(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113098758 B
(45)授权公告日 2022.10.18

(21)申请号 202110335805.1

(22)申请日 2021.03.29

(65)同一申请的已公布的文献号
申请公布号 CN 113098758 A

(43)申请公布日 2021.07.09

(73)专利权人 河北白沙烟草有限责任公司
地址 052165 河北省石家庄市珠江大道366号

(72)发明人 高萍 吕亚楠 刘冬梅

(74)专利代理机构 石家庄新世纪专利商标事务所有限公司 13100
专利代理师 董金国 黄敬霞

(51)Int.Cl.
H04L 51/04(2022.01)
H04L 51/23(2022.01)
H04L 9/40(2022.01)
H04L 67/02(2022.01)

审查员 杨金雪

权利要求书2页 说明书11页 附图8页

(54)发明名称

一种基于企业微信的企业消息推送安全网关系统

(57)摘要

本发明公开了一种基于企业微信的企业消息推送安全网关系统，属于企业信息安全管理领域，其包括：第一处理模块用于接收企业应用推送的第一消息，并创建该第一消息的第二消息；消息管理模块，用于根据管理请求管理第二消息的消息缓存；第二处理模块用于读取消息缓存的第二消息，并根据一个或者多个推送规则调用域外接口向域外服务器发送包含该第二消息全部或者部分参数信息的第三消息；其中，仅第三消息包含企业微信账户的接口密钥。本发明作用在于面对跨信息域的接口调用时，一个信息域内的多个应用只能通过本发明的安全网关系统安全推送规则向另一个信息域的服务提供方推送消息，以实现跨域信息安全。

CN 113098758 B

1.一种基于企业微信的企业消息推送安全网关系统,其特征在于,包括:

第一处理模块,用于接收企业应用推送的第一消息,并根据所述第一消息的全部或者部分参数信息对该第一消息进行鉴权,如果鉴权结果为真,则创建该第一消息的第二消息,并根据预配置的消息模板将第一消息中的部分信息段内容翻译重写为第二消息中部分内容;

消息管理模块,用于根据管理请求管理所述第二消息的消息缓存;以及

第二处理模块,用于读取所述消息缓存的第二消息,并根据一个或者多个推送规则调用企业微信服务器上企业微信账户提供的接口向企业微信服务器发送包含该第二消息全部或者部分参数信息的第三消息;

其中,仅第三消息包含所述企业微信账户的接口密钥。

2.根据权利要求1所述的系统,其特征在于,所述第一处理模块,具体用于:

提供一内部消息推送接口,以便所述企业应用通过调用该消息推送接口向所述第一处理模块推送所述第一消息;

所述第一消息的参数信息包含其企业应用的应用ID、用于推送消息的消息模板ID和该消息推送接口的接口授权码。

3.根据权利要求1所述的系统,其特征在于,所述企业微信服务器上企业微信账户提供的接口包括企业微信消息推送服务的外部消息推送接口。

4.根据权利要求1所述的系统,其特征在于,所述第一处理模块,还用于,根据所述第一消息的应用ID和消息模板ID对所述第一消息进行鉴权。

5.根据权利要求1所述的系统,其特征在于,所述第二处理模块,还用于,

读取所述消息缓存的第二消息,并根据一个或者多个推送规则调用外部服务器上SaaS服务提供的接口向所述外部服务器发送包含该第二消息全部或者部分参数信息的第四消息;所述第四消息包含被所述第三消息引用的数据内容;

其中,仅第四消息包含所述SaaS服务的接口密钥。

6.根据权利要求1所述的系统,其特征在于,所述第二处理模块推送第三消息的规则包括:对所述第二消息的内容进行检查的内容规则,和/或,确定所述第三消息的推送时间的时间规则。

7.根据权利要求1所述的系统,其特征在于,其还包括:

用于消息模板、应用接入、禁用词设置、消息模板授权、消息发送统计及发现日志查询的后台管理系统;以及,用于消息炸弹防护的消息推送计数器;

推送消息接收人不在所述消息模板配置推送范围内,或,

所述第三消息的消息内容包含禁用词的,

则,

拒绝推送。

8.根据权利要求2所述的系统,其特征在于,所述企业应用需要提供授权的接口密钥才能调用所述内部消息推送接口;或者,所述企业应用按Webservice接口调用规范向所述内部消息推送接口推送第一消息。

9.根据权利要求3所述的系统,其特征在于,所述第二处理模块还用于:

利用Redis的原子计数器,判断一段时间内接收的第二消息数超过预设值时对自身调

用所述外部消息推送接口的行为进行拦截。

10.根据权利要求9所述的系统,其特征在于,所述第二处理模块还用于:

根据一消息推送监听器的触发,将所述消息接收人的所述原子计数器加1,并判断返回值是否超过预设值,如果未超过,取出第二消息中推送企业微信账号ID、应用ID,循环调用企业微信API获取AccessToken并向该消息接收人推送所述第三消息。

一种基于企业微信的企业消息推送安全网关系统

技术领域

[0001] 本发明涉及企业信息安全管理领域,特别是一种基于消息推送系统架构的企业网关。

背景技术

[0002] 企业微信是腾讯(Tencent)基于微信(WeChat)构建的一套企业通讯与办公平台工具。其提供了开发者接口,企业可以基于业务场景建立各种企业微信的应用来实现价值链升级、服务升级以及生态构建,这类应用最重要的功能是实现待处理工作的实时提醒、提升员工工作便捷性,帮助实现企业组织效率的提升。在面对复杂的企业方组织结构时,大型企业中企业微信的直接管理者与建立在该企业微信的应用的管理者不能实现同等的可信任等级,当需要以企业微信账号管理者身份中对构建于其域内的应用与域外的微信服务器的双向通信进行管理时,如果让各应用自行接入企业微信,接口密钥(Access Token)容易泄露;如果利用接口下发高级管理规则,再由应用自己处理,规则信息的泄露会给企业带来信息安全风险;如果一个应用因其本身程序BUG或错误操作在短时间内推送大量的信息到企业员工所使用终端上,会给员工造成生活上的干扰,难免影响其他应用的消息也会被淹没而影响其正常功能。

[0003] 中国专利申请201810886043.2公开了一种基于企业微信的消息推送方法,具体包含以下步骤:创建消息模板、设定消息的触发条件、在满足触发条件,则自动将相应的消息发送消息到客户端、企业微信调用接口发送消息、客户端接收到消息,并返回接收状态反馈信息。该发明的基于企业微信的消息推送方法,可以实现自动触发消息的推送,并且能够给不同的人发送不同的消息内容。然而,其技术方案并未涉及如何实现具体的消息转发规则。

发明内容

[0004] 本发明目的在于解决使用企业微信时,涉及多层级管理的多应用接口的消息推送时,如果存在高级别管理规则时,如何在不泄露该规则信息的情况下,对多应用进行满足该规则的广播消息进行管理。

[0005] 本发明提供的技术方案是一种基于企业微信的企业消息推送安全网关系统,包括:

[0006] 第一处理模块,用于接收企业应用推送的第一消息,并根据所述第一消息的全部或者部分参数信息对该第一消息进行鉴权,如果鉴权结果为真,则创建该第一消息的第二消息;

[0007] 消息管理模块,用于根据管理请求管理所述第二消息的消息缓存;以及

[0008] 第二处理模块,用于读取所述消息缓存的第二消息,并根据一个或者多个推送规则调用企业微信服务器上企业微信账户提供的接口向企业微信服务器发送包含该第二消息全部或者部分参数信息的第三消息;

[0009] 其中,仅第三消息包含所述企业微信账户的接口密钥。

[0010] 进一步的,所述第一处理模块,具体用于:

[0011] 提供一内部消息推送接口,以便所述企业应用通过调用该消息推送接口向所述第一处理模块推送所述第一消息;

[0012] 所述第一消息的参数信息包含其企业应用的应用ID、用于推送消息的消息模板ID和该消息推送接口的接口授权码。

[0013] 进一步的,所述企业微信服务器上企业微信账户提供的接口包括企业微信消息推送服务的外部消息推送接口。

[0014] 进一步的,所述第一处理模块,还用于,根据所述第一消息的应用ID和消息模板ID对所述第一消息进行鉴权。

[0015] 进一步的,所述第二处理模块,还用于,

[0016] 读取所述消息缓存的第二消息,并根据一个或者多个推送规则调用外部服务器上SaaS服务提供的接口向所述外部服务器发送包含该第二消息全部或者部分参数信息的第四消息;所述第四消息包含被所述第三消息引用的数据内容;

[0017] 其中,仅第四消息包含所述SaaS服务的接口密钥。

[0018] 进一步的,所述第二处理模块,推送第三消息的规则包括:对所述第二消息的内容进行检查的内容规则,和/或,确定所述第三消息的推送时间的时间规则。

[0019] 进一步的,该系统其还包括:

[0020] 用于消息模板、应用接入、禁用词设置、消息模板授权、消息发送统计及发现日志查询的后台管理系统;以及,用于消息炸弹防护的消息推送计数器;

[0021] 推送消息接收人不在所述消息模板配置推送范围内、所述消息内容包含禁用词的拒绝推送。

[0022] 进一步的,所述企业应用需要提供授权的接口密钥才能调用所述内部消息推送接口。或者,所述企业应用按Webservice接口调用规范向所述内部消息推送接口推送第一消息。

[0023] 进一步的,所述第二处理模块还用于:

[0024] 利用Redis的原子计数器,判断一段时间内接收的第二消息数超过预设值时对自身调用所述外部消息推送接口的行为进行拦截。

[0025] 进一步的,所述第二处理模块还用于:

[0026] 根据一消息推送监听器的触发,将所述消息接收人的所述原子计数器加1,并判断返回值是否超过预设值,如果未超过,取出第二消息中推送企业微信账号ID、应用ID,循环调用企业微信API获取Access Token并向该消息接收人推送所述第三消息。

[0027] 本发明技术方案能够在企业内部网络各个企业应用需要同时连接企业微信账户时,提供一个统一的消息管理平台,实现完整的内外消息传递的高效隔离,在变更消息管理规则时,只需要统一调整第二处理模块的推送规则,而内部的企业应用无需各自分别调整,并且也不必了解具体的推送规则,即由第一处理模块同提供的内网的接口下,全部企业应用不必直接连接外网即可使用企业微信的相关功能,实现了严格分级的企业信息安全管理。

附图说明

[0028] 图1为现有技术中企业微信的接口调用方法的示意图；

[0029] 图2为本发明一个实施例的企业消息推送安全网关系统的结构示意图；

[0030] 图3为本发明一个实施例的企业消息推送安全网关系统的安全网关服务器的组件部署示意图；

[0031] 图4为本发明一个实施例的企业消息推送安全网关系统的安全网关服务器的组件调用关系示意图；

[0032] 图5为本发明另一个实施例的企业消息推送安全网关系统的安全网关服务器的组件调用关系示意图；

[0033] 图6为本发明一个实施例的企业消息推送安全网关系统的软件架构示意图；

[0034] 图7为本发明一个实施例的企业消息推送安全网关系统的消息推送方法的流程图一；

[0035] 图8为本发明一个实施例的企业消息推送安全网关系统的消息推送方法的流程图二；

[0036] 图9为本发明一个实施例中第一消息、第二消息和第三消息的数据转换示意图。

具体实施方式

[0037] 首先需要说明的是，参考图1的，现有技术中，运行于应用服务器的各个企业应用(应用1、应用2……)各自分别根据腾讯公司在其企业微信服务器上提供的微信消息推送服务所提供的外部消息推送接口使用企业微信的SaaS产品。对于一个企业微信账户，分配有用于账户身份识别的Access Token，在调用该接口(Interface，如API)时，需要给出该Access Token。Access Token及与企业微信账户相关的信息被配置于各个企业应用中，以便在各自不相关的需要消息推送时调用相应的外部消息推送接口提供的接口资源。这至少产生了一个问题，对于大型企业而言，其应用数量较大，单一应用的信息安全风险将被应用总量放大，比如，在相同管理机制下的安全风险，一个应用出现问题的概率如果是0.1，那么对于存在10个应用的情况，出现问题的则成为必然。可以理解的，实际场景中，各个应用并必须运行于同一应用服务器，对于涉及分布于不同地点及环境的应用服务器，大型企业在使用企业微信类外部SaaS服务时将面临更大的总体安全风险。中国专利申请201810886043.2公开的关于基于企业微信的消息推送方法的多个技术方案，其可以实现自动触发消息的推送，并且能够给不同的人发送不同的消息内容。该技术方案并未被主张用于解决多应用下企业微信的安全问题。然而，该公开中，创建的模板是指预先设定好消息内容，然后通过该平台定时或事件推送的模板，并没有面向企业开发的内部应用系统提供统一的消息推送服务和安全接入以实现一种内容等安全信息的审核和隔离。本申请的第一处理模块中根据第一消息中携带的消息模板ID所调用的消息模板，包含该消息模板可以推送的企业微信等外部服务器的SaaS服务，并限定了哪些企业内部应用可以通过该模板进行消息推送，以实现一个面向第三方面应用开发商的内部消息推送接口，在任何内部消息推送接口不慎被人恶意调用发送消息炸弹或者违规消息可以及时拦截进而实现跨信息域的信息安全。本文中，信息域指信息被隔离划分后所分配的网络安全域，在一个信息域中的信息可以自由流通，信息域也包括虚拟安全域，网络安全域的划分可以是或者不是与网络路由

的网段划分重合的。

[0038] 下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，旨在用于解释本发明，而不能理解为对本发明的限制。

[0039] 下面参考附图描述本发明实施例的基于企业微信的企业消息推送安全网关系统。

[0040] 图2是根据本发明一个实施例的企业消息推送安全网关系统(以下简称安全网关系统)的结构示意图。

[0041] 本实施例中，基于企业微信的企业消息推送安全网关系统，包括设置在内部网络的第一处理模块110、消息管理模块120和第二处理模块130。第一处理模块110、消息管理模块120和第二处理模块130之间由包括接口调用在内的数据耦合关系，对于安全网关系统，第一处理模块110、消息管理模块120和第二处理模块130可以部署于一个或者多个具体设备。在本发明的多个实施例中，第一处理模块110为域内企业应用提供内部消息推送接口，但企业应用不限于内部网络应用，本发明的域内和域外包括但不限于内部网络和外部网络这样的网络拓扑概念，更具体的说，域内和域外是指，对于具体的接受管理的信息数据，可以根据级别被分为若干信息流通区域，在一个信息流通区域内信息数据具有同等的管理级别，同管理级别的信息数据之间称为域内信息，其他管理级别的信息数据称为本管理级别信息数据的域外信息数据，本发明的安全网关系统的一个作用在于管理跨信息流通区域之间的信息数据的交互，阻止不合法的跨域信息数据交互，并且将相应的阻止规则限制于安全网关系统内部，通过独立的管理实现一个较高的安全级别。

[0042] 本实施例中，第一处理模块110用于接收企业应用推送的第一消息，并根据第一消息的全部或者部分参数信息对该第一消息进行鉴权，如果鉴权结果为真，即通过该企业应用的身份认证，则创建该第一消息的第二消息。第一处理模块110提供了替代图1中微信消息推送服务所提供的外部消息推送接口的内部消息推送接口，该接口用于在内网中为各个企业应用提供一个统一的接口，各个企业应用使用该接口向第一处理模块110各自的第一消息，第一处理模块110接收到第一消息后，根据一个解析鉴权过程，判断该第一消息是否来自一次合法的调用，健全成功后，根据第一消息的参数信息为第一消息创建其第二消息，第二消息包含了第一消息所体现的通信意图，但采用了与第一消息不同的数据封装形式，这意味着向各个企业应用公开的接口数据结构，实际上并非是在消息管理模块120中真实保存的数据结构。在一个使用强加密的解析方式的示例中，企业应用调用第一处理模块110的接口向其发送的第一消息中有应用ID，这些应用ID可能是可以被其他企业应用所获取的，然而，在安全环境下还为各个企业应用配置了一个私钥，这些应用ID是经过非对称加密的，那么，即使泄露了某个企业应用的应用ID或者第一消息中的其他与鉴权相关的信息，由于未能同时掌握该应用的私钥，也有效的向第一处理模块110发送一个伪造的第一消息，因为虽然第一处理模块110会接受该消息，但是经过解析鉴权后，认为鉴权结果为假，即，调用不合法，则会及时丢弃该第一消息，而防止因为来自一个企业应用的攻击而影响其他大多数企业应用的整体正常功能，实现了攻击过滤。容易理解的，第一处理模块110中，由合法的一个第一消息转化为一个或者多个第二消息的，或者由多个第一消息转化为一个号或者多个第二消息的第二消息生成规则，被用于实现安全网关系统内部的数据处理的真实规则信息与企业应用第一消息的构建规则之间的信息隔离，以防止企业应用或者其他第三方获得

安全网关系统内部的推送规则的信息。

[0043] 消息管理模块120用于根据管理请求管理第二消息的消息缓存。本实施例中，在消息管理模块120中可以管理至少一个全部第二消息数据的消息缓存区块，这些第二消息由第一处理模块110根据通过鉴权的第一消息解析生成，并根据消息管理模块120提供的数据结构进行临时存储，以备由第二处理模块130根据其推送规则实时处理。一些实施例中，消息管理模块120对该消息缓存的管理使用以第一处理模块110为生产者，第二处理模块130为消费者的任务处理模式，典型的一个示范是，先进先出的队列形式。对于配置有并行处理规则的第二处理模块130，可以为消息管理模块120配置多进多出的消息缓存，以提高数据交换效率，因此消息缓存的数据结构不限于队列等简单堆栈结构。一些实施例中，外部网络中企业微信服务器，或者其微信消息推送服务。或者微信消息推送服务的外部消息接口并不限于一个，作为消息缓存的一种形式，由消息管理模块120管理的第二消息的缓冲池为第二处理模块130提供了更灵活的监听接口。

[0044] 第二处理模块130用于读取消息管理模块120的消息缓存中的第二消息，并根据一个或者多个推送规则调用企业微信服务器上企业微信账户提供的接口向企业微信服务器发送包含该第二消息全部或者部分参数信息的第三消息。一个简单的示范中，与第一消息和第二消息必须是有区别的这一点不同，一个第三消息可以直接是一个第二消息的全部信息。在一些较复杂的示范中，第一消息包含了数据量较大的图片、声音、视频等参数信息，意图存储于微信素材服务器，然后通过另外的第一消息对其进行调用，即意图通过多个第一消息拼接出包含完整上下文的信息，信息中可能包含较大数据。因此，参考图5的一个具体示范中，第二处理模块130的一个推送规则是，对于并非指向企业微信服务器的第一消息，第二处理模块130可以根据其指定方向，将其携带的信息内容携带于第四消息向指定设备推送，调用域外的外部服务器上SaaS服务提供的接口，如域外的微信素材服务器通过素材库提供的素材管理接口，但是，这些指定的数据传输方向对企业应用来说仍然是被隔离的。在该示范中，仅第三消息包含所述企业微信账户的接口密钥，仅第四消息包含所述SaaS服务的接口密钥，对于各个企业应用并不掌握这些接口密钥。

[0045] 图3给出了本实施例的一个示例中，内部消息推送服务作为第一处理模块110的程序指令模块，消息队列管理器作为消息管理模块120的程序指令模块，消息推送监听服务作为第二处理模块130的程序指令模块，被部署于同一安全网关服务器。容易理解的，在另一些实施例中，使用这些服务进程可以分散的部署于不同的服务器上，运行这些服务进程的服务器共同组成本发明的安全网关系统。

[0046] 参考图3、4的，在本发明的一个具体示例中，安全网关服务器上运行安全网关软件系统，安全网关软件系统包括实现本发明各个模块程序指令。安全网关软件系统包括三个层级：外部应用、消息推送服务和后台管理。其中，后台管理包括应用接入管理、禁用词管理、消息模板管理、消息发送统计、消息发送日志等功能模块，后台管理层功能由Web服务器提供，为消息推送服务层提供基础的推送规则相关的配置信息和查询服务。消息推送服务层，用于实现第一处理模块110、消息管理模块120、第二处理模块130的程序模块，其包括消息推送对内服务API服务，消息推送对外API服务，使用RocketMQ实现的消息队列管理器，使用Redis实现的消息推送计数器等程序模块。外部应用即企业应用和饥饿腾讯提供的企业微信SaaS平台提供的腾讯微信API服务，具体的，本示例中企业应用全部位于内部网络，即

均为企业内部应用。

[0047] 如图7所示的,根据安全网关软件系统的三个层级,安全网关软件系统实现了一种企业微信消息安全推送方法,在现有腾讯微信消息推送接口基础上开发供企业内部应用使用,可安全、快速的推送消息到移动端,其包括以下过程:

[0048] 步骤S1,设置消息推送调用方应用、调用接口密钥。在作为消息推送调用方的企业应用中设置其应用ID,以及第一处理模块的调用内部消息推送接口的接口密钥。

[0049] 一个具体示范的,步骤S1中,后台管理系统具有应用配置模块,添加调用消息推送Webservice接口的应用名称,接口调用密钥。

[0050] 一个具体示范的,步骤S1中,由系统管理员在企业应用接入管理模块中添加企业内部应用名称、调用对内接口授权码。

[0051] 步骤S2,建立消息模板,设置消息类型、数据来源参数、推送企业微信账号、企业微信应用ID、推送人员范围、可调用应用、是否启用禁用词管理。

[0052] 一个具体示范的,步骤S2中,由系统管理员在消息模板管理添加模板名称、推送人员范围,可选择具体人员或部门,选择推送的微信公众号或企业微信应用。

[0053] 一个具体示范的,步骤S2中,后台管理系统具有消息模板管理模块,添加模板名称、消息连接地址、消息内容、消息格式(文本、图片、文本卡片、文件)、推送人员范围、推送目标微信账号、是否开启禁用词过滤。

[0054] 一个具体示范的,步骤S2中,添加的字段值可引用系统提供的预定义变量,包括:

[0055] $msg_id 发送方消息记录ID,自定义消息地址时使用

[0056] $title 消息标题

[0057] $link 消息点击跳转地址

[0058] $content 发送消息内容

[0059] $media_id 上传到微信平台的图片、文件id

[0060] 步骤S3,维护禁用词词库。禁用词词库是一种内容规则库。可以通过后台管理的交互界面对禁用词词库进行管理。示范的,由系统管理员在禁用词管理模块添加禁用词短语实现一个内容规则库的管理操作。

[0061] 步骤S4,调用方调用对内消息推送Webservice接口,参数包括:调用方应用ID、访问密钥、推送内容、跳转链接、推送人员工号、使用的消息模板.

[0062] 一个具体示例,在步骤S4中,企业内部应用调用消息推送对内API服务,以JSON格式传入参数,包括:调用方应用ID、接口授权码,使用的消息模板ID,消息标题、消息内容、消息连接、图片URL、文件(Base64),接收人工号,JSON格式示例如下:

[0063]
```
{
    "app_id": "",
    "app_key": "",
    "msg_template_id": "",
    "title": "",
    "content": "",
    "url": "/xtpt/view/&id=12345",
    "pic_url": "",
```

[0071] "file": "",

[0072] "rec_staff_num": ""

[0073] }

[0074] 步骤S5,对内消息推送Webservice收到推送数据后,判断访问密钥是否正确,判断调用方应用是否授权使用消息模板,判断推送人员是否在消息模板设置的推送人员范围内,如果校验失败拒绝发送,否则将数据写入消息队列并返回消息发送回执号给调用方。示范的,第一处理模块的内部消息推送服务对检查调用方接口密钥是否正确,是否授权使用消息推送模板,推送人员是否在模板授权的人员范围内,并将推送消息内容放入消息队列,返回消息推送状态查询回执号给调用方。

[0075] 步骤S6,对外消息推送监听器触发后,从消息队列取出推送数据,根据推送人员工号将Redis计数器加1,并判断返回值是否超过预设值,如果未超过,取出消息模板设置值,如果开启禁用词过滤,通过分词器解析推送内容,判断是否包括敏感词,如果存在拒绝发送。取出消息模板设置的推送企业微信账号ID、应用ID,循环调用企业微信API获取Access Token并发送推送数据,记录API返回结果。

[0076] 一个具体示例中,步骤S6中,消息推送监听服务的消费者监听器从消息队列获取推送消息,将消息计算器+1,并判断是否超过预设值,如果没有获取到消息计算器,根据职工号创建计算器,失效时间为预设的分钟数。如果消息开启禁用词过滤,将消息内容进行分词,并判断分词是否在设置的敏感词中,调用腾讯微信平台提供的API发送消息到接收人移动端上。

[0077] 一个具体实例中,步骤S6中,提前准备好停用词库;对消息内容进行清洗,把特殊的标点符号去除;通过HanLP开源库对清洗后的消息进行分词;将分词与停用词库进行比对,如果存在匹配结果就拦截。

[0078] 步骤S7,调用方根据回执号查询消息推送结果。一个具体示例中,企业内部应用作为第一处理模块内部消息推送接口的调用方,获得该调用返回的回执号,然后根据第一处理模块的查询接口以该回执号为参数查询其对应第一消息的推送状态。一个优选的示例中,第一消息的推送状态信息包括其对应的第三消息在第二处理模块的推送状态信息。

[0079] 上述企业微信消息安全推送方法的各个示例的一个方面的改进示例中,所述基于企业微信消息安全推送方法还包括以下过程:消息推送Webservice接口检查推送消息类型如果为文件、图片类型则将传入的URL参数进行Base64转码,并上传到模板对应的微信账号,保存返回的media_id,并将其他传入参数分别赋值给预定义变量($title,$link,$content,$media_id)用实际值替换消息模板中的占位符。

[0080] 图4示出了安全网关软件系统在消息推送服务层的内部接口调用关系。可以看出,内部消息推送服务为企业内部应用提供了内部消息推送接口,以实现消息推送对内API服务功能;内部消息推送服务在接收到第一消息后,调用消息推送鉴权服务的校验接口对第一消息进行鉴权;消息推送鉴权服务对第一消息鉴权结构为真,即通过鉴权后对发送者身份认证后,内部消息推送服务将该第一消息解析为第二消息,调用消息队里管理器的队列写入服务,将第一消息相关的第二消息放入作为消息缓存的消息队列中;消息推送监听服务,始终根据配置的推送规则从消息队列读取第二消息,并调用外部消息推送接口发送第二消息的第三消息。

[0081] 具体的，本示例消息推送监听服务的推送规则包括：

[0082] 第一规则，即内容规则，调用内容检测模块的内容检测接口对第二消息进行内容检测，仅对通过检测的第二消息进行内容的推送。内容检测模块配置有内容规则库和NLP分词模块，通过对第二消息的文本信息进行分词，并与内容规则库中的内容规则进行匹配，如禁用词等。另一些实施例中，NLP分词模块也可以是其他训练好的神经网络模块，如提供目标识别的图卷积网络模块，内容规则库可以是用于训练神经网络模块的样本集。

[0083] 第二规则，即时间规则，调用消息推送过载保护模块和消息推动计数器模块，检查预设时间内推送的消息树是否超过预设值。其中，消息推送过载保护查询消息推动计数器中近30分钟推送第三消息的数量，如果大于预设值，则认定当前过载，推迟当前要发送的第三消息的时间。消息推送监听服务每发送一条思安消息，则更新消息推送计数器的计数加1，特别的，初次写入首次更新失败时，将计数值设置为一个预设值。

[0084] 图6给出了另一个具体实施例，是一个一种基于企业微信的企业消息推送安全网关系统，与图5示例的区别在于第二处理模块还用于，读取消息缓存的第二消息，并根据一个或者多个推送规则调用外部服务器(微信素材服务器)上SaaS服务提供的接口向外部服务器发送包含该第二消息全部或者部分参数信息的第四消息；第四消息包含被第三消息引用的数据内容；其中，仅第四消息包含SaaS服务的接口密钥。

[0085] 本实施例中，企业内部网络中设有企业应用服务器和安全网关服务器，安全网关服务器还具有跨企业内部网络和外部网络两个网段的路由功能。企业应用服务器上运行有应用1、应用2等企业应用，这些企业应用仅能通过安全网关服务器与外部网络的微信素材服务器和企业微信服务器实现基于消息转发的通信连接。在一个系统配置阶段，企业应用中配置有应用ID、一个或者多个消息模板ID以及第一处理模块所提供内部消息推送接口的接口密钥(也称接口授权码)，接口密钥由其应用ID加盐后经过一个单向哈希获得。企业应用通过调用内部消息推送接口实现其第一消息向指定消息接收人的推送。示范的，一个第一消息中，包含的参数信息包括：应用ID、用于推送本条消息的消息模板ID、接口密钥、消息接收人、消息文本、企业微信消息推送页中的跳转链接、图片、声音、视频等其他数据文件。具体的，第一消息可以是机房在线报警系统向指定若干负责人发送的包含机房报警信息的一个JSON结构数据，本实施例中负责人通过企业微信接收这些机房报警信息。本实施例中第一消息、第二消息、第三消息和第四消息均具是不同的，不同点至少包含JSON结构或者参数值。

[0086] 安全网关服务器包括第一处理模块、消息管理模块和第二处理模块。第一处理模块包括：提供内部消息推送接口的内部消息推送服务、提供校验接口的消息推送鉴权服务、提供应用授权信息接口的应用授权管理模块，以及提供消息模板信息接口的消息模板授权管理模块。

[0087] 消息推送鉴权服务通过调用应用授权信息接口的、消息模板信息接口的实现鉴权服务。内部消息推送服务的内部消息推送接口被调用后，启动一个关于该调用的第一消息的鉴权线程，该线程调用校验接口，以实现根据该第一消息的全部或者部分参数信息对该第一消息进行鉴权。具体的，鉴权方法包括：该企业应用是否有该第一消息中指定的消息模板ID的使用权限；该企业应用本次发送的第一消息中指定的消息接收人，是否在其指定消息模板ID的消息模板的消息接收人清单中。应用授权管理模块和消息模板授权管理模块由

tomcat连接的Oracle数据库实现。调用应用授权信息接口时，调用参数包括该企业应用的应用ID和第一消息中为该企业应用分配的接口密钥。调用消息模板授权管理模块时，调用参数包括该企业应用本次第一消息中消息模板ID、微信端显示的消息类型、推送的企业微信账号或者微信公众账号，以及该第一消息允许接收的消息接收人清单。

[0088] 内部消息推送服务调用校验接口并认可一个第一消息合法后，即接口返回为真，鉴权通过，将该第一消息转化为第二消息。一个转化方法是，将第一消息中参数替换为其消息模板ID指定的消息模板中的预定义变量名，即根据第一消息调用的消息模板，将第一消息转换为第二消息。另一个转化方式是，对于包含大文件的第一消息，作为单独的一帧第二消息并设置一个引用字段，包含第二消息的在缓存队列中的索引号，以便由第二处理模块分别推送。获得第二消息后，内部消息推送服务调用队列写入服务，将第二消息写入消息管理模块的消息队列管理器。本实施例中，消息队列管理器使用RocketMQ实现，其提供了用于监听的API。

[0089] 第二处理模块包括用于保存停用词的内容规则库、提供分词接口的NLP分词模块(如Jieba、HanLP分词等自然语言分词处理模块)、提供内容检测接口的内容检测模块、Redis实现的消息推送计数器、消息推送过载保护检测模块，以及消息推送监听服务。参考图8，示范的，消息推送监听服务通过以下步骤同时实现第一、第二推送规则：

[0090] 步骤S11，监听消息队列管理器的第二消息，如果非空，则读取一条最早的第二消息；调用内容检测接口对第二消息中的内容进行检查，如果不符合要求则丢弃。

[0091] 具体的，以文本为例，内容检测模块被调用后，调用NLP分词模块的接口对第二消息中的内容拆分为单词或者短语，

[0092] 步骤S12，检查预设的时间段内消息接收人收到的消息数量是否大于预设值，若超过预设值，则暂停发送。

[0093] 具体的，该步骤调用消息推送过载保护检测模块，根据其返回的预设时间内推送的消息数与预设值的比较结果，进行判断。具体数值，由消息推送计数器进行根据不同的消息接收人进行存储。

[0094] 步骤S20，如果第二消息中包含图片等大文件，则将其编辑为第四消息，并调用微信素材服务器中素材库的素材管理接口进行上传。

[0095] 步骤S30，将第二消息编辑为第三消息，调用企业微信服务器中微信消息推送服务的外部消息推送接口，推送到指定的企业微信账号、微信公众以及消息接收人。

[0096] 一个示例中，该步骤的第三消息的企业微信账号、微信公众以及消息接收人与第一消息中企业微信账号、微信公众以及消息接收人采用不同的编码方式携带相同的信息。

[0097] 步骤S40，为消息推送计数器中指定的消息接收人的接收消息计数器+1。

[0098] 容易理解，上述过程可以防止个别企业应用出现消息炸弹问题时，实际的消息接收人不受到骚扰，同时保证其他企业应用的正常使用。

[0099] 由上可知，通过本发明的基于企业微信的消息推送方法主要通过对企业微信消息发送平台接口进行二次封装，提供统一的接口，同时在管理后台设定用户管理功能和消息发送管理功能，通过管理者选择需要发送的人员及选择消息发送的模板，或者自定义消息发送内容，并由平台调用封装的接口对消息进行定制化的发送，从而实现供企业内部应用使用，可安全、快速的推送消息到移动端的安全网管系统。

[0100] 可以看出，本发明提供的基于企业微信的企业消息推送安全网关系统，其网关是一种域内信息与域外信息的信息转发设备，可以是或者不是一种内外网之间的路由转发设备。基于上述各个实施例的说明，本发明的安全网关系统一个构思在于，消息模板通过预设一个范本，默认取内部应用给的消息内容，设置好后授权给企业内部应用使用。其一个方面的作用在于面对跨信息域的接口调用时，一个信息域内的多个应用(如企业内部应用)通过本发明的模板翻译体系向另一个信息域的服务提供方(如企业微信，或者其他外部服务器上SaaS服务)推送消息，并通过安全网关系统实现的转发方式对信息进行有效筛选，防止不合规的数据推送和/或实现信息拦截。图9提供了一个具体示例，以进一步描述这种模板翻译体系。该示例中，各个内部应用通过调用第一处理模块110提供的内部消息推送接口向第一处理模块110推送第一消息，第一消息中包含内部应用的应用ID以及所配置的内部接口密钥(接口访问授权码)以证明该推送合法性的认证段，还包含消息标题、消息内容、跳转URL、图片URL、文件(如base64形式大数据量的二进制文件)以及消息接收人列表等信息的信息段；其中信息段还包含一个消息模板ID，第一处理模块在验证第一消息的合法性后，根据消息模板ID调用内部预配置的消息模板，并使用该消息模板，将第一消息中的部分信息段内容翻译重写为第二消息中部分内容，如，将第一消息中的消息标题、消息内容、跳转URL和图片URL重写为第二消息中的消息标题、消息内容、跳转URL和图片URL；同时，消息模板中还包含为该内部应用分配的消息ID、消息类型等不向内部应用公开的配置信息。第一处理模块110作为生产者向消息管理模块120提供第二消息，消息管理模块120对各个第二消息进行缓存管理，等待第二处理模块130作为消费者进行任务处理。第二处理模块130从消息管理模块120读取第二消息，并根据一个或者多个推送规则调用外部服务的接口向外部服务器发送第三消息或者第四消息，其中，第二处理模块130根据第二消息中的消息ID和应用ID，从其连接的数据表中索引出其对应的服务ID(对于公众号可以是AppID，对于企业微信可以是CorpID)以及对应的外部接口密钥(Secret，以获取Access_token)以生成一个第三消息，并将第二消息中文件部分放入一个第四消息另行发送，在第三消息中包含为该文件部分分配的文件ID，以便外部服务进行调用。示范的，重写的翻译方法是预设了一些变量，在消息模板配置中可以使用这些变量拼接想要发送的消息内容。

[0101] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、数据耦合关系或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不是必须针对相同的实施例或示例。而且，描述的具体特征、结构、数据耦合关系或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外，在不相互矛盾的情况下，本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

[0102] 此外，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此，限定有“第一”、“第二”的特征可以明示或者隐含地包括至少一个该特征。在本发明的描述中，“多个”的含义是至少两个，例如两个，三个等，除非另有明确具体的限定。

[0103] 流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或者多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部

分，并且本发明的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本发明的实施例所属技术领域的技术人员所理解。

[0104] 在流程图中表示或在此以其他方式描述的逻辑和/或步骤，例如，用于实现逻辑功能的可执行指令的定序列表，可以具体实现在任何计算机可读介质中，以供指令执行系统、装置或设备(如基于计算机的系统、包括处理器的系统或其他可以从指令执行系统、装置或设备取指令并执行指令的系统)使用，或结合这些指令执行系统、装置或设备而使用。就本说明书而言，"计算机可读介质''可以是任何可以包含、存储、通信、传播或传输程序以供指令执行系统、装置或设备或结合这些指令执行系统、装置或设备而使用的装置。计算机可读介质的更具体的示例(非穷尽性列表)包括以下：具有一个或多个布线的电连接部(电子装置)，便携式计算机盘盒(磁装置)，随机存取存储器(RAM)，只读存储器(ROM)，可擦除可编辑只读存储器(EPROM或闪速存储器)，光纤装置，以及便携式光盘只读存储器(CDROM)。另外，计算机可读介质甚至可以是可在其上打印所述程序的纸或其他合适的介质，因为可以例如通过对纸或其他介质进行光学扫描，接着进行编辑、解译或必要时以其他合适方式进行处理来以电子方式获得所述程序，然后将其存储在计算机存储器中。

[0105] 应当理解，本发明的各部分可以用硬件、软件、固件或它们的组合来实现。在上述实施方式中，多个步骤或方法可以用存储在存储器中且由合适的指令执行系统执行的软件或固件来实现。例如，如果用硬件来实现，和在另一实施方式中一样，可用本领域公知的下列技术中的任一项或他们的组合来实现：具有用于对数据信号实现逻辑功能的逻辑门电路的离散逻辑电路，具有合适的组合逻辑门电路的专用集成电路，可编程门阵列(PGA)，现场可编程门阵列(FPGA)等。

[0106] 本技术领域的普通技术人员可以理解实现上述实施例揭示的方法中包含的全部或部分步骤是可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，该程序在执行时，包括方法实施例的步骤之一或其组合。

[0107] 此外，在本发明各个实施例中的各功能单元可以集成在一个处理模块中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。所述集成的模块如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中。上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0108] 尽管上面已经为了说明本发明的原理而采用的示例性实施方式示出和描述了本发明的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本发明的限制，本领域的普通技术人员在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。这些变化、修改、替换和变型也视为本发明的保护范围。

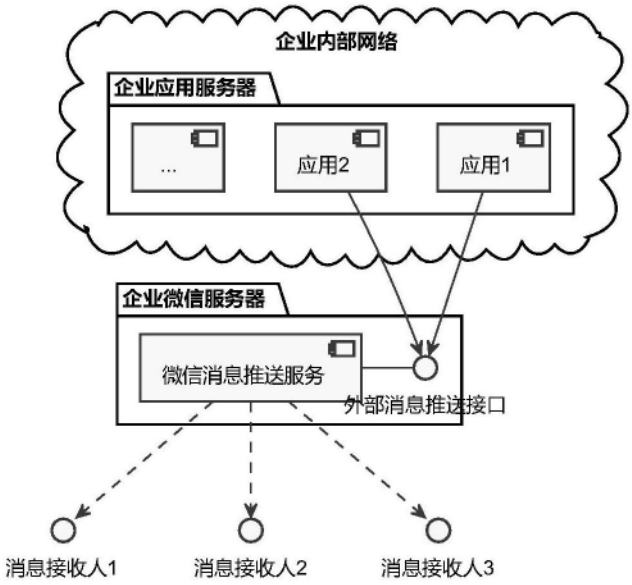
企业内部网络
企业应用服务器
...
应用2
应用1
企业微信服务器
微信消息推送服务
外部消息推送接口
消息接收人1
消息接收人2
消息接收人3

图1


第一处理模块 110
消息管理模块 120
第二处理模块 130

图2

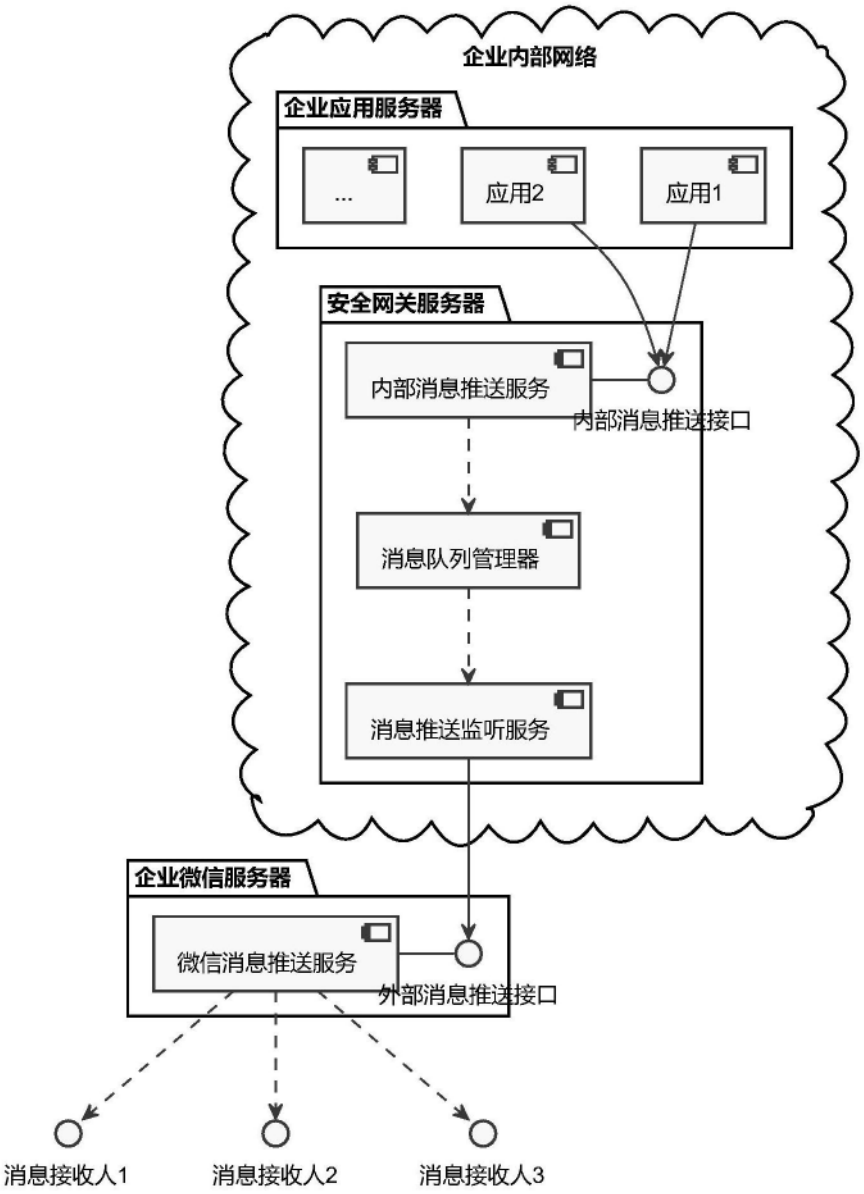
企业内部网络
企业应用服务器
...
应用2
应用1
安全网关服务器
内部消息推送服务
内部消息推送接口
消息队列管理器
消息推送监听服务
企业微信服务器
微信消息推送服务
外部消息推送接口
消息接收人1
消息接收人2
消息接收人3

图3

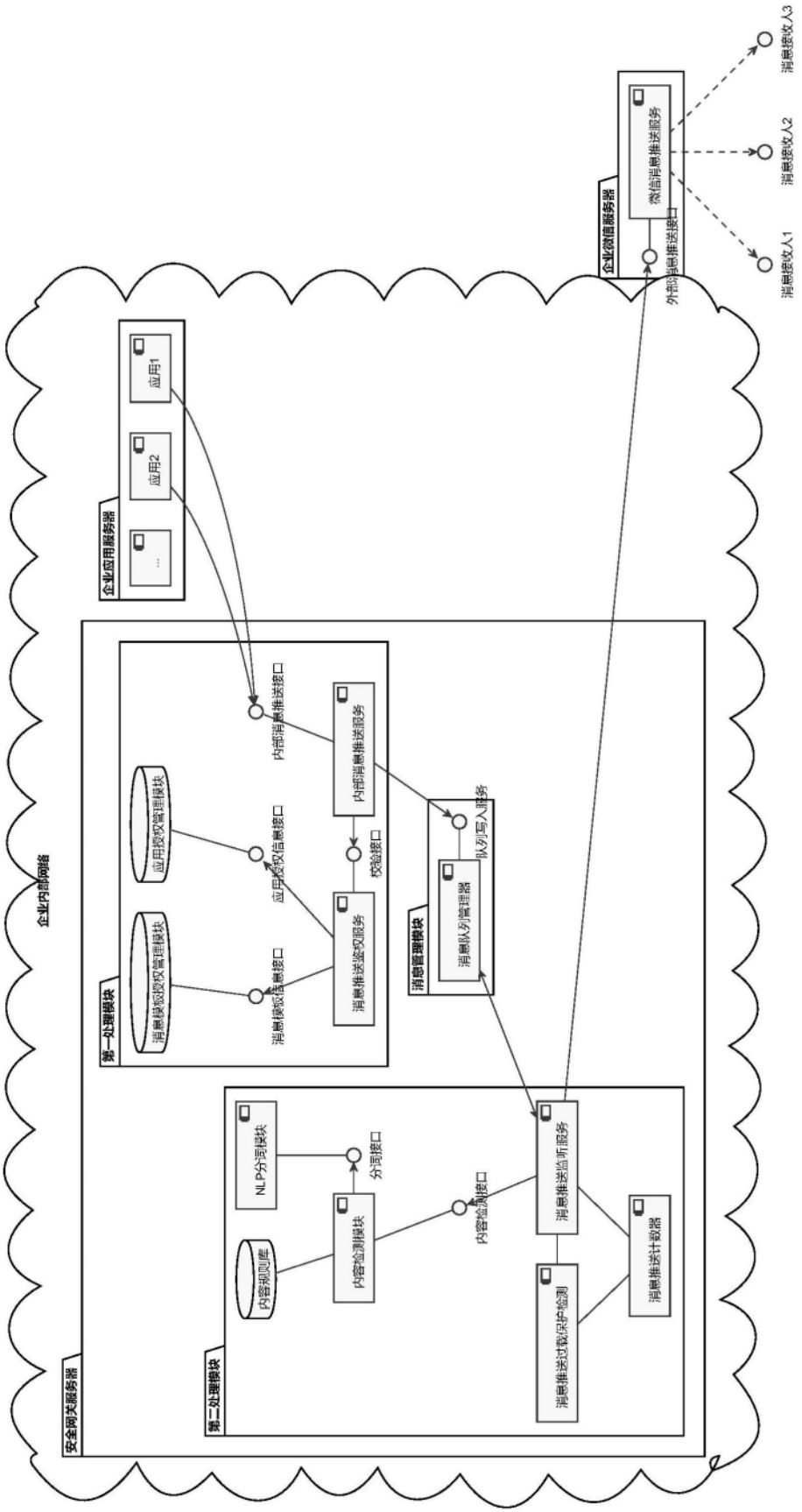
企业内部网络
安全网关服务器
第一处理模块
消息模板授权管理模块
应用授权管理模块
消息模板信息接口
应用授权信息接口
消息推送鉴权服务
校验接口
内部消息推送接口
内部消息推送服务
消息管理模块
消息队列管理器
队列写入服务
第二处理模块
NLP分词模块
分词接口
内容规则库
内容检测模块
内容检测接口
消息推送监听服务
消息推送过载保护检测
消息推送计数器
企业应用服务器
应用1
应用2
...
企业微信服务器
微信消息推送服务
外部消息推送接口
消息接收人1
消息接收人2
消息接收人3

图4

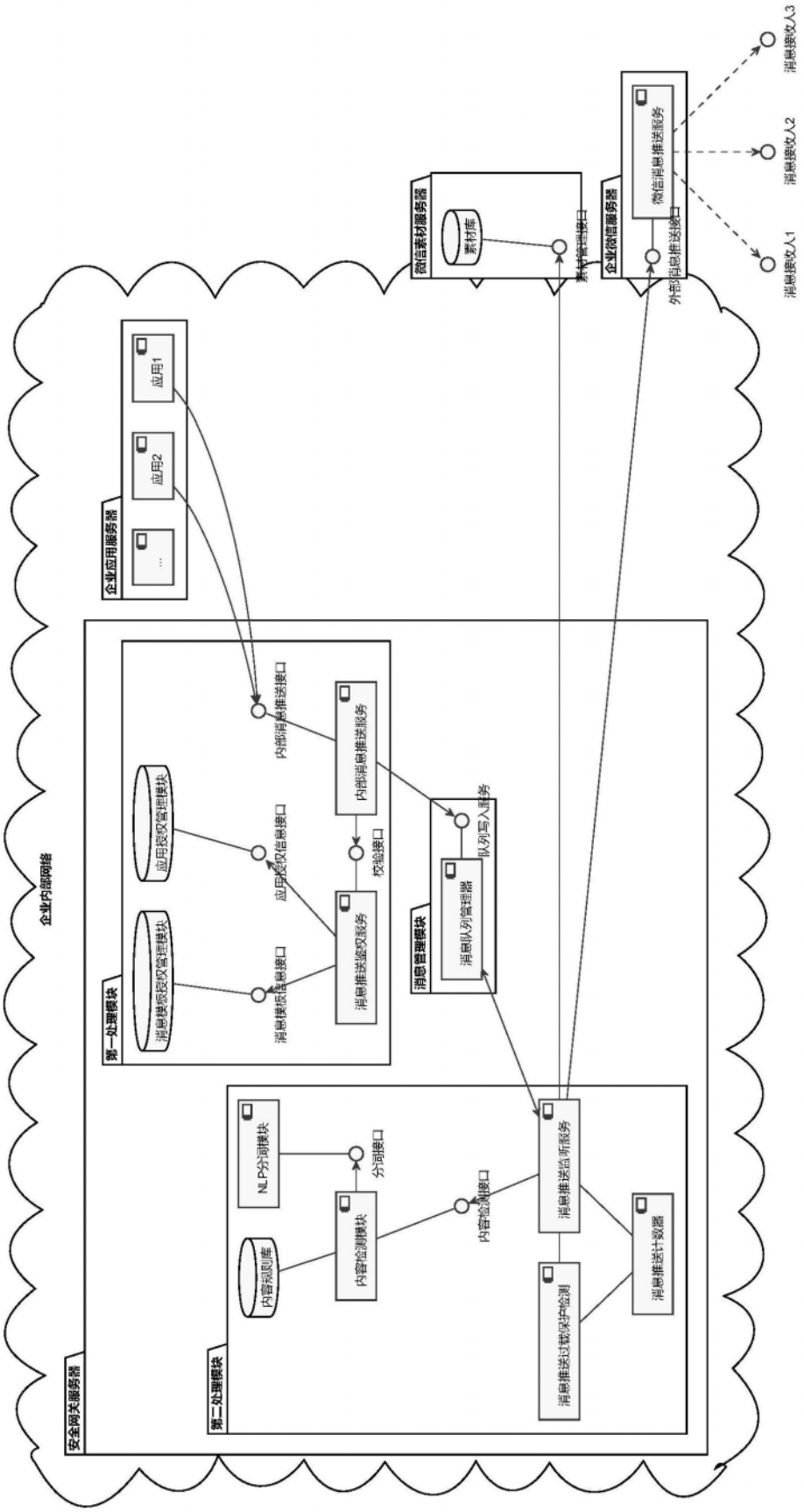
企业内部网络
安全网关服务器
第一处理模块
消息模板授权管理模块
应用授权管理模块
消息模板信息接口
应用授权信息接口
消息推送鉴权服务
校验接口
内部消息推送接口
内部消息推送服务
第二处理模块
NLP分词模块
分词接口
内容预规则库
内容检测模块
内容检测接口
消息推送治理服务
消息推送过载保护检测
消息推送计数器
消息管理模块
消息队列管理器
队列写入服务
企业应用服务器
应用1
应用2
...
微信素材服务器
素材库
素材管理接口
企业微信服务器
微信消息推送服务
外部消息推送接口
消息接收人1
消息接收人2
消息接收人3

图5

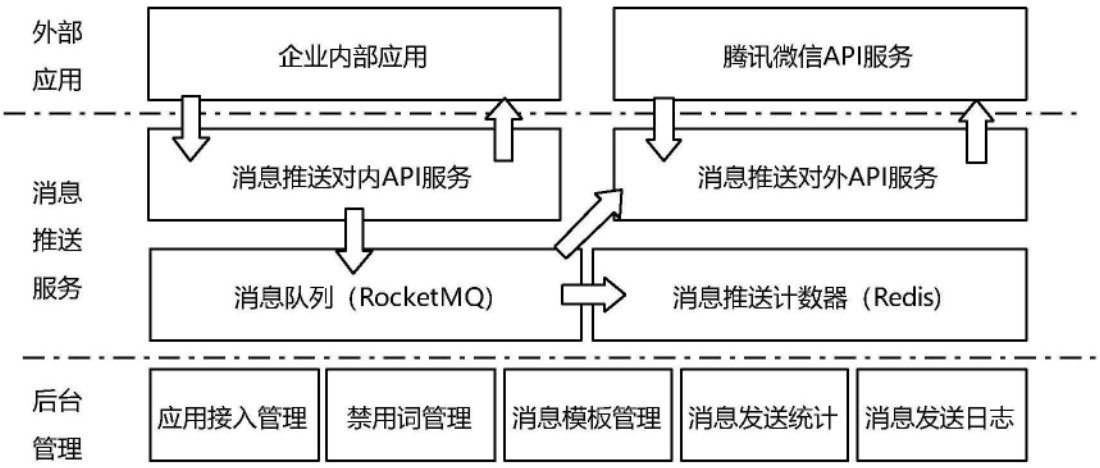
外部
应用
企业内部应用
腾讯微信API服务
消息
推送
服务
消息推送对内API服务
消息推送对外API服务
消息队列（RocketMQ）
消息推送计数器（Redis）
后台
管理
应用接入管理
禁用词管理
消息模板管理
消息发送统计
消息发送日志

图6

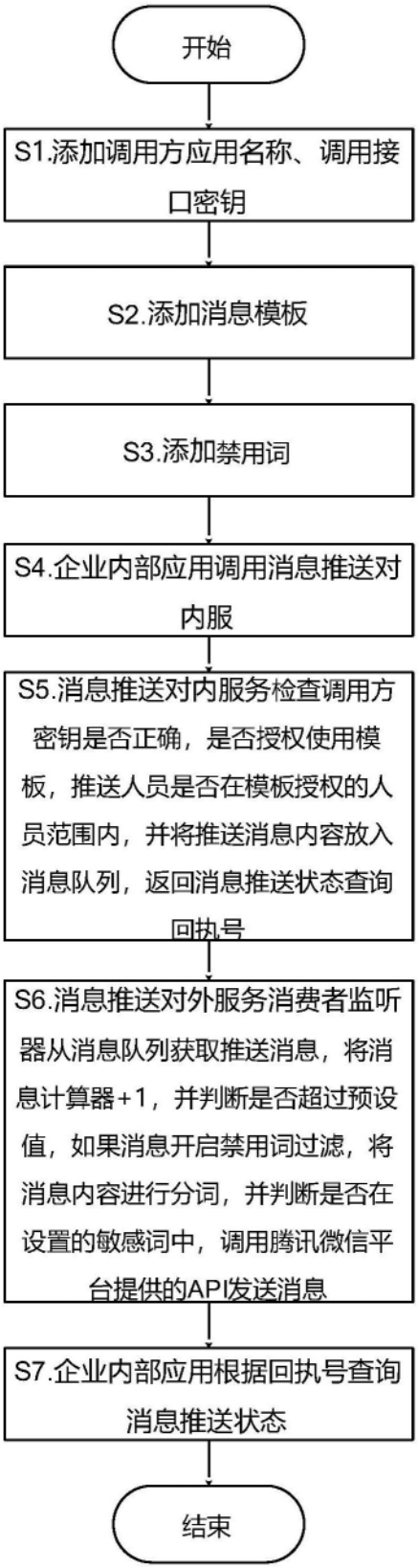
开始
S1.添加调用方应用名称、调用接口密钥
S2.添加消息模板
S3.添加禁用词
S4.企业内部应用调用消息推送对内服
S5.消息推送对内服务检查调用方密钥是否正确，是否授权使用模板，推送人员是否在模板授权的人员范围内，并将推送消息内容放入消息队列，返回消息推送状态查询回执号
S6.消息推送对外服务消费者监听器从消息队列获取推送消息，将消息计算器+1，并判断是否超过预设值，如果消息开启禁用词过滤，将消息内容进行分词，并判断是否在设置的敏感词中，调用腾讯微信平台提供的API发送消息
S7.企业内部应用根据回执号查询消息推送状态
结束

图7

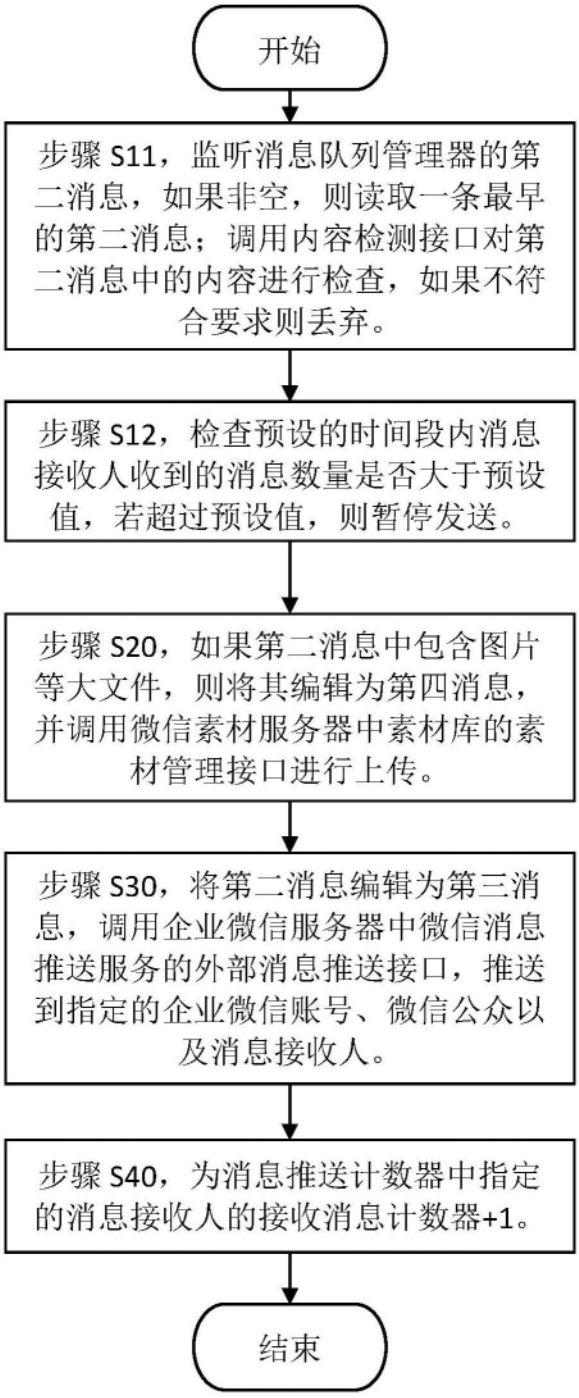
开始
步骤 S11，监听消息队列管理器的第二消息，如果非空，则读取一条最早的第二消息；调用内容检测接口对第二消息中的内容进行检查，如果不符合要求则丢弃。
步骤 S12，检查预设的时间段内消息接收人收到的消息数量是否大于预设值，若超过预设值，则暂停发送。
步骤 S20，如果第二消息中包含图片等大文件，则将其编辑为第四消息，并调用微信素材服务器中素材库的素材管理接口进行上传。
步骤 S30，将第二消息编辑为第三消息，调用企业微信服务器中微信消息推送服务的外部消息推送接口，推送到指定的企业微信账号、微信公众以及消息接收人。
步骤 S40，为消息推送计数器中指定的消息接收人的接收消息计数器+1。
结束

图8

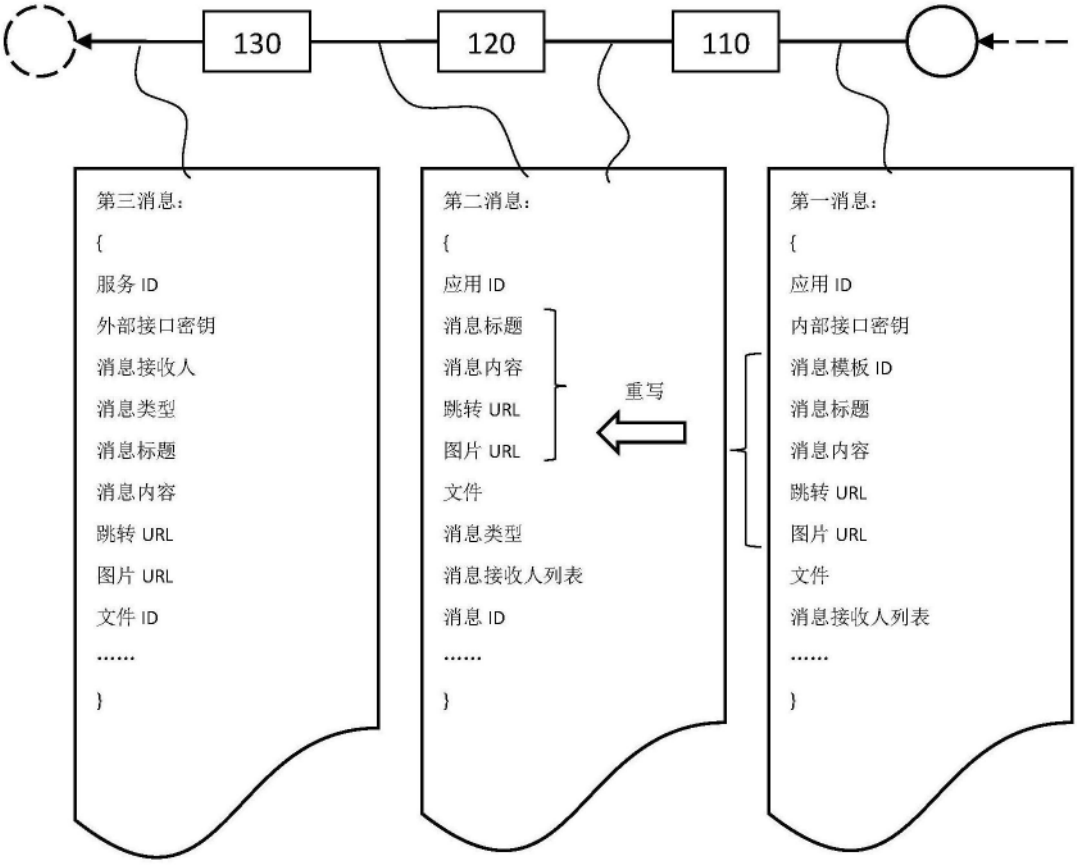
130
120
110
第三消息：
{
服务 ID
外部接口密钥
消息接收人
消息类型
消息标题
消息内容
跳转 URL
图片 URL
文件 ID
……
}
第二消息：
{
应用 ID
消息标题
消息内容
跳转 URL
图片 URL
文件
消息类型
消息接收人列表
消息 ID
……
}
重写
第一消息：
{
应用 ID
内部接口密钥
消息模板 ID
消息标题
消息内容
跳转 URL
图片 URL
文件
消息接收人列表
……
}

图9