址 IP_{gG} 和端口 $PORT_{mas}$, 将 MAS 提供的对外服务发布至外网 DMZ 区.

(5) 在外网 DMZ 区域名服务器和 VPN 移动应用环境配置中, 将域名 $HOST_{mas}$ 指向 Gap_G 的 DMZ 端地址 IP_{gG}. 确保通过办公 Wi-Fi 或 VPN 接入的终端使用统一的域名访问 MAS 服务.

(6) 反向代理 $Nginx_{G1}$ 地址 IP_{nG1}, 在 $Nginx_{G1}$ 上配置 MAS 代理访问至 IP_{gG}, 代理推送接口.

(7) 将互联网域名 $HOST_{app}$ 指向外网防火墙 FW_G 的互联网地址 IP_{fG}, 在 FW_G 中配置将 $Nginx_{G1}$ 绑定域名 $HOST_{app}$.

(8) 配置 $Nginx_{G1}$, 对 MAS 业务接口 URL 进行过滤, 只允许通过域名 $HOST_{app}$ 访问 MAS 服务接口, 只对外推送消息接口一项服务.

(9) EMM 的配置同理, 将自动升级、设备管理接口发布至互联网.

图 5 集团接口服务代理示意图

2.2.2 厂级接口服务的代理

厂级接口服务的代理如图 6 所示.

(1) 厂级 MAS 服务器 Mas_N 内网地址为 IP_{mN}, 对外提供业务接口、管理后台两项服务.

(2) 厂级反向代理 $Nginx_N$ 地址为 IP_{nN}. 在 $Nginx_N$ 上配置 Mas_N 的代理访问至 IP_{mN}, 代理厂级业务接口.

(3) 在 $Nginx_{G2}$ 上配置 $Nginx_N$ 的代理访问至 IP_{nN}, 代理来自于 $Nginx_N$ 的厂级业务接口. 对于多家基层单位, 以此方法分别配置厂级业务接口的代理.

(4) 厂级安全隔离网闸 Gap_N 的 DMZ 端地址为 IP_{gN}, 在 Gap_N 上配置将内网 $Nginx_N$ 地址映射为外部地址 IP_{gN} 和端口 $PORT_{mas}$. 将 MAS 服务 DMZ 区域名 $HOST_{mas}$ 指向 Gap_N 的 DMZ 端地址 IP_{gN}.

2.3 网络环境无缝切换的优化

用户无论处于移动网络、外部 Wi-Fi 还是办公 Wi-Fi, 在改变所处网络环境后, 系统都能够在新环境中自动连接, 实现用户基本无感知的无缝切换.

(1) 配置办公 Wi-Fi 列表: 在 EMM 服务上维护各单位适用的办公 Wi-Fi 列表. 移动门户 APP 完成用户绑定后, 根据用户所在单位下载相应的办公 Wi-Fi 列表, 每次接入 EMM 服务认证时, 检测是否有新版本的办公 Wi-Fi 列表, 如有则进行更新, 确保办公 Wi-Fi 列表处于最新状态.

(2) 网络状态切换时的处理策略: 当移动端接入网络状态切换后, 若未处于办公 Wi-Fi 下, 则自动尝试通过互联网 (集团线路 1) 建立至集团 VPN 的安全通道; 若处于办公 Wi-Fi 列表所包含名称的网络中, 则访问域名为 $HOST_{mas}$ 的服务端, 判断是否为办公 Wi-Fi. 若能够访问域名为 $HOST_{mas}$ 的服务端, 则处于办公 Wi-Fi, 可正常开展业务; 若不能访问, 则在下次网络状态切换之前, 都认为移动端处于非办公 Wi-Fi 下, 标记该

状态并自动尝试通过互联网建立集团 VPN 安全通道. 此时, 只要移动端能够访问互联网, 或处于企业内部办公 Wi-Fi 网络中, 都能够访问域名为 $HOST_{mas}$ 的服务端, 并通过当前线路的代理服务与 MAS 对接; 由于不同的 MAS 服务各司其职, 反向代理服务只是转发数据, 不另外生成会话, 所以网络切换后, 即使切换了代理服务也不会影响 MAS 的会话状态, 从而实现业务的无缝切换.

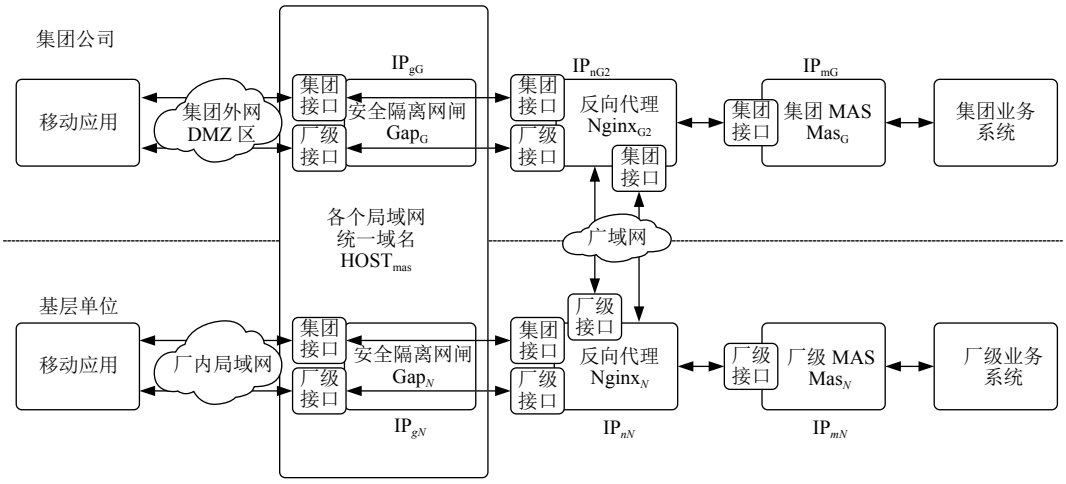

图 6 两级接口服务代理示意图

3 结语

本文在某发电集团企业的移动平台现状基础上进一步研究, 设计了双网隔离环境下支持两级应用的集团级移动平台, 通过网络架构升级, 以及对身份认证、接口服务和网络环境无缝切换的优化, 解决了系统两级应用的问题, 并进行了部分应用实践, 方案具有可行性, 为双网隔离环境的集团企业建设移动平台提供了一定的参考.

参考文献

1 王鑫. 移动应用 App 的发展研究. 内蒙古财经大学学报, 2017, 15(1): 114–117. [doi: 10.3969/j.issn.2095-5871.2017.01.027]

2 王鑫. Native App 与 Web App 移动应用发展. 计算机系统应用, 2016, 25(9): 250–253.

3 杜帅, 鄂海红, 许可. 混合移动应用开发模式的新策略. 软件, 2015, 36(6): 12–17. [doi: 10.3969/j.issn.1003-6970.2015.06.003]

4 王荣海. 基于 Hybrid App 技术的企业移动应用系统构建研究. 软件工程, 2016, 19(7): 46–49. [doi: 10.3969/j.issn.1008-0775.2016.07.014]

5 钮卿. 手机移动办公系统在双网隔离环境下的设计与优化. 电力信息与通信技术, 2014, 12(7): 109–114.

6 张云翔. 电力企业基建移动应用平台研究与应用. 电力信息与通信技术, 2016, 14(9): 94–98.

7 周志烽, 何超林, 梁超, 等. 电网调度移动平台的构建与应用. 电力信息与通信技术, 2014, 12(12): 91–96.

8 张向阳, 朱建生, 刘承亮, 等. 铁路企业移动应用平台的研究与开发. 铁路计算机应用, 2017, 26(9): 15–19, 23. [doi: 10.3969/j.issn.1005-8451.2017.09.004]

9 高嘉泽, 高强, 吴国全, 等. 面向移动应用的后端服务平台. 计算机系统应用, 2014, 23(2): 22–27. [doi: 10.3969/j.issn.1003-3254.2014.02.004]

10 苏凯, 吴广财. 移动管理驾驶舱离线访问研究与实现. 电力信息与通信技术, 2014, 12(2): 80–85. [doi: 10.3969/j.issn.1672-4844.2014.02.017]

11 赵永国, 张诗军. 电力行业移动应用安全体系关键技术研究. 电力信息与通信技术, 2017, 15(3): 20–26.

12 刘强, 杨维永, 刘金锁. 电力移动信息化安全研究. 电力信息与通信技术, 2015, 13(8): 83–88.

13 薛文婷, 马良, 耿海洋. 电网企业移动终端的应用及安全分析. 电力信息与通信技术, 2017, 15(10): 132–136.

14 陈希, 刘颖卿, 叶蕴芳. 构筑移动应用安全评测体系. 电信工程技术与标准化, 2015, 28(12): 11–16. [doi: 10.3969/j.issn.1008-5599.2015.12.003]

15 邹煜. 企业级移动应用平台建设与安全保障体系探析. 网络空间安全, 2016, 7(6): 80–82. [doi: 10.3969/j.issn.1674-9456.2016.06.024]

16 何慧萍, 张华兵, 李永攀, 等. 移动统一接入平台安全体系研究与应用. 电力信息与通信技术, 2014, 12(6): 114–118.

17 邓庚盛, 付爱英, 熊永春. Nginx 反向代理技术在移动应用服务架构中的应用. 科技广场, 2017, (9): 83–87.