接收分组的配置。此外,通信系统 100 还可以结合用户数据报协议 / IP(UDP/IP) 或者任何其它适当的协议(根据需求和基于具体的需求)来操作。

[0016] 在示例性实施例中,通信系统 100 实现电子邮件消息的云扫描和在受保护网络中的本地策略应用,以便对电子邮件消息进行阻止、隔离、允许或者重新路由。在一个示例中,从外部客户端 120 到受保护网络 114 中的预期接收方的电子邮件消息,可以路由到云电子邮件网络 113 中的电子邮件威胁传感器 130。电子邮件威胁传感器 130 可以针对威胁对该电子邮件消息进行扫描,与电子邮件策略设备 140 进行通信。电子邮件策略设备可以向消息元数据应用本地策略,扫描结果数据以确定是否应当阻止该电子邮件消息到达受保护网络。如果元数据和扫描策略并不禁止在受保护网络中接收该电子邮件消息,则电子邮件策略设备 140 可以接收该电子邮件消息,可以针对被本地扫描策略所禁止的内容,对该电子邮件消息进行扫描,并相应地对该电子邮件消息进行阻止、允许、隔离或者重新路由。

[0017] 为了便于示出通信系统 100 的某些示例性技术,重要的是理解这些通信可以穿越网络环境。可以将下面的基本信息视作为能适当地解释本公开内容的基础。

[0018] 来自进站和出站电子邮件的威胁可能扰乱计算机网络,导致不稳定和 / 或不安全的系统。例如,进站电子邮件可以包含、生成、调用、响应于恶意软件或者与恶意软件相关联,其中该恶意软件可能感染接收客户端和 / 或主机,并潜在地传播给计算机网络中的其它网络单元和客户端。如本申请所使用的,‘威胁’包括恶意软件(malware),其通常是用于描述被设计为在计算机上参与敌对行为和 / 或不必要的行为的广义术语,通常包括被设计为干扰计算机或者网络的正常操作、获得对于计算机系统的未授权访问、和 / 或破坏、泄露或者修改数据的任何软件。恶意软件的示例可以包括,但不限于:病毒、垃圾软件、网络钓鱼诈骗、拒绝服务(DOS)攻击、帐号搜集、僵尸网络、间谍软件、广告、木马和蠕虫。此外,威胁

还可以包括：不遵循网络策略的电子邮件，和 / 或包含敏感信息和 / 或机密信息，但未被授权传输该信息的电子邮件。

[0019] 为了防止从入站电子邮件到受保护网络的威胁，可以在去往互联网的网关处，在受保护网络中布置电子邮件保护设备，或者也可以放置在别处来接收入站电子邮件。电子邮件保护设备可以提供针对电子邮件的病毒扫描，过滤出包含恶意软件或者其它不期望的内容（例如，粗俗的语言、淫秽物品等）的电子邮件，或者从恶意软件生成的其它电子邮件或者与恶意软件相关联的其它电子邮件。在该场景中，在受保护网络中接收具有该受保护网络中的目的地址的每一封电子邮件，以便对其进行扫描。通常，恶意软件扫描涉及对消息进行分解和扫描。因此，电子邮件可能消耗网络的大量带宽。此外，如果网络接收所有电子邮件来对它们进行扫描，可能不能防止拒绝服务攻击。

[0020] 用于保护网络免受入站电子邮件的威胁的另一种技术，涉及云电子邮件服务。通常，将云服务规定成对于作为网络（例如，互联网）上的服务来传输的计算资源的使用。通常，在云基础架构中提供有计算、存储和网络资源，有效地将工作负载从本地网络转移到云网络上。特定的网络所使用的云电子邮件服务可以包括：接收针对该特定网络的入站电子邮件，针对潜在威胁对这些电子邮件进行扫描，过滤与恶意软件相关联的电子邮件或者包含其它不期望的内容的电子邮件（例如，基于病毒扫描、垃圾软件扫描和 / 或其它参照标准），将未被过滤的电子邮件转发到该网络中。相应地，云电子邮件服务可以应用目的网络的策略，以过滤包含某些恶意软件和 / 或其它不期望的内容的电子邮件。

[0021] 为了应用特定于网络的策略，以便在云网络中针对特定的受保护网络来过滤电子邮件消息，将该受保护网络的特定于网络的配置提供给云。在一些实现中，受保护网络的网络管理员可以访问该云服务，以便增加和 / 或更新他们的特定于网络的配置。在其它实现中，网络管理员可以本地地增加和 / 或更新他们的特定于网络的配置，随后将这些配置推送到云。云服务通常是地理分散的，甚至可能分布在全球范围内。因此，在对所有云站点中的特定于网络的配置进行更新时，会发生延迟。因此，一些云电子邮件服务可能没有与相同的特定于网络的配置同步（当对这些配置进行了更新时）。

[0022] 虽然云电子邮件服务可以为进入给定的网络的入站电子邮件提供威胁保护，同时节省该网络的带宽，但仍然需要本地解决方案来防止机密信息或者敏感信息，在没有适当的授权的情况下离开本网络。例如，可以通过内部部署的装置（或者其它适当的网络单元），来传送来自于该网络的出站邮件，其中该应用可以执行合规性和数据丢失防护扫描。当不同的系统提供特定于入站的电子邮件保护和特定于出站的电子邮件保护，这些保护通常通过单独的用户界面来维护和管理。因此，单独的用户配置、报告、消息队列和消息隔离可以通过这些多个不同的系统来提供，其导致网络管理员产生繁重的管理任务。

[0023] 如图 1 中所概述的，用于网络环境下的云电子邮件扫描和本地策略应用的通信系统，可以解决这些问题（和其它问题）。在图 1 的通信系统 100 中，一种混合解决方案使云电子邮件服务和受保护网络的策略对进入受保护网络的入站电子邮件消息进行扫描，以便在该网络中进行本地地评估，该网络的电子邮件策略设备对该电子邮件消息应用策略。离开该网络的出站电子邮件消息在离开该网络之前，在电子邮件策略设备处进行过滤。通信系统 100 应用策略和实时地报告威胁检测，而无需在不同于电子邮件策略设备的位置（其可以是内部部署的设备）存储用户配置。是否在受保护网络中接收该电子邮件消息，取决

于用户配置。如果不需要该电子邮件消息数据来执行任何动作,则电子邮件策略设备可以拒绝该电子邮件消息。具体而言,在将电子邮件消息传送到受保护网络之前,电子邮件策略设备可以基于消息元数据中的信息或者来自于云电子邮件服务的扫描结果数据,对包含威胁的电子邮件消息进行阻止。因此,可以节省受保护网络的带宽。另外,受保护网络中的电子邮件策略设备可以提供集中管理,其包括配置、管理、报告和隔离。获授权用户可以通过单一用户界面,管理云电子邮件服务和内部部署的电子邮件策略设备,其中该单一用户界面可以是通过电子邮件策略设备来提供的。

[0024] 转到图 1 的基础架构,其示出了根据一个示例性实施例的通信系统 100。通常,可以在任何类型或者拓扑的网络中实现通信系统 100。受保护网络 114、互联网 110、云电子邮件网络 113 和外部网络 112 中的每一个,都表示用于接收和发送通过通信系统 100 传播的信息分组的互连通信路径的一系列点或者节点。这些网络提供节点之间的通信接口,其可以配置成任何局域网 (LAN)、虚拟局域网 (VLAN)、广域网 (WAN)、无线局域网 (WLAN)、城域网 (MAN)、内联网、外联网、虚拟专用网 (VPN)、以及有助于在网络环境下通信的任何其它适当的体系结构或者系统、或者其任意组合 (包括有线和 / 或无线通信)。

[0025] 在通信系统 100 中,可以根据任何适当的通信消息协议,来发送和接收包括分组、帧、信号、数据等的网络业务。适当的通信消息协议可以包括:诸如开放系统互连 (OSI) 模型、或者其任何派生物或变型 (例如,传输控制协议 / 互联网协议 (TCP/IP)、用户数据报协议 / IP (UDP/IP)) 之类的多层方案。另外,在通信系统 100 中还可以提供通过蜂窝网络的无线信号通信。可以提供适当的接口和基础架构来实现与蜂窝网络的通信。

[0026] 分组是可以在诸如互联网 110 之类的分组交换网络上,在源节点和目的节点之间进行路由的一个数据单元。一个分组包括源网络地址和目的网络地址。这些网络地址可以是 TCP/IP 消息协议中的互联网协议 (IP) 地址。如本申请所使用的术语 ‘数据’ 指代任何类型的二进制、数字、语音、视频、文本或者脚本数据、或者任何类型的源代码或者目标代码、或者能够在电子设备和 / 或网络中从一个点向另一个点传输的具有任何适当格式的任何其它适当信息。另外,消息、请求、响应和队列具有网络业务的形式,因此它们可以包括分组、帧、信号、数据等。

[0027] 如本申请所引用的, ‘受保护网络’ (如,受保护网络 114) 旨在意味着自有网络,或者在特定的实体或者组织的控制之下的网络,该网络被配置为防护来自入站 (以及可能的出站) 电子邮件消息的威胁。尝试到达受保护网络中的某些节点 (例如,邮件服务器) 的通信,首先被路由经过该受保护网络的一个或多个网络单元 (例如,网关、防火墙、代理服务器、安全设备等)。在一个示例性实施例中,受保护网络可以是针对该网络中的节点,使用专用地址空间 (例如,互联网协议 (IP) 地址空间) 的专用网络。专用地址空间可以遵循网络工作组的以下文档所设置的标准: Y. Rekhter 等人于 1996 年 2 月的请求注解 (RFC) 1918 和 / 或 R. Hinden 等人于 2005 年 10 月的请求注解 (RFC) 4193。另外地或者替代地,受保护网络可以实现任何其它适当形式的地址空间,该地址空间允许特定的实体或者组织对去往和来自该受保护网络的网络通信进行控制。

[0028] 外部网络 112 可以表示在受保护网络 114 之外的任何其它网络,外部网络 112 能够通过互联网 110,向受保护网络 114 发送电子邮件消息和 / 或从受保护网络 114 接收电子邮件消息。云电子邮件网络 113 可以表示通过互联网 110,向受保护网络 114 传送电子邮件

威胁服务的计算资源。

[0029] 为了便于说明目的,图 1 示出了互联网 110 促进外部网络 112、云电子邮件网络 113 和受保护网络 114 之间的网络通信。但是,也可以使用任何其它公共、未保护网络来促进这些网络通信。另外,本申请所公开的概念可等同地适用于专用网络(例如,内联网)之内,其中在该情况下,可以在该专用网络或者虚拟专用网(VPN)中提供外部客户端和云电子邮件服务。例如,一个组织可以拥有其自己的云电子邮件服务(在其专用网络内部),以及在其组织内拥有多个电子邮件策略设备(例如,按部门、按大楼等来分)。此外,这些电子邮件策略设备在专用网络中,可以是地理上不同的,也可以是地理上相同的。

[0030] 通常,在上面所述的几种实现中,可以将进入受保护网络 114 的进站电子邮件消息,重定向到云电子邮件网络 113 的电子邮件威胁传感器 130。这可以通过诸如互联网 110,或者通过专用网络(例如,组织的内联网)之类的未保护网络来发生。电子邮件威胁传感器 130 可以对于所接收的电子邮件消息执行防病毒和/或防垃圾邮件扫描,以便识别潜在威胁。电子邮件策略设备 140 和电子邮件威胁传感器 130 之间进行通信,确定是否阻止或者隔离该电子邮件消息,或者确定是否允许将该电子邮件消息转发到受保护网络 114 中的邮件服务器 155。如果对该电子邮件消息进行转发,则内部客户端 150 可以用于通过邮件服务器 155 来访问该电子邮件消息,或者邮件服务器 155 可以将该电子邮件消息传送到内部客户端 150。

[0031] 在一种示例性实现中,电子邮件威胁传感器 130 和电子邮件策略设备 140 都是网络单元,这意味着涵盖网络设备、服务器、路由器、开关、网关、网桥、负载均衡器、处理器、模块或者任何其它适当的设备、组件、单元或者可用于在网络环境中交换信息的对象。网络单元可以包括有助于实现其操作的任何适当的硬件、软件、组件、模块或者对象,以及用于接收、发送和/或在网络环境中传输数据或信息的适当接口。这可以包括用于允许数据或者信息的有效交换的适当算法和通信协议。

[0032] 关于与通信系统 100 相关联的内部结构,电子邮件威胁传感器 130 和电子邮件策略设备 140 中的每一个可以包括存储器单元(例如,存储器单元 132、142),以便存储在本申请所概述的操作中使用的信息。电子邮件威胁传感器 130 和电子邮件策略设备 140 中的每一个可以根据需要和具体的需求,将信息保持在任何适当的存储器单元(例如,随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程 ROM(EPROM)、电可擦除可编程 ROM(EEPROM)、专用集成电路(ASIC)等)、软件、硬件、固件或者任何其它适当的组件、设备、单元或者对象中。本申请所讨论的存储器项中的任何一个(例如,存储器单元 132、142)应当被解释成涵盖在广义术语‘存储器单元’之中。此外,在通信系统 100 中使用、跟踪、发送或者接收的信息,可以用任何数据库、寄存器、队列、表、高速缓存、控制列表或者其它存储结构来提供,所有这些可以在任何适当的时间帧处进行引用。此外,任何这些存储选项(例如,报告/消除队列 147、配置数据数据库 148、隔离的消息 149)还可以包括在如本申请所使用的广义术语‘存储器单元’之中。

[0033] 在某些示例性实现中,本申请所概述的功能可以通过在一个或多个易失性介质中编码的逻辑(例如,在 ASIC 中提供的嵌入式逻辑、数字信号处理器(DSP)指令、由处理器或者其它类似机器执行的软件(其潜在地包含目标代码和源代码)等)来实现,其中所述一个或多个易失性介质可以包括非临时性计算机可读介质。在这些实例中的一些,存储器单

元可以存储用于本申请所描述的操作的数据。这包括能够存储软件、逻辑、代码或者处理器指令的存储器单元,其中这些软件、逻辑、代码或者处理器指令被执行以实现本申请所描述的动作。

[0034] 在一种示例性实现中,通信系统 100 的网络单元(例如,电子邮件威胁传感器 130 和 / 或电子邮件策略设备 140) 可以包括用于实现或者用于鼓励如本申请所概述的操作的软件模块(例如,云扫描模块 133、通信模块 134、进站邮件策略模块 143、出站邮件策略模块 144 和 / 或本地扫描模块 145)。可以基于具体的配置和 / 或供应需求,以任何适当的方式对这些模块进行适当地组合。在示例性实施例中,这些操作可以通过在位于这些单元之外实现的硬件来执行,或者包括在某个其它网络设备中,以实现预定的功能。此外,可以将这些模块实现成软件、硬件、固件或者其任何适当组合。此外,这些单元还可以包括能够与其它网络单元进行协调,以便实现这些操作的软件(或者往复式软件),如本申请所概述的。

[0035] 另外,电子邮件威胁传感器 130 和电子邮件策略设备 140 中的每一个可以包括处理器(例如,处理器 131、141),该处理器可以执行软件或者某种算法,以执行如本申请所讨论的动作。处理器可以执行与数据相关联的任何类型的指令,以实现本申请所详细描述的操作。在一个示例中,处理器可以将一个单元或者制品(例如,数据)从一种状态或事物转换到另一种状态或事件。在另一个示例中,本申请所概述的动作可以使用固定逻辑或者可编程逻辑来实现(例如,由处理器执行的软件 / 计算机指令),本申请所识别的模块可以是某种类型的可编程处理器、可编程数字逻辑(例如,现场可编程门阵列(FPGA)、EPROM、EEPROM) 或者包括数字逻辑、软件、代码、电子指令的 ASIC、或者其任何适当的组合。本申请所描述的这些潜在处理单元、模块和机器中的任何一个,应当被解释成涵盖在广义术语‘处理器’之中。

[0036] 外部和内部电子邮件客户端 120 和 150 可以是:被配置为能够访问和管理各个电子邮件邮箱的任何系统。在一个实施例中,可以将外部和内部电子邮件客户端 120 和 150 配置成用于连接到各个邮件服务器的计算机程序或者邮件用户代理(MUA)。例如,内部电子邮件客户端 150 可以连接到邮件服务器 155,以便从相关联的电子邮件邮箱获取电子邮件消息。在一个实施例中,可以以有线或者无线网络节点(它们通常服务成用于网络连接的终端点),将外部和内部客户端 120 和 150 提供在它们各自的网络中。例如,这些节点可以包括桌面型计算机、膝上型计算机、移动设备、个人数字助理、智能电话、平板计算机或者其它类似的设备。

[0037] 邮件服务器 155 可以是包括消息传输代理(MTA)的网络单元,以便使用客户端-服务器应用体系结构,将电子邮件消息从一个计算机传送到另一个计算机。邮件服务器 155 可以从另一个邮件服务器接收电子邮件消息(例如,通过电子邮件威胁传感器 130 和电子邮件策略设备 140),将该电子邮件消息传送到其预期接收方。‘预期接收方’可以是电子邮件邮箱(例如,电子邮件邮箱 156),后者是用于接收和存储特定的用户或者账号的电子邮件消息的仓库。电子邮件邮箱可以在邮件服务器 155 上提供(例如,电子邮件邮箱 156),可以在拥有接收电子邮件客户端(例如,内部客户端 150)的网络节点上提供,也可以在可访问该邮件服务器和接收电子邮件客户端的另一个存储单元中提供。可以通过在接收方电子邮件地址中,放置在‘@’符号之前的本地地址或者用户名,用电子邮件消息的接收方电子邮件地址来标识该电子邮件邮箱。

[0038] 外部客户端 120 可以连接到另一个邮件服务器（没有示出），其中这里的另一个邮件服务器可以在具有外部客户端 120 的受保护网络中提供。替代地，该邮件服务器可以在云网络中提供（例如，通过互联网）、在外部客户端 120 远程连接到的另一个网络中提供，也可以与外部客户端 120 集成在一起。

[0039] 云电子邮件网络 113 可以包括诸如电子邮件威胁传感器 130 之类的网络单元，以便向诸如受保护网络 114 之类的其它网络提供电子邮件威胁服务。云电子邮件网络 113 还可以包括其它网络单元，例如，一个或多个网关、设备、防火墙、服务器，和 / 或有助于为接收电子邮件的网络实现电子邮件威胁服务的其它设备、组件、单元或者对象。电子邮件威胁传感器 130 的云扫描模块 133 可以包括一个或多个防病毒和 / 或防垃圾邮件组件，以便对电子邮件消息进行分解，对它们的各个组成部分（例如，消息数据、附件、超链接等）执行操作性的密集扫描，以识别恶意软件、垃圾邮件或者其它威胁。

[0040] 电子邮件威胁传感器 130 的通信模块 134 可以向受保护网络的电子邮件策略设备提供电子邮件消息信息，其中云电子邮件网络 113 为该受保护网络提供电子邮件威胁服务。例如，当电子邮件威胁传感器 130 接收到针对受保护网络 114 中的预期接收方的电子邮件消息时，通信模块 134 可以根据需要，向电子邮件策略设备 140 提供消息元数据、扫描结果和电子邮件消息数据。此外，通信模块 134 可以基于从通信模块 134 接收的信息，从电子邮件策略设备 140 接收响应。响应可以指示是否请求更多的数据（例如，扫描结果、电子邮件消息数据），或者是否应当基于策略，对电子邮件消息进行阻止。

[0041] 电子邮件策略设备 140 可以是受保护网络 114 中的网络单元。在一个示例性实施例中，可以在受保护网络 114 中实现电子邮件策略设备 140，以便从电子邮件威胁传感器 130 接收通信，并在根据电子邮件地址，将进站电子邮件消息转发到预期接收方之前，接收该进站电子邮件消息。此外，在通过另一个邮件服务器将出站电子邮件消息转发到外部客户端之前，电子邮件策略设备 140 还可以通过邮件服务器 155 从内部客户端接收该出站电子邮件消息。

[0042] 可以提供用户界面 146，以便允许获授权用户（例如，网络管理员）针对进入受保护网络 114 的电子邮件消息或者从受保护网络 114 外出的电子邮件消息，输入配置。在一个示例性实施例中，用户界面 146 可以包括具有图形用户界面（GUI）和适当的输入设备（例如，键盘、鼠标、跟踪球、触摸屏等）的控制台，以便允许用户输入可以保存在配置数据数据库 148 中的配置数据。

[0043] 配置数据可以包括基于某种消息元数据和 / 或扫描结果的策略。例如，配置数据可以包括：用于当电子邮件消息的扫描结果指示存在病毒时，阻止（或者允许）该电子邮件消息的策略。此外，配置数据还应当包括：用于当扫描结果指示存在某种类型的恶意软件（其不是病毒）时，允许电子邮件消息的策略。

[0044] 其它配置数据可以包括垃圾软件门限设置（例如，1-10）。在该示例中，如果超过该门限，则将该电子邮件消息识别成垃圾邮件，并对其进行阻止。在一种示例性场景中，用户可以为了某些类型的期望的电子邮件内容（例如，针对特定的药物的广告），配置较高的门限设置，以便允许接收这些电子邮件消息。此外，配置数据还可以是基于电子邮件消息的发送者（例如，域名或者特定的 IP 地址）。例如，配置数据可以包括：用于针对来自于特定发送方 IP 地址的电子邮件消息，关闭垃圾邮件扫描的策略。

[0045] 此外,用户还可以根据策略,配置对电子邮件消息采取不同的动作。示范性动作包括:阻止电子邮件消息发送到受保护网络,阻止电子邮件消息发送到受保护网络中的一个电子邮件地址的预期接收方,或者对电子邮件消息进行隔离。

[0046] 进站邮件策略模块 143 可以基于与进站电子邮件消息相关联的消息元数据和 / 或扫描结果,应用来自于配置数据数据库 148 的策略。此外,进站邮件策略模块 143 还可以基于策略评估,向电子邮件威胁传感器 130 发送适当的响应。

[0047] 配置数据还可以包含:针对要进行识别和 / 或过滤的网络特定内容(例如,图像分析、禁止的词 / 短语、机密和 / 或敏感信息等),需要对一些或者所有电子邮件消息进行另外的扫描的策略。本地扫描模块 145 可以配置为:针对云扫描中不包括的网络特定内容,对电子邮件消息进行扫描。例如,本地扫描可以包括:进站或者出站电子邮件消息的扫描,以应用在云扫描中没有应用的网络特定图像和 / 或文本分析(例如,针对淫秽物品、不可接受的图像、词语或者短语等)。此外,本地扫描还可以包括:进行扫描,以便对经由电子邮件策略设备 140 的敏感信息和机密信息进行识别和潜在地过滤。

[0048] 此外,电子邮件策略设备 140 还可以节省用于报告和指示目的某种信息。可以使用诸如阻止了什么电子邮件消息、以及该阻止的原因之类的消息元数据和 / 或信息,来传播报告 / 消息队列 147。因此,用户可以访问针对电子邮件消息问题的内部部署的(或者本地)报告。隔离的消息 149 可以包含:被电子邮件策略设备 140 阻止转发到受保护网络 114 中的它们目的地址的电子邮件消息的消息数据。

[0049] 虽然在图 1 中将报告 / 消息队列 147、配置数据数据库 148 和隔离的消息 149 表示成单独的存储单元,但这只是用于说明目的。在任何适当的配置中,可以对这些存储单元进行组合或者分离。此外,这些存储单元可以与电子邮件策略设备 140 集成在一起,也可以分布在受保护网络 114 中,或者分布在可以由电子邮件策略设备 140 访问的另一个网络中。

[0050] 转到图 2,该图根据一个示范性实施例,示出了外部客户端 120、电子邮件威胁传感器 130、电子邮件策略设备 140 和邮件服务器 155 之间的潜在网络通信的交互图 200。在该示范性交互中,外部客户端 120 是发送到邮件服务器 155 的电子邮件消息的源(或者‘发送客户端’),其中邮件服务器 155 是该电子邮件消息的目的地(或者‘接收主机’),并且拥有邮箱 156。在该示例中,电子邮件邮箱 156 是该电子邮件消息的预期接收方。发送的电子邮件消息可以具有分组的形式,其中这些分组具有与外部客户端 120 相关联的发送主机或者邮件服务器的源 IP 地址,以及受保护网络 114 中的邮件服务器 155 的目的 IP 地址。

[0051] 在 202,外部客户端 120 向接收方电子邮件地址发送电子邮件消息,其中接收方电子邮件地址标识在受保护网络 114 中的邮件服务器 155 上拥有电子邮件邮箱 156。该电子邮件消息被路由到云电子邮件网络 113 中的邮件威胁传感器 130。在一种示范性实现中,可以使用域名系统(DNS)的邮件交换(MX)记录,对电子邮件消息进行路由。域名的一个或多个 MX 记录可以指定:如何在简单邮件传输协议(SMTP)中对该电子邮件消息进行路由。SMTP 是用于在互联网协议网络之中进行电子邮件传输的互联网标准协议。在该场景中,云电子邮件网络 113 可以配置为向受保护网络 114 提供电子邮件威胁服务,并因此接收进入受保护网络 114 的所有进站电子邮件消息。

[0052] 在 204,电子邮件威胁传感器 130 使用适当的电子邮件协议,发起与电子邮件策略设备 140 的网络连接。在一个示范性实施例中,可以使用 SMTP。在 J. Klensin 等人于 2005

年 10 月的请求注解 (RFC) 5321 中,对 SMTP 进行了更新,其包括扩展的 SMTP (ESMTP) 增加。

[0053] 在一个示例性实现中,在 206 处,电子邮件策略设备 140 可以接受该网络连接,将其是否支持针对 SMTP 协议的定制扩展告之于众。定制扩展可以配置为:允许电子邮件威胁传感器 130 向电子邮件策略设备 140 传送关于电子邮件消息的另外信息(例如,消息元数据、扫描结果数据)。在一个实施例中,ESMTP 命令是专用的,并在进行从电子邮件威胁传感器 130 到电子邮件策略设备 140 的加密连接时,由电子邮件策略设备 140 进行广告。在其它实施例中,可以使用任何其它适当的协议来实现电子邮件威胁传感器 130 和电子邮件策略设备 140 之间的其它信息的通信。在一个特定的示例中,可以忽略相关 RFC 的至少一部分,可以实现 SMTP 会话中的非标准命令/协议来实现这些通信。

[0054] 一旦在电子邮件威胁传感器 130 和电子邮件策略设备 140 之间建立了网络连接,并且假定支持定制扩展或者其它适当的协议,在 208 处,电子邮件威胁传感器 130 就可以向电子邮件策略设备 140 发送消息元数据。消息元数据可以包括,但不限于:用于该电子邮件消息的连接和/或协议信息。连接信息可以包括:发送主机(例如,与外部客户端 120 相对应的邮件服务器)的 IP 地址和发送主机的域。协议信息可以包括标准 SMTP 信息(例如,发送方和接收方信息)。具体而言,协议信息可以包括发送方电子邮件地址或者域名,它们可以与该电子邮件消息的实际发送主机不相同。此外,协议信息还可以包括接收方电子邮件地址或者域。如果在受保护网络中不存在该预期接收方(电子邮件邮箱),则可以使用该信息来实现阻止电子邮件消息转发到受保护网络 114。

[0055] 在 210,电子邮件策略设备 140 对所接收的消息元数据和元数据策略进行评估。评估消息元数据可以包括:读取和解释该元数据。此外,可以对(例如,来自于配置数据数据库 148)元数据策略进行评估,以确定是否向所接收的消息元数据应用任何策略。可以基于所接收的消息元数据,确定在受保护网络 114 中接收该电子邮件消息(例如,通过进站邮件策略模块 143)是否被元数据策略禁止。这些策略可以由获授权用户在电子邮件策略设备 140 的用户界面中进行配置。例如,这些策略可以保存在配置数据数据库 148 中。电子邮件策略设备可以是内部部署的、本地设备或者其它网络单元,该设备可由获授权用户容易地访问。

[0056] 根据元数据的内容和可应用的策略,可以采取不同的动作。阻止电子邮件消息是可以采取的一种可能动作的示例。可以采取阻止动作,以防止电子邮件消息进入受保护网络。当将该电子邮件消息从另一个网络转发到该受保护网络中的任何节点时,就发生了进入该受保护网络。如果一个策略禁止在受保护网络中接收具有特定的消息元数据(例如,特定的源 IP 地址或者源域)的电子邮件消息(或者进入),则可以采取这种阻止动作。

[0057] 对电子邮件消息进行隔离是可以采取的一种可能动作的另一个示例。在该情况下,该策略可以准许受保护网络接收该电子邮件消息(例如,在电子邮件策略设备 140 处),但禁止将该电子邮件消息转发到受保护网络的预期接收方,如本申请所进一步描述的。隔离可以包括:保存电子邮件消息(例如,保存在隔离的消息 149 中),阻止该电子邮件消息转发到预期接收方。另外,基于本地扫描结果,在受保护网络中接收到该电子邮件消息(其进入)之后,也可以采取阻止动作,如本申请所进一步描述的。

[0058] 众多不同的策略配置可以用于基于消息元数据,管理电子邮件消息。在一种可能的配置中,一个策略可以明确地识别具体的发送主机网络地址、发送主机域名、发送方电子

邮件地址和 / 或要进行阻止、允许或者隔离的发送方域名。在另一种可能的配置中,可以使用模式匹配来确定要阻止哪些域。例如,如果发送主机的 IP 地址的查询返回 XYZ. com,则可以阻止 *. XYZ. com。在另一种配置中,一个策略可以包含:当电子邮件消息的接收方(或者目的地)邮件用户名在受保护网络 114 中不存在时,阻止将电子邮件消息转发到受保护网络 114 的规则。这些示例性配置仅用于说明目的,其并不旨在限制:用于基于消息元数据来管理电子邮件消息的众多配置可能性。另外,如果基于电子邮件消息的消息元数据,确定该电子邮件消息被策略禁止,则可以将该阻止和 / 或隔离动作和任何有关的信息记录在报告 / 消息队列 147 中。

[0059] 在 212, 电子邮件策略设备 140 可以基于其对于消息元数据的评估,以及任何有关的元数据策略的应用,向电子邮件威胁传感器 130 发送响应。在一个实施例中,该响应可以是指示是否向电子邮件策略设备 140 发送与该电子邮件消息相关联的更多信息的代码。因此,如果基于该电子邮件消息的具体元数据,没有任何策略被配置为阻止该电子邮件消息,则该响应码可以表示针对更多数据的请求。更多数据可以包括该电子邮件消息的扫描结果数据(例如,防病毒和 / 或防垃圾扫描结果数据)。但是,如果配置了基于电子邮件消息的具体元数据来禁止该电子邮件消息的策略,则该响应码可以表示不向电子邮件策略设备 140 发送与该电子邮件消息相关联的另外数据的请求。因此,在该场景中,可以从受保护网络中有效地阻止该电子邮件消息。

[0060] 在 214, 电子邮件威胁传感器 130 确定该响应是否表示针对更多数据的请求。如果其不是表示针对更多数据的请求,则在 236, 电子邮件威胁传感器 130 可以向发送的外部客户端 120 发送电子邮件消息状态,其中该状态指示不向该电子邮件消息的预期接收方传送该电子邮件消息。但是,如果该响应是针对更多数据的请求,则在 216, 可以对该电子邮件消息进行扫描(例如,防病毒扫描、防垃圾邮件扫描)。在一个实施例中,云扫描模块 133 可以执行这些扫描操作。扫描可以是使用电子邮件威胁传感器 130 的处理资源的密集操作,其对消息进行分解,对该电子邮件消息中的消息数据、附件和 / 或超链接执行扫描。

[0061] 在 218, 电子邮件威胁传感器 130 可以向电子邮件策略服务器 140 发送针对该电子邮件消息的扫描结果数据。在 220, 电子邮件策略设备 140 评估该电子邮件消息的扫描结果数据和扫描策略。评估扫描结果数据可以包括:对扫描结果数据进行读取和解析。此外,可以对(例如,来自于配置数据数据库 148 的)扫描策略进行评估,以确定是否向所接收的扫描结果数据应用任何策略。具体而言,可以基于所接收的扫描结果数据,确定在受保护网络 114 中接收该电子邮件消息(例如,由进站邮件策略模块 143)是否被扫描策略禁止。这些策略可以由获授权用户在电子邮件策略设备 140 的用户界面中进行配置。由于可以通过电子邮件策略设备 140 的用户界面 146 来维持配置数据数据库 148, 因此对于配置数据数据库 148 的更新,可以立即被电子邮件策略设备 140 实时地访问到。

[0062] 有众多不同的配置和动作(例如,阻止、隔离、允许重新路由等),可以用于基于电子邮件消息扫描结果数据和扫描策略,来管理电子邮件消息。针对受保护网络中的垃圾邮件和 / 或病毒通信,不同的实体可以具有不同的容忍度门限。给定的网络可以与另一个网络相比,具有用于接受垃圾电子邮件的更高门限设置。给定的网络可以具有下面的策略:禁止本网络中的任何节点接收具有所识别的病毒的任何电子邮件消息。另一个网络可以具有下面的策略:例如,当为了商业目的,需要具有所识别的病毒的电子邮件消息时,允许接收

这种病毒电子邮件消息。在其它配置中,给定的网络可以具有下面的策略:禁止将具有所识别病毒(或者垃圾邮件)的电子邮件消息传送到本网络中的预定电子邮件地址,但仍然可用于在该网络中的某些类型的安全设备(例如,电子邮件策略设备 140)中接收该电子邮件消息,以便对其进行隔离(例如,隔离在隔离的消息 149 中)。

[0063] 在另一个示例中,给定的网络可以允许特定的电子邮件广告,后者可以与该网络相关联的商业有关。如果电子邮件威胁传感器 130 通常在其防垃圾邮件扫描中,将这些电子邮件广告识别成垃圾邮件,则可以在电子邮件策略设备 140 处,对策略进行配置(例如,通过用户界面 146),以便允许这种特定类型的电子邮件广告。可以设置门限数量,以指示一个邮件被识别成垃圾邮件。如果网络具有接受垃圾邮件的更高容忍度,则可以设置更高门限数量。此外,可以按照用户、用户组或者网络,对垃圾邮件容忍门限进行配置。另外地或者替代地,可以基于电子邮件消息的发送者(例如,具体电子邮件地址的域名)来设置这种配置。相应地,可以针对特定的可信任域,对垃圾邮件过滤进行关闭。因此,可以在网络中,对用于入站和出站电子邮件消息的网络特定逻辑进行控制,而无需依赖于将配置数据推送到云服务。

[0064] 如果基于电子邮件消息的扫描结果数据,确定一个策略对该电子邮件消息进行阻止或者隔离,则可以将该阻止或隔离动作和任何有关的信息记录在例如报告/消息队列 147 中。这些示例性配置仅用于说明目的,其并不旨在限制:用于基于扫描结果数据来管理电子邮件消息的众多配置可能性。

[0065] 在 222,电子邮件策略设备 140 可以基于其对于扫描结果数据的评估,以及任何有关的扫描策略的应用,向电子邮件威胁传感器 130 发送响应。在一个实施例中,该响应可以是指示是否向电子邮件策略设备 140 发送该电子邮件消息的代码。因此,如果基于该电子邮件消息的具体扫描结果数据,没有任何策略被配置为阻止在受保护网络 114 中接收该电子邮件消息,则该响应码可以表示针对该电子邮件消息的请求。当策略禁止将该电子邮件消息转发给其接收方电子邮件地址,但允许受保护网络(例如,电子邮件策略设备 140)接收该电子邮件消息,以用于另外的处理和/或隔离目的时,也可以发送针对该电子邮件消息的请求。但是,如果基于该电子邮件消息的具体扫描结果,一个策略被配置为阻止在受保护网络 114 中接收该电子邮件消息,则该响应码可以表示不向电子邮件策略设备 140 发送与该电子邮件消息相关联的另外数据的请求。因此,在该场景中,可以从受保护网络中有效地阻止该电子邮件消息。

[0066] 在 224,电子邮件威胁传感器 130 确定该响应是否表示针对该电子邮件消息的请求。如果其不是表示针对该电子邮件消息的请求,则在 236,电子邮件威胁传感器 130 可以向发送的外部客户端 120 发送电子邮件消息状态,其中该状态指示不向该电子邮件消息的预期接收方传送该电子邮件消息。但是,如果该响应是针对该电子邮件消息的请求,则在 226,电子邮件威胁传感器 130 可以向电子邮件策略服务器 140 转发该电子邮件消息。

[0067] 在 228,电子邮件策略设备 140 可以对该电子邮件消息执行另外的处理。在一个实施例中,可以针对该特定的受保护网络中不允许的、而云扫描不是必须进行过滤的网络特定内容,执行另外的扫描。例如,给定的网络可能不允许某些类型的图像(例如,淫秽图像)或者某些词语或短语(例如,亵渎)。如果电子邮件威胁传感器 130 在其防病毒和/或防垃圾邮件扫描中没有识别这些项,则可以在电子邮件策略设备 140 处,对本地扫描策略

进行配置（例如，通过用户界面 146），并应用于从电子邮件威胁传感器 130 接收的电子邮件消息。还可以针对机密信息或者敏感信息来执行扫描，以便控制该信息的接收（例如，通过入站电子邮件消息）和该信息的分发（例如，通过出站电子邮件消息）。

[0068] 在电子邮件策略设备 140 处，可以对电子邮件消息采取阻止或者隔离动作。该动作可以取决于本地扫描结果（如果有的话）、并取决于消息元数据和扫描结果数据的先前评估（如果在 210 和 / 或 220 处，应用的策略指示应当对该电子邮件消息进行隔离的话）。阻止动作可以防止将该电子邮件消息传送到其预期接收方。隔离动作可以通过将电子邮件消息保存在隔离的消息 149 中，对该电子邮件消息进行隔离。在另一种实现中，可以将该电子邮件消息重新路由到另一个位置，例如以便用于另外的分析。

[0069] 在 230，基于针对特定于网络的禁止内容的另外扫描，确定该电子邮件消息是否被策略禁止。如果该电子邮件消息未被策略禁止（例如，不执行另外的扫描，或者执行另外的扫描，但没有指示禁止该电子邮件消息），则在 232，可以将该电子邮件消息转发到邮件服务器 155，后者可以将该消息转发到电子邮件邮箱 156。

[0070] 可以通过任何适当的机制，来确定在 232 处向邮件服务器 155 传送该电子邮件消息，其中这些机制可以是基于受保护网络 114 的具体需求来实现的。例如，可以使用标准的 SMTP 邮件传送规则。可以使用电子邮件消息中的接收方电子邮件地址，来查询域名系统（DNS），各种类型的 DNS 记录（例如，MX 记录、A 记录）可以提供邮件服务器 155 的网络地址。在另一种实现中，可以通过预先配置的路由，来确定这种传送。网络管理员可以配置电子邮件策略设备 140，将（在接收方电子邮件地址中所指示的）特定的域的电子邮件消息，转发到（例如，邮件服务器 155 的）特定目的网络地址。在另一种实现中，可以通过替代的目录服务，来确定这种传送。网络管理员可以配置电子邮件策略设备 140 查询目录服务中的一个属性（例如，LDAP/ 活动目录），来确定（例如，邮件服务器 155 的）目的网络地址。

[0071] 如果在 228 处执行另外的扫描，并且确定一个或多个本地扫描策略禁止将该电子邮件消息传送到受保护网络 114 中的其预期接收方，则可以对该电子邮件消息进行阻止或者隔离。在 234，电子邮件策略设备 140 向电子邮件威胁传感器 130 发送响应，其中该响应指示已对该电子邮件消息进行了阻止或者隔离。在 236，电子邮件威胁传感器 130 可以向发送方外部客户端 120 发送用于指示没有将该电子邮件消息传送到其预期接收方的状态。

[0072] 在 230，还可以基于消息元数据和元数据策略的先前评估（在 210 处）以及扫描结果数据和扫描策略（在 220 处），确定是否有一个策略需要该电子邮件消息被隔离。在该场景下，并不阻止电子邮件策略设备 140 接收该电子邮件消息，但在 230 处，阻止将该电子邮件消息转发到邮件服务器 155。因此，在 226 处，电子邮件策略设备 140 接收该电子邮件消息。该电子邮件消息可能需要另外的扫描，也可能不需要另外的扫描，但确定先前的策略评估是否需要对该电子邮件消息进行隔离。

[0073] 如果基于本地扫描策略，不需要对该电子邮件消息进行隔离，并且也不需要进行阻止，则在 232，可以将该电子邮件消息转发到邮件服务器 155，后者可以将该消息传送到电子邮件邮箱 156。在 234，电子邮件策略设备 140 可以向电子邮件威胁传感器 130 发送用于指示已将该电子邮件消息传送到其预期接收方的响应。在 236，电子邮件威胁传感器 130 可以随后向发送方外部客户端 120 发送用于指示已将该电子邮件消息传送到其预期接收方的状态。

[0074] 如果在 230 处,确定需要对该电子邮件消息进行隔离,则例如通过将该电子邮件消息保存在隔离的消息 149 中,来隔离该电子邮件消息。在 234,电子邮件策略设备 140 向电子邮件威胁传感器 130 发送用于指示已对该电子邮件消息进行了阻止或者隔离的响应。在 236,电子邮件威胁传感器 130 可以向发送方外部客户端 120 发送用于指示没有将该电子邮件消息传送到其预期接收方的状态。

[0075] 在另一个实现选项中,网络管理员可以对电子邮件策略设备 140 进行配置,以便即使某些电子邮件消息违反元数据策略、扫描策略和 / 或本地扫描策略中的一个或多个,也将这些电子邮件消息传送到它们的预期接收方。如果在一个电子邮件消息中检测到威胁和 / 或禁止的内容,则可以对该检测进行记录,和 / 或可以向适当的用户或者系统发送通知。类似地,如果电子邮件消息的消息元数据违反元数据策略,则可以对该违反进行记录,和 / 或可以发送通知。可以将该电子邮件消息传送到其预期接收方。替代地,可以将该电子邮件消息转发到指定的目的网络地址,以便进行进一步扫描、远程隔离或者检查。

[0076] 转到图 3,该图示出了可以与电子邮件威胁传感器 130 相关联的流程 300 的可能操作的示例性流程图。在一个实施例中,流程 300 的一个或多个操作可以由扫描模块 133 和 / 或通信模块 134 来执行。

[0077] 在 302,电子邮件威胁传感器 130 接收从发送客户端向受保护网络中的预期接收方发送的电子邮件消息。该预期接收方可以是受保护网络中的邮件服务器的电子邮件邮箱。在电子邮件消息的接收方电子邮件地址中标识了预期接收方。具体而言,可以在接收方电子邮件地址中,提供与电子邮件邮箱相对应的本地地址(或者用户名)以及与受保护网络相对应的域名。发送客户端可以在配置所述邮件服务器的受保护网络之外。

[0078] 在 304,(例如,扫描模块 133)可以针对诸如恶意软件和垃圾邮件之类的威胁,对该电子邮件消息进行扫描。在该示例性实施例中,在电子邮件威胁传感器 130 连接到受保护网络的电子邮件策略设备之前,发生对电子邮件消息的扫描(在 304 处)。但是,在其它实施例中,可以在电子邮件威胁传感器 130 和电子邮件策略设备 140 之间的某种通信之后,发生对于该电子邮件消息的扫描,如本申请所进一步描述的。

[0079] 在 306,电子邮件威胁传感器与受保护网络中的电子邮件策略设备建立连接。此外,电子邮件策略设备还可以广告其是否支持诸如针对 SMTP 协议的定制扩展之类的协议,以允许电子邮件威胁传感器发送关于该电子邮件消息的其它信息(例如,消息元数据、扫描结果数据)。在 308,电子邮件威胁传感器向电子邮件策略设备发送该电子邮件消息的消息元数据。该消息元数据可以包括与该电子邮件消息相关联的连接信息和 / 或协议信息。

[0080] 在 310,电子邮件威胁传感器从电子邮件策略设备接收响应。该响应可以是基于应用于消息元数据的电子邮件策略设备的策略配置。在 312,确定该响应是否表示针对与该电子邮件消息相关联的更多数据的请求。如果该响应不是针对更多数据的请求,则该响应指示在受保护网络中接收该电子邮件消息被元数据策略禁止。在该情况下,电子邮件威胁传感器可以在 330 处发送状态消息,以便向发送客户端通知:预期接收方不接收该电子邮件消息。

[0081] 如果来自于电子邮件策略设备的响应是针对更多数据的请求,则在 314 处,(例如,扫描模块 133)可以对该电子邮件消息进行扫描。314 处的该扫描操作表示:在电子邮件威胁传感器连接到电子邮件策略设备之后,并且确定元数据策略并不禁止在受保护网络

中接收该电子邮件消息之后,对该电子邮件消息进行扫描的另一个实施例。因此,根本不会对基于消息元数据的策略所阻止的电子邮件消息进行扫描。因此,可以通过在 314 处,而不是在 304 处执行扫描,来节省处理。

[0082] 在 316,电子邮件威胁传感器可以向电子邮件策略设备发送扫描结果数据。在 318,电子邮件威胁传感器从电子邮件策略设备接收响应。该响应可以是基于应用于扫描结果数据的电子邮件策略设备的策略配置。

[0083] 在 320,确定该响应是否表示针对该电子邮件消息的请求。如果该响应不是针对于电子邮件消息的请求,则该响应指示在受保护网络中接收该电子邮件消息被扫描策略禁止。在该情况下,电子邮件威胁传感器可以在 330 处发送状态消息,以便向发送客户端通知:预期接收方不接收该电子邮件消息。

[0084] 如果在 320 处,确定来自于电子邮件策略设备的响应是针对电子邮件消息的请求,则在 322 处,电子邮件威胁传感器向电子邮件策略设备发送该电子邮件消息。在 324 处,电子邮件威胁传感器从电子邮件策略设备接收响应。该响应可以是基于应用于该电子邮件消息的另外扫描的策略配置。但是,如果不执行另外的扫描,则该响应可以是基于向预期接收方发送的电子邮件消息。

[0085] 在 324 处从电子邮件策略设备接收到该响应之后,在 326 处,确定该电子邮件消息是否被电子邮件策略设备上的策略阻止或者隔离。如果该电子邮件消息被阻止或者隔离,则电子邮件威胁传感器可以在 330 处发送状态消息,以便向发送客户端通知:没有向预期接收方发送该电子邮件消息。但是,如果该电子邮件消息未被阻止或者隔离,则在 328 处,电子邮件威胁传感器可以发送状态消息,以向发送客户端通知:将该电子邮件消息发送给预期接收方。

[0086] 转到图 4A 和图 4B,这些图示出了可以与电子邮件策略设备 140 相关联的流程 400 的可能操作的示例性流程图。在一个实施例中,流程 400 中的一个或多个操作可以由进站邮件策略模块 143 和 / 或本地扫描模块 145 来执行。

[0087] 在图 4A 和图 4B 中,流程 400 假定已经在电子邮件策略设备和提供云中的威胁服务的电子邮件威胁传感器之间,建立了连接(如图 2 和图 3 中所详细描述)。在 402,电子邮件策略设备从电子邮件威胁传感器接收消息元数据。在 404,对该消息元数据进行评估,并且就该电子邮件消息是否被任何元数据策略配置所禁止来做出确定。如果基于该消息元数据(例如,连接信息、协议信息),元数据策略禁止该电子邮件消息,则在 432 处,可以将电子邮件消息阻止记录在报告 / 消息队列 147 中。随后,在 434 处,由于对该电子邮件消息进行了阻止,因此可以向电子邮件威胁传感器发送用于指示不请求更多的数据的响应。

[0088] 如果基于消息元数据,没有任何元数据策略禁止该电子邮件消息(如 404 处所确定的),则在 406,电子邮件策略设备可以向电子邮件威胁传感器发送用于请求与该电子邮件消息相关联的扫描结果数据的响应。在 408,电子邮件策略设备可以从电子邮件威胁传感器接收针对该电子邮件消息的扫描结果数据。这些扫描结果数据可以包括:源自于在电子邮件云网络中,对该电子邮件消息所执行的扫描的防病毒扫描结果和 / 或防垃圾邮件扫描结果。

[0089] 在 410,对扫描结果数据进行评估,确定该电子邮件消息是否被任何扫描策略配置所禁止。如果基于这些扫描结果数据,一个扫描策略禁止该电子邮件消息,则在 432 处,可

以将电子邮件消息阻止记录在报告 / 消息队列 147 中。可以针对给定网络的具体需求,对扫描策略配置进行调整。在一些场景中,所有显性云扫描结果(例如,针对于病毒或者垃圾邮件)可能被扫描策略禁止。然而,在其它场景中,某些病毒或者垃圾电子邮件可能未被禁止。在 434,由于该电子邮件消息被扫描策略禁止在受保护网络中接收,因此可以向电子邮件威胁传感器发送用于指示不请求更多的数据的响应。

[0090] 如果基于这些扫描结果数据,没有任何扫描策略禁止该电子邮件消息(如 410 处所确定的),则在 412,电子邮件策略设备可以向电子邮件威胁传感器发送用于请求该电子邮件消息的响应。在 414,电子邮件策略设备可以从电子邮件威胁传感器接收该电子邮件消息。

[0091] 在接收到该电子邮件消息之后,在 416 处,确定是否应当对该电子邮件消息进行隔离。在流程 400 的实施例中,电子邮件策略设备的策略配置可能需要对基于消息元数据或者云扫描结果数据而被禁止的某些电子邮件消息进行隔离。在该实现中,可以在元数据和扫描策略评估期间,将该电子邮件消息在电子邮件策略设备中识别和标记成阻止和 / 或隔离的(例如,在隔离的消息 149 中)。一旦接收到该电子邮件消息,则可以(例如,在报告 / 消息队列 147 中)执行搜索,以确定是否已经将该电子邮件消息确定为被策略所禁止,并根据需要来标记成要进行隔离。

[0092] 如果在 416 处,确定该电子邮件消息先前已被标记为要进行隔离,则在 426 处,可以通过例如将该消息数据保存在隔离的消息 149 中,对该电子邮件消息进行隔离。在 432 处,可以将该电子邮件消息在例如报告 / 消息队列 147 中,记录成阻止的(和 / 或隔离的)。在 434,可以向电子邮件威胁传感器发送用于指示该电子邮件消息已被阻止和 / 或隔离,并因此没有被预期接收方接收的响应。

[0093] 如果在 416 处,确定该电子邮件消息先前没有被标记为要进行隔离,则在 418 处,确定该电子邮件消息是否需要进一步扫描。例如,可以针对传送元数据的进站电子邮件消息和云扫描结果评估,针对禁止的内容,配置特定于网络的策略。如果该电子邮件消息需要进一步的扫描,则在 420 处,对该电子邮件消息进行扫描。

[0094] 在 422 处,对本地扫描结果进行评估,并且就该电子邮件消息是否被任何本地扫描策略配置所禁止来做出确定。如果基于本地扫描结果,至少一个本地扫描策略禁止该电子邮件消息,则在 428 处,确定是否有一个策略需要该电子邮件消息被隔离。如果有,则在 430,对该电子邮件消息进行隔离。无论是否对该电子邮件消息进行隔离,在 432 处,都可以将电子邮件消息阻止记录在例如报告 / 消息队列 147 中。随后,在 434,可以向电子邮件威胁传感器发送用于指示该电子邮件消息已被阻止和 / 或隔离,并因此没有被预期接收方接收的响应。

[0095] 如果基于本地扫描结果,没有任何本地扫描策略禁止该电子邮件消息(如 422 处所确定的),或者如果该电子邮件消息不需要进一步的扫描(如 418 处所确定的),则在 424,电子邮件策略设备根据该电子邮件消息中的接收方电子邮件地址,对该电子邮件消息进行转发。具体而言,电子邮件策略设备可以将该电子邮件消息转发到邮件服务器,后者配置为在受保护网络中接收电子邮件消息。随后,该邮件服务器可以将该电子邮件消息传送给预期接收方(例如,电子邮件邮箱)。在 436,电子邮件策略设备还可以向电子邮件威胁传感器发送用于指示已将该电子邮件消息转发给预期接收方的响应。

[0096] 图 5 根据一个实施例,示出了以点对点 (PtP) 配置进行布置的计算系统 500。具体而言,图 5 示出了通过多个点对点接口来互连处理器、存储器和输入 / 输出设备的系统。通常,可以用与计算系统 500 相同或者相类似的方式,来配置通信系统 100 中的网络单元里的一个或多个。例如,可以用与示例性计算系统 500 相同或者相类似的方式,来配置本申请所描述的电子邮件威胁传感器 130 和电子邮件策略设备 140 中的每一个,其中处理器 131 和 141 分别与处理器 574 和 / 或 584 相对应,存储器单元 132 和 142 分别与存储器单元 532 和 / 或 534 相对应。

[0097] 如图 5 中所示,系统 500 可以包括一些处理器,但为了清楚说明起见,只示出了两个处理器 570 和 580。虽然示出了两个处理器 570 和 580,但应当理解的是,系统 500 的实施例还可以包括仅一个这种处理器。处理器 570 和 580 中的每一个可以包括一组内核 (即,处理器内核 574A 和 574B 与处理器内核 584A 和 584B),以执行一个程序的多个线程。这些内核可以被配置为:以类似于上面参照图 1-4 所讨论的方式来执行指令代码。每一个处理器 570、580 可以包括至少一个共享高速缓存 571、581。共享高速缓存 571、581 可以存储由处理器 570、580 的一个或多个组件 (例如,处理器内核 574 和 584) 使用的数据 (例如,指令)。

[0098] 此外,处理器 570 和 580 还可以包括集成内存控制器逻辑 (MC) 572 和 582,以分别与存储器单元 532 和 534 进行通信。存储器单元 532 和 / 或 534 可以存储由处理器 570 和 580 使用的各种数据。在替代的实施例中,内存控制器逻辑 572 和 582 可以是与处理器 570 和 580 相独立的分离逻辑电路。

[0099] 处理器 570 和 580 可以是任何类型的处理器,例如,参照图 1 所讨论的那些处理器。处理器 570 和 580 可以分别使用点对点接口电路 578 和 588,通过点对点 (PtP) 接口 550 来交换数据。处理单元 570 和 580 可以使用点对点接口电路 576、586、594 和 598,分别通过点对点接口 552 和 554 与芯片集 590 来交换数据。此外,芯片集 590 还可以使用接口电路 592 (其可以是 PtP 接口电路),通过高性能图形接口 539,与高性能图形电路 538 来交换数据。在替代的实施例中,可以将图 5 中所示出的 PtP 链路中的任意一个或者全部,实现成不同于 PtP 链路的多点分支总线。

[0100] 芯片集 590 可以通过接口电路 596,与总线 520 进行通信。总线 520 可以具有通过其进行通信的一个或多个设备,例如,总线桥接 518 和 I/O 设备 516。通过总线 510,总线桥接 518 可以与诸如键盘 / 鼠标 512 (或者诸如触摸屏、跟踪球等之类的其它输入设备)、通信设备 526 (例如,调制解调器、网络接口设备、或者可以通过计算机网络 560 进行通信的其它类型的通信设备)、音频 I/O 设备 514 和 / 或数据存储设备 528 之类的其它设备进行通信。数据存储设备 528 可以存储由处理器 570 和 / 或 580 执行的代码。在替代的实施例中,该总线体系结构的任何部分可以使用一个或多个 PtP 链路来实现。

[0101] 图 5 中所描述的计算机系统是可以用于实现本申请所讨论的各种实施例的计算系统的一个实施例的示意性视图。应当理解的是,可以将图 5 中所描述的系统的各种组件,组合在片上系统 (SoC) 体系结构或者任何其它适当的配置中。例如,本申请所公开的实施例可以并入到包括移动设备 (例如,智能蜂窝电话、平板计算机、个人数字助理、便携式游戏设备等) 的系统中。应当理解的是,在至少一些实施例中,可以使用 SoC 体系结构来提供这些移动设备。

[0102] 图6根据一个实施例,示出了一种处理器内核600。处理器内核600可以是用于任何类型的处理器(例如,微处理器、嵌入式处理器、数字信号处理器(DSP)、网络处理器、或者用于执行代码的其它设备)的内核。虽然在图6中仅示出了一个处理器内核600,但一个处理器可以替代地包括一个以上的图6中所示出的处理器内核600。例如,处理器内核600表示参照图5的处理器570和580所示出和描述的处理器内核574a、574b、584a和584b的一个示例性实施例。处理器内核600可以是单线程内核,或者对于至少一个实施例来说,处理器内核600可以是多线程的,每一个内核可以包括一个以上的硬件线程上下文(或者“逻辑处理器”)。

[0103] 此外,图6还根据一个实施例,示出了耦接到处理器内核600的存储器602。存储器602可以是各种各样的存储器中的任何一种(其包括存储器层次结构的各层),如本领域普通技术人员所公知或者可获得的。存储器602可以包括将由处理器内核600执行的代码604,其中代码604可以是一个或多个指令。处理器内核600可以遵循代码604所指示的程序指令序列。各条指令进入前端逻辑606,并由一个或多个解码器608进行处理。该解码器可以生成微操作(例如,具有预定的格式的固定宽度微操作),以作为其输出,或者该解码器可以生成其它指令、微指令或者用于反映原始代码指令的控制信号。此外,前端逻辑606还包括寄存器重命名逻辑610和调度逻辑612,其中调度逻辑612通常分配资源,对于与要执行的指令相对应的操作进行排队。

[0104] 此外,处理器内核600还可以包括具有一组执行单元616-1到616-N的执行逻辑614。一些实施例可以包括:专用于特定的功能或者功能集的多个执行单元。其它实施例可以包括只包括一个执行单元,或者只包括能够执行特定的功能的一个执行单元。执行逻辑614执行代码指令所指定的操作。

[0105] 在完成了代码指令所指定的操作的执行之后,后端逻辑618可以隐退代码604的这些指令。在一个实施例中,处理器内核600允许乱序执行,但需要按顺序地隐退指令。隐退逻辑620可以采用各种的已知形式(例如,重排序缓冲器等)。用此方式,在代码604的执行期间,至少依据解码器所产生的输出、寄存器重命名逻辑610所使用的硬件寄存器和表格、以及执行逻辑614所修改的任何寄存器(没有示出),对处理器内核600进行变换。

[0106] 虽然在图6中没有示出,但处理器可以在具有处理器内核600的芯片上包括其它单元,本申请参照图5示出和描述了这些单元中的至少一些。例如,如图5中所示,处理器可以包括内存控制逻辑以及处理器内核600。处理器可以包括I/O控制逻辑和/或可以包括与内存控制逻辑集成在一起的I/O控制逻辑。

[0107] 应当注意,使用本申请所提供的示例,围绕两个、三个或者更多网络单元来描述了交互。但是,这只是用于清楚说明和举例目的。在某些情况下,通过仅参照有限数量的网络单元,可以更容易地描述给定的流程集的功能中的一个或多个。应当理解的是,通信系统100以及其教导内容是可容易扩展的,能适应很大数量的组件,以及更复杂/混杂的布置和配置。因此,所提供的示例应当不限制本发明的保护范围,或者抑制通信系统100的广泛教导,如潜在地应用于无数的其它体系结构。

[0108] 同样重要的是要注意,前述的流程图(即,图2-4)仅示出了可以由通信系统100执行,或者可以在通信系统100中执行的可能的相关场景的一些。当需要时,可以删除或者去除这些操作中的一些,或者可以对这些操作进行相当地修改或者改变,而不脱离本发明

的保护范围。此外,很多这些操作被描述成与一个或多个其它操作同时地或者并行地执行。但是,可以对这些操作的时间进行相当地改变。为了举例和讨论目的,提供了前述的操作流程。通信系统 100 提供了相当的灵活性,其在于:可以在不脱离本发明的教导内容的基础上,提供任何适当的排列、年表、配置和定时机制。

[0109] 虽然参照特定的排列和配置来详细地描述了本发明,但可以显著地改变这些示例性配置和排列,而不脱离本发明的保护范围。此外,可以基于具体的需求和实现,对某些组件进行组合、分离、消除或者增加。另外,虽然参照有助于所述通信处理的特定单元和操作来示出了通信系统 100,但这些单元和操作可以用能实现通信系统 100 的预定功能的任何适当体系结构、协议和 / 或处理来替代。

[0110] 下面的示例与根据本说明书的实施例有关。一个或多个实施例可以提供用于向电子邮件消息应用策略的方法。该方法可以包括:由受保护网络中的进站策略模块接收电子邮件消息的消息元数据;基于所述消息元数据,确定在所述受保护网络中接收所述电子邮件消息是否被一个或多个元数据策略中的至少一个元数据策略所禁止;如果在所述受保护网络中接收所述电子邮件消息被所述至少一个元数据策略禁止,则阻止将所述电子邮件消息转发到所述受保护网络。

[0111] 在一个实施例的一个示例中,所述阻止包括:向云网络中的电子邮件威胁传感器发送响应码,其中所述电子邮件威胁传感器从另一个网络中的发送客户端接收所述电子邮件消息。

[0112] 一个实施例的一个示例还包括:如果在所述受保护网络中接收所述电子邮件消息未被所述一个或多个元数据策略禁止,则请求针对所述电子邮件消息的扫描结果数据。

[0113] 一个实施例的一个示例还包括:由所述受保护网络中的进站策略模块接收所述扫描结果数据;基于所述扫描结果数据,确定在所述受保护网络中接收所述电子邮件消息是否被一个或多个扫描策略中的至少一个扫描策略禁止;如果在所述受保护网络中接收所述电子邮件消息被所述至少一个扫描策略禁止,则阻止将所述电子邮件消息转发到所述受保护网络。

[0114] 一个实施例的一个示例还包括:如果在所述受保护网络中接收所述电子邮件消息未被所述一个或多个扫描策略禁止,则请求所述电子邮件消息。

[0115] 一个实施例的一个示例还包括:当请求所述电子邮件消息时,由所述受保护网络中的进站策略模块接收所述电子邮件消息;将所述电子邮件消息转发到所述受保护网络中的邮件服务器,其中所述邮件服务器将所述电子邮件消息传送给所述电子邮件消息的预期接收方。

[0116] 一个实施例的一个示例还包括:当请求所述电子邮件消息时,由所述受保护网络中的进站策略模块接收所述电子邮件消息;针对一个或多个本地扫描策略所禁止的内容,对所接收的电子邮件消息进行扫描;响应于在所述扫描期间发现至少一些禁止的内容,对所述电子邮件消息进行隔离。

[0117] 一个实施例的一个示例还包括:当请求所述电子邮件消息时,由所述受保护网络中的进站策略模块接收所述电子邮件消息;针对一个或多个本地扫描策略所禁止的内容,对所接收的电子邮件消息进行扫描;响应于在所述扫描期间发现至少一些禁止的内容,阻止将所述电子邮件消息传送给所述电子邮件消息的预期接收方。

[0118] 一个实施例的一个示例还包括：响应于在所述扫描期间没有发现任何禁止的内容，将所述电子邮件消息转发给所述受保护网络中的邮件服务器，其中所述邮件服务器将所述电子邮件消息传送给所述电子邮件消息的预期接收方。

[0119] 一个或多个实施例提供了存储有用于向电子邮件消息应用策略的指令的至少一种机器可读存储介质，当所述指令由处理器执行时，使得所述处理器执行以下操作：由受保护网络中的进站策略模块接收电子邮件消息的消息元数据；基于所述消息元数据，确定在所述受保护网络中接收所述电子邮件消息是否被一个或多个元数据策略中的至少一个元数据策略禁止；如果在所述受保护网络中接收所述电子邮件消息被所述至少一个元数据策略禁止，则阻止将所述电子邮件消息转发到所述受保护网络。一个实施例的一个示例还包括当由所述处理器执行时，使得所述处理器执行以下操作的指令：向云网络中的电子邮件威胁传感器发送响应码，以阻止将所述电子邮件消息转发到所述受保护网络，其中所述电子邮件威胁传感器从另一个网络中的发送客户端接收所述电子邮件消息。

[0120] 一个实施例的一个示例还包括当由所述处理器执行时，使得所述处理器执行以下操作的指令：如果在所述受保护网络中接收所述电子邮件消息未被所述一个或多个元数据策略禁止，则请求针对所述电子邮件消息的扫描结果数据。

[0121] 一个实施例的一个示例还包括当由所述处理器执行时，使得所述处理器执行以下操作的指令：由所述受保护网络中的进站策略模块接收所述扫描结果数据；基于所述扫描结果数据，确定在所述受保护网络中接收所述电子邮件消息是否被一个或多个扫描策略中的至少一个扫描策略禁止；如果在所述受保护网络中接收所述电子邮件消息被所述至少一个扫描策略禁止，则阻止将所述电子邮件消息转发到所述受保护网络。

[0122] 一个实施例的一个示例还包括当由所述处理器执行时，使得所述处理器执行以下操作的指令：如果在所述受保护网络中接收所述电子邮件消息未被所述一个或多个扫描策略禁止，则请求所述电子邮件消息。

[0123] 一个实施例的一个示例还包括当由所述处理器执行时，使得所述处理器执行以下操作的指令：当请求所述电子邮件消息时，由所述受保护网络中的进站策略模块接收所述电子邮件消息；将所述电子邮件消息转发到所述受保护网络中的邮件服务器，其中所述邮件服务器将所述电子邮件消息传送给所述电子邮件消息的预期接收方。

[0124] 一个实施例的一个示例还包括当由所述处理器执行时，使得所述处理器执行以下操作的指令：当请求所述电子邮件消息时，由所述受保护网络中的进站策略模块接收所述电子邮件消息；针对被一个或多个本地扫描策略所禁止的内容，对所接收的电子邮件消息进行扫描；响应于在扫描所述电子邮件消息时，发现至少一些禁止的内容，对所述电子邮件消息进行隔离。

[0125] 一个实施例的一个示例还包括当由所述处理器执行时，使得所述处理器执行以下操作的指令：当请求所述电子邮件消息时，由所述受保护网络中的进站策略模块接收所述电子邮件消息；针对被一个或多个本地扫描策略所禁止的内容，对所接收的电子邮件消息进行扫描；响应于在所述扫描期间发现至少一些禁止的内容，阻止将所述电子邮件消息传送给所述电子邮件消息的预期接收方。

[0126] 一个实施例的一个示例还包括当由所述处理器执行时，使得所述处理器执行以下操作的指令：响应于在所述扫描期间没有发现任何禁止的内容，将所述电子邮件消息转发

给所述受保护网络中的邮件服务器,其中所述邮件服务器配置为:将所述电子邮件消息传送给所述电子邮件消息的预期接收方。

[0127] 一个或多个实施例包括一种用于向电子邮件消息应用策略的装置,该装置包括:受保护网络中的处理器;在所述处理器上执行的进站策略模块,所述进站策略模块配置为:接收电子邮件消息的消息元数据;基于所述消息元数据,确定在所述受保护网络中接收所述电子邮件消息是否被一个或多个元数据策略中的至少一个元数据策略禁止;如果在所述受保护网络中接收所述电子邮件消息被所述至少一个元数据策略禁止,则阻止将所述电子邮件消息转发到所述受保护网络。

[0128] 一个实施例的一个示例还包括:所述进站策略模块配置为:向云网络中的电子邮件威胁传感器发送响应码,以阻止将所述电子邮件消息转发到所述受保护网络,其中所述电子邮件威胁传感器从另一个网络中的发送客户端接收所述电子邮件消息。

[0129] 一个实施例的一个示例还包括:所述进站策略模块配置为:如果在所述受保护网络中接收所述电子邮件消息未被所述一个或多个元数据策略禁止,则请求针对所述电子邮件消息的扫描结果数据。

[0130] 一个实施例的一个示例还包括:所述进站策略模块配置为:接收所述扫描结果数据;基于所述扫描结果数据,确定在所述受保护网络中接收所述电子邮件消息是否被一个或多个扫描策略中的至少一个扫描策略禁止;如果在所述受保护网络中接收所述电子邮件消息被所述至少一个扫描策略禁止,则阻止将所述电子邮件消息转发到所述受保护网络。

[0131] 一个实施例的一个示例还包括:所述进站策略模块配置为:如果在所述受保护网络中接收所述电子邮件消息未被所述一个或多个扫描策略禁止,则请求所述电子邮件消息。

[0132] 一个实施例的一个示例还包括:所述进站策略模块配置为:当请求所述电子邮件消息时,接收所述电子邮件消息;将所述电子邮件消息转发到所述受保护网络中的邮件服务器,其中所述邮件服务器将所述电子邮件消息传送给所述电子邮件消息的预期接收方。

[0133] 一个实施例的一个示例还包括:所述进站策略模块配置为:当请求所述电子邮件消息时,接收所述电子邮件消息;针对被本地扫描策略所禁止的内容,对所接收的电子邮件消息进行扫描;响应于在所述扫描期间发现至少一些禁止的内容,对所述电子邮件消息进行隔离。

[0134] 一个实施例的一个示例还包括:所述进站策略模块配置为:当请求所述电子邮件消息时,接收所述电子邮件消息;针对被本地扫描策略所禁止的内容,对所接收的电子邮件消息进行扫描;响应于在所述扫描期间发现至少一些禁止的内容,阻止将所述电子邮件消息传送给所述电子邮件消息的预期接收方。

[0135] 一个实施例的一个示例还包括:所述进站策略模块配置为:响应于在所述扫描期间没有发现任何禁止的内容,将所述电子邮件消息转发给所述受保护网络中的邮件服务器,其中所述邮件服务器配置为:将所述电子邮件消息传送给所述电子邮件消息的预期接收方。

[0136] 一个或多个实施例提供了存储有用于向电子邮件消息应用策略的指令的至少一种机器可读存储介质,当所述指令由处理器执行时,使得所述处理器执行以下操作:接收具有接收方电子邮件地址的电子邮件消息,所述接收方电子邮件地址标识受保护网络中的预

期接收方；向所述受保护网络中的进站邮件策略模块发送所述电子邮件消息的消息元数据；如果在所述受保护网络中接收所述电子邮件消息被一个或多个元数据策略中的至少一个元数据策略禁止，则阻止将所述电子邮件消息转发到所述受保护网络。

[0137] 一个实施例的一个示例还包括当由所述处理器执行时，使得所述处理器执行以下操作的指令：针对一个或多个威胁，对所述电子邮件消息进行扫描；如果在所述受保护网络中接收所述电子邮件消息未被所述一个或多个元数据策略禁止，则向所述受保护网络中的进站邮件策略模块发送扫描结果数据。

[0138] 一个实施例的一个示例还包括当由所述处理器执行时，使得所述处理器执行以下操作的指令：如果在所述受保护网络中接收所述电子邮件消息未被所述一个或多个扫描策略禁止，则向所述受保护网络中的进站邮件策略模块发送所述电子邮件消息。

[0139] 一种特定的示例性实现可以包括：用于在受保护网络中接收电子邮件消息的消息元数据的模块；用于基于所述消息元数据，确定在所述受保护网络中接收所述电子邮件消息是否被一个或多个元数据策略中的至少一个元数据策略禁止的模块；用于如果在所述受保护网络中接收所述电子邮件消息被所述至少一个元数据策略禁止，则阻止将所述电子邮件消息转发到所述受保护网络的模块。此外，该实现还可以包括：用于如果在所述受保护网络中接收所述电子邮件消息未被所述一个或多个元数据策略禁止，则请求针对所述电子邮件消息的扫描结果数据的模块。此外，该实现还可以包括：用于在所述受保护网络中接收所述扫描结果数据的模块；用于基于所述扫描结果数据，确定在所述受保护网络中接收所述电子邮件消息是否被一个或多个扫描策略中的至少一个扫描策略禁止的模块；用于如果在所述受保护网络中接收所述电子邮件消息被所述至少一个扫描策略禁止，则阻止将所述电子邮件消息转发到所述受保护网络的模块。此外，该实现还可以包括：用于如果在所述受保护网络中接收所述电子邮件消息未被所述一个或多个扫描策略禁止，则请求所述电子邮件消息的模块。另外，该实现还可以包括：用于当所述电子邮件消息被请求时，在所述受保护网络中接收所述电子邮件消息的模块；用于针对被一个或多个本地扫描策略所禁止的内容，对所接收的电子邮件消息进行扫描的模块；用于响应于在所述扫描期间发现至少一些禁止的内容，对所述电子邮件消息进行隔离或者阻止的模块。

[0140] 另一种示例性实现可以包括：用于接收具有接收方电子邮件地址的电子邮件消息的模块，其中所述接收方电子邮件地址标识受保护网络中的预期接收方；用于向所述受保护网络中的进站邮件策略模块发送所述电子邮件消息的消息元数据的模块；用于如果在所述受保护网络中接收所述电子邮件消息被一个或多个元数据策略中的至少一个元数据策略禁止，则阻止将所述电子邮件消息转发到所述受保护网络的模块。此外，该实现还可以包括：用于针对一个或多个威胁，对所述电子邮件消息进行扫描的模块；用于如果在所述受保护网络中接收所述电子邮件消息未被所述一个或多个元数据策略禁止，则向所述受保护网络中的进站邮件策略模块发送扫描结果数据的模块。此外，该实现还可以包括：用于如果在所述受保护网络中接收所述电子邮件消息未被所述一个或多个扫描策略禁止，则向所述受保护网络中的进站邮件策略模块发送所述电子邮件消息的模块。

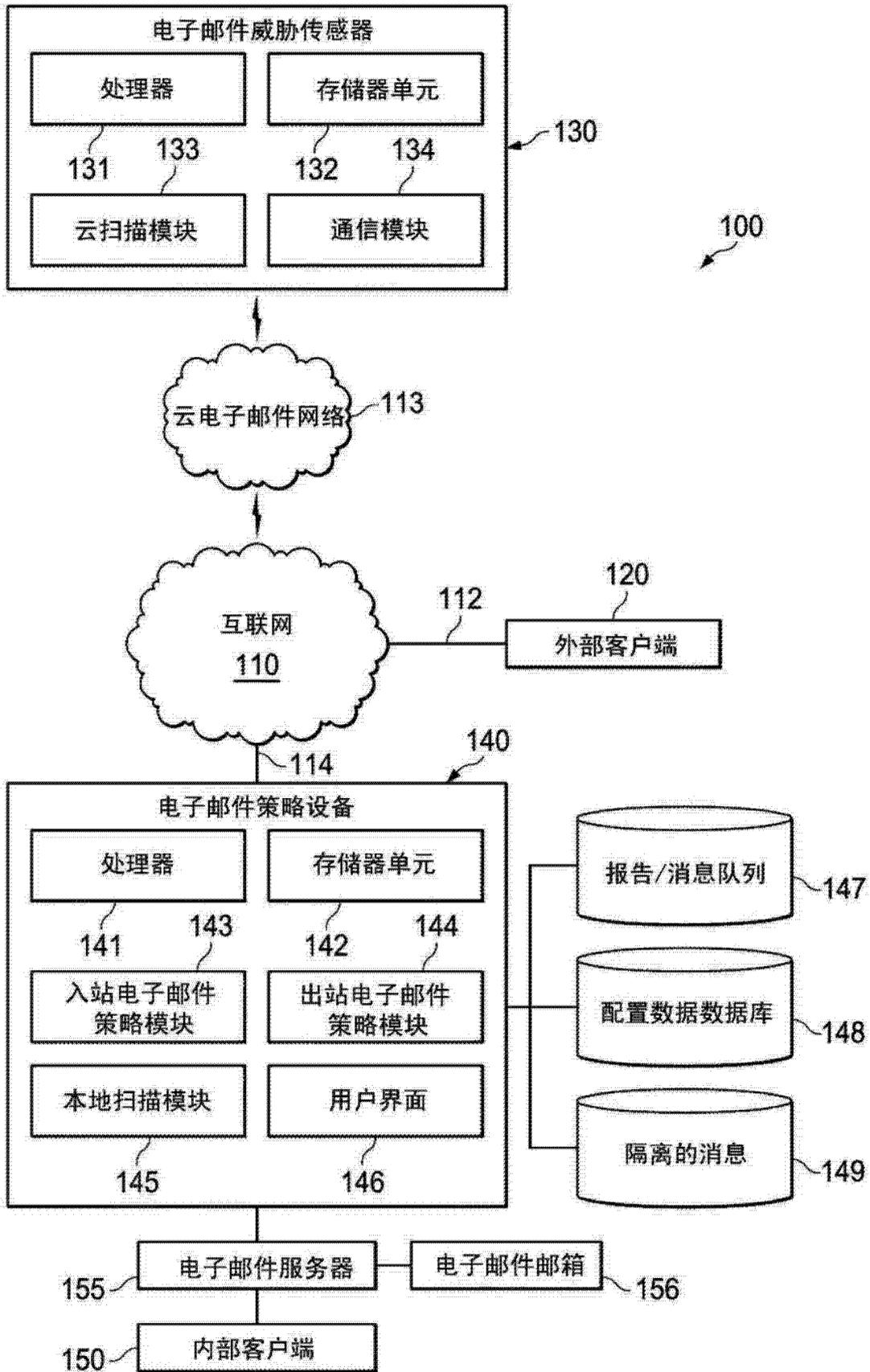


图 1

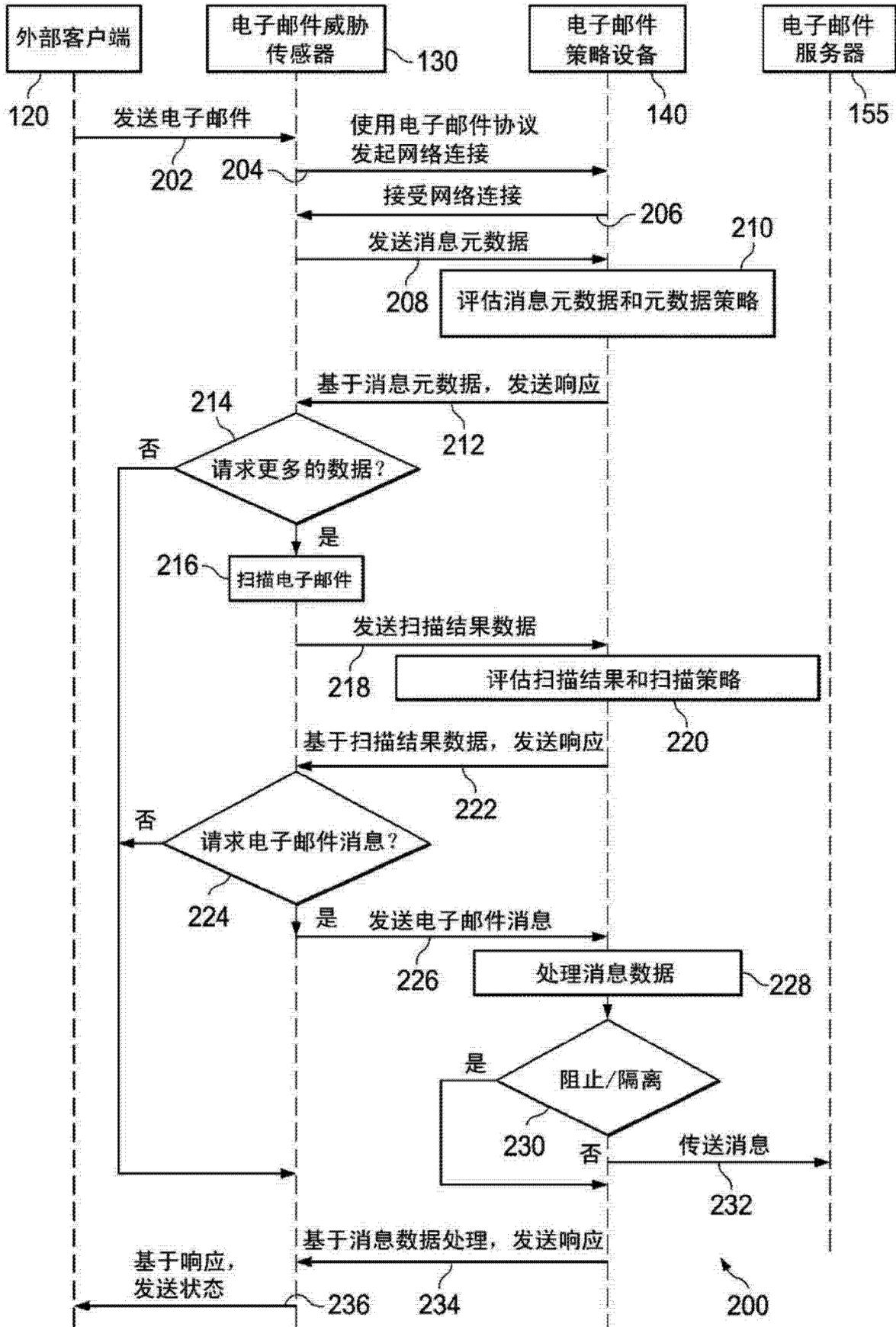


图 2

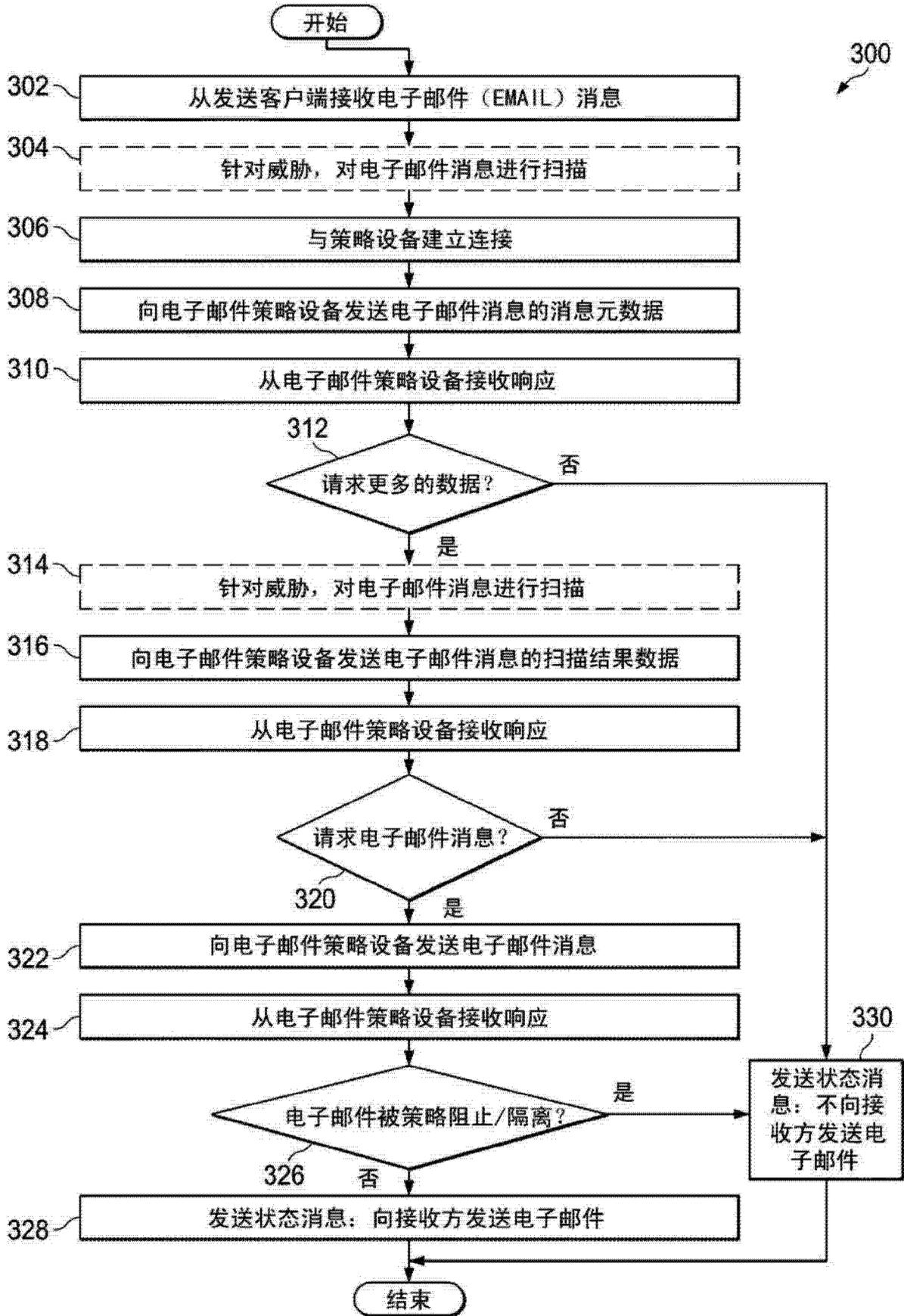


图 3

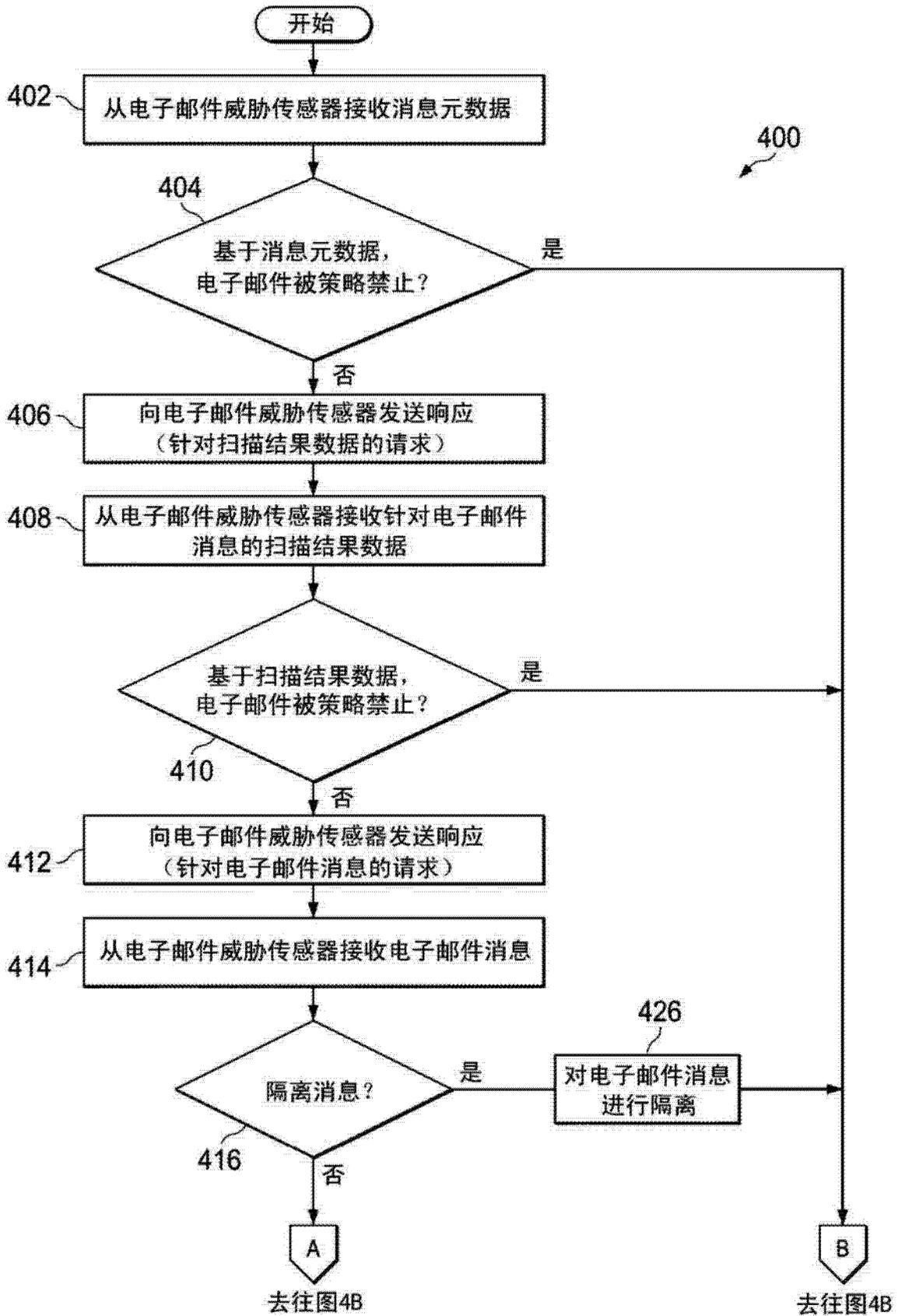


图 4A

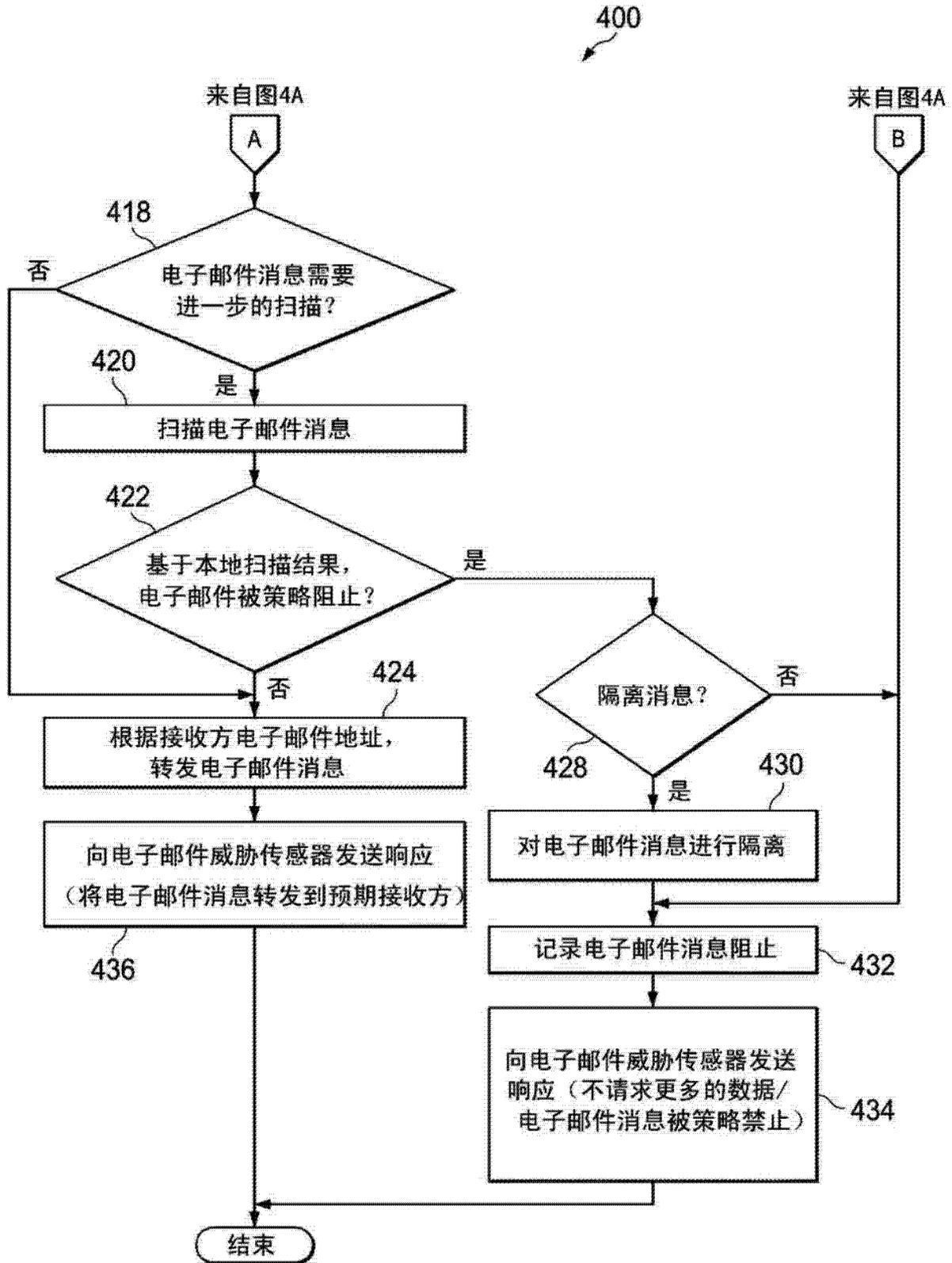


图 4B

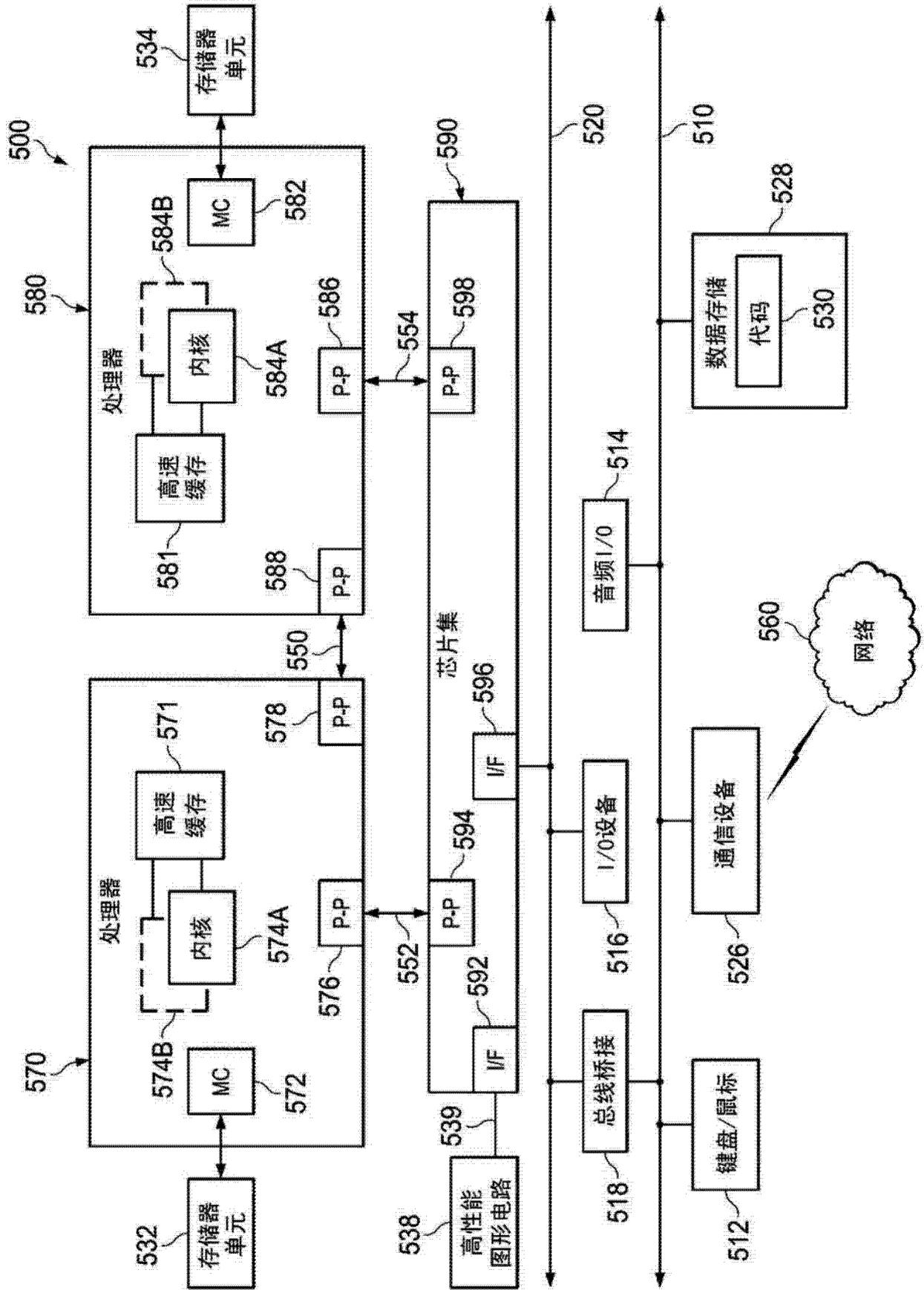


图 5

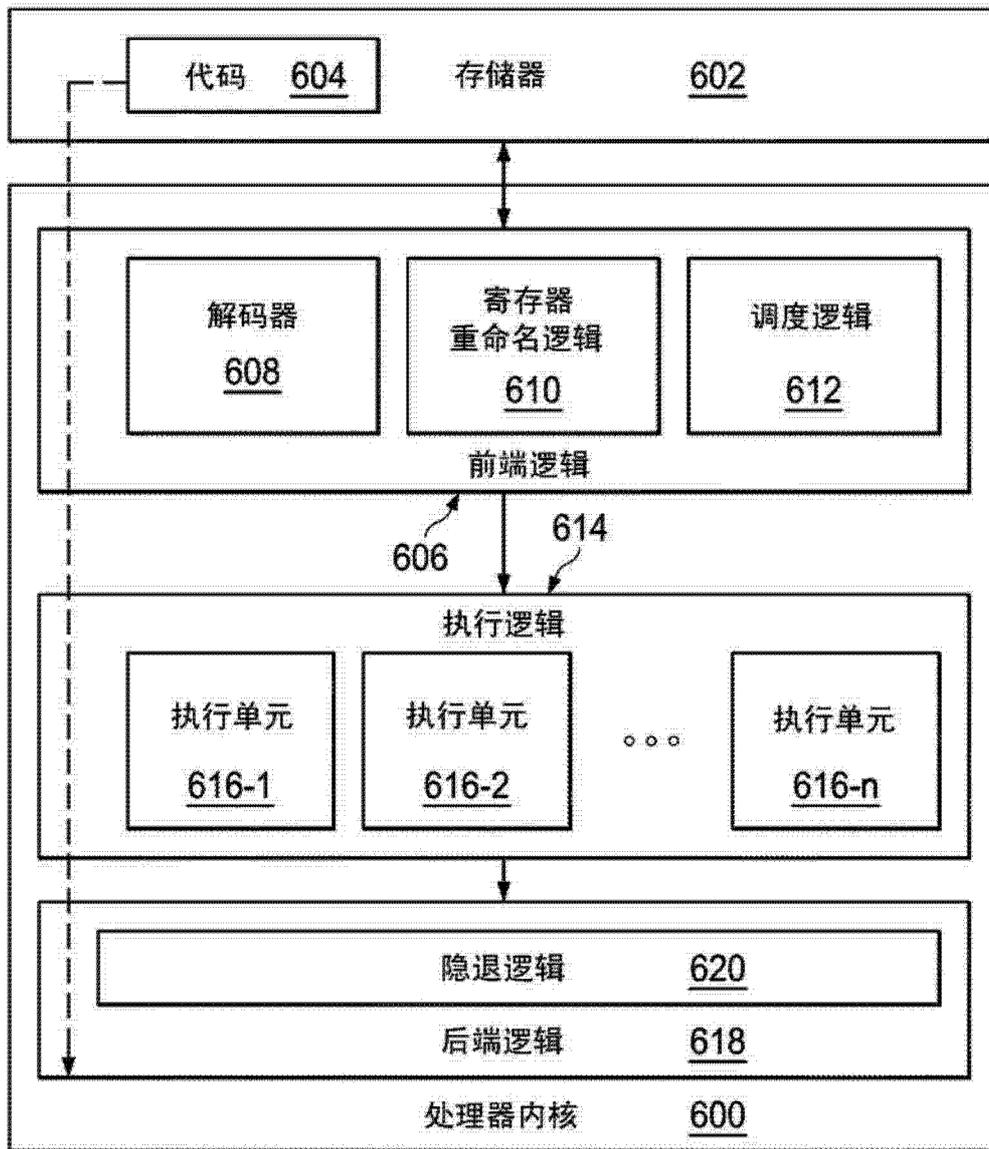


图 6