计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2019,28(10):98−102 [doi: 10.15888/j.cnki.csa.007083]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

面向网络隔离架构的业务流行为控制高可信交互框架①

黄姗姗, 蒋厚明, 胡　牧, 刘士进, 魏珍珍

(南京南瑞信息通信科技有限公司, 南京 210008)
通讯作者: 黄姗姗, E-mail: huangshanshan@sgepri.sgcc.com.cn

摘　要: 本文提出一种面向网络隔离架构的业务流行为控制的高可信交互框架, 解决了企业互联网移动应用难以访问复杂安全架构下的高安全区业务数据的问题, 确保了业务系统关键数据的安全. 在网络安全防护要求下, 引入移动接入网关, 分解业务数据跨安全区交互过程, 通过特殊的访问转换与通信方法, 实现了业务数据通过各型隔离装置的安全、可信传输和业务流行为控制. 该框架目前已在员工报销、考勤打卡、电力系统配网抢修、移动巡检等多个业务领域得到广泛应用.

关键词: 网络隔离架构; 高可信交互框架; 互联网移动应用; 高安全区业务数据; 移动接入网关; 业务流行为控制

引用格式: 黄姗姗,蒋厚明,胡牧,刘士进,魏珍珍.面向网络隔离架构的业务流行为控制高可信交互框架.计算机系统应用,2019,28(10):98–102. http://www.c-s-a.org.cn/1003-3254/7083.html

Highly Trusted Interaction Framework for Business Behavior Control Based on Network Isolation Architecture

HUANG Shan-Shan, JIANG Hou-Ming, HU Mu, LIU Shi-Jin, WEI Zhen-Zhen

(Nanjing NARI Information & Communication Technology Co. Ltd., Nanjing 210008, China)

Abstract: This study proposes a highly trusted interaction framework for business behavior control based on network isolation architecture. This framework not only makes the access of business data in the high security zone under the complex security architecture for enterprise internet mobile applications possible but also ensures the security of key data of the business system. Under the requirements of network security protection, the mobile access gateway is introduced to decompose the interaction process of business data across the security zone. Then, it designs an access conversion and communication method, which realizes the safe and reliable transmission of business data through various isolation devices and business flow control. The framework has been widely used in many business areas such as employee reimbursement, attendance punching, power system distribution repair and mobile inspection.

Key words: network isolation architecture; highly trusted interaction framework; Internet mobile applications; high security zone business data; mobile access gateway; business flow control

1　研究背景

随着移动互联网的迅猛发展, 越来越多大型企业需要在外网部署针对客户或者员工的互联网应用, 例如报销、员工办公和外网移动作业应用等[1], 但这些应用访问的数据大都保存在企业内网, 如果直接将企业内网数据暴露到互联网, 将带来严重的安全风险[2]. 在信息外网部署各业务系统相应的移动服务, 甚至单独开发一套支撑互联网移动应用的移动服务, 不仅无法

① 基金项目: 公司自筹项目: 移动应用公共服务组件关键技术研究 (5246DR190020)
Foundation item: NARI-Funded Project: Key Technology Research of Common Service Component for Moble Applications (5246DR190020)
收稿时间: 2019-03-05; 修改时间: 2019-04-02; 采用时间: 2019-04-12; csa 在线出版时间: 2019-10-15

复用已在内网建设的移动应用服务, 还增加了互联网移动应用的开发成本, 同时将业务应用服务部署在信息外网会带来数据泄露的风险以及其他安全隐患[3]. 因此, 如何在保障数据安全的基础上实现移动应用的高效访问成为企业尤其是大型企业移动信息化的重要研究难题. 已有的电力内外网隔离环境即时消息传输[4]没有提供数据加解密等功能, 且只验证了用于文本传输的效果, 没有涉及工单下载、图片信息资源同步等操作的时效性; 信息内外网边界安全检测系统[5]、智能电网信息内外网[6]、内外网数据安全交换技术[7]过于简略, 提供的功能不能满足当下的实际需求.

为解决这一难题, 在自主研发高性能、低延迟的移动接入网关的基础上, 本文提出一种面向网络隔离架构的业务流行为控制的高可信交互框架, 在网络安全防护要求下, 分解业务数据跨安全区交互过程, 设计了一种访问转换与通信方法, 实现了业务数据通过各型隔离装置的安全、可信传输和业务流行为控制, 基本业务的完整数据访问流程用时少于 0.2 s; 还提供内容过滤、数据加密、流量控制等应用层的安全防护措施, 实现对业务流的控制. 解决了企业互联网移动应用难以访问复杂安全架构下的高安全区业务数据的问题, 确保了业务系统关键服务的安全.

2 高可信交互框架

该面向网络隔离架构的业务流行为控制的高可信交互框架的目标是给大型企业移动信息化提供移动接入网关、安全防护、内外网穿透、数据跨网双向通信和业务流控制等服务. 下文从移动接入网关、高可信交互框架两个模块进行阐述.

2.1 高性能移动接入网关

面向网络隔离架构的高可信交互框架在信息外网和信息内网高安全区部署高可信交互框架, 并引入移动接入网关, 网关又名网间连接器、协议转换器, 用于 2 个协议不同的网络或系统间[4]. 本框架中网关作为互联网移动应用与内网业务系统进行服务访问和通信交互的中介, 其主要作用是会话共享、内容过滤、服务路由和性能监控.

移动接入网关包括前置机服务器、中间库服务器以及后置机服务器 3 个部分. 其中, 前置机服务器部署在信息外网, 后置机服务器和中间库服务器部署在信息内网, 如图 1 所示.

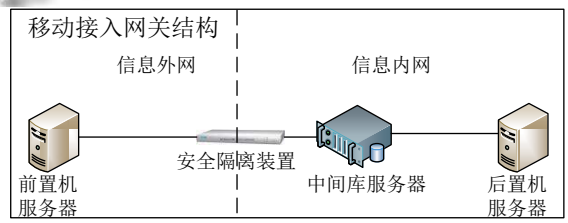

图 1 移动接入网关结构图

部署在信息外网的前置机与互联网移动应用直接相连, 后置机与内网业务应用服务直接相连, 中间库作为前后置机数据交换的中转站, 前后置机轮询获取中间库数据. 信息内外网之间通过安全隔离装置进行服务访问和数据交互[6].

前置机和后置机均包括会话管理模块、服务发现模块、服务代理模块、任务调度模块、数据清理模块. 具体的功能架构图如图 2 所示.

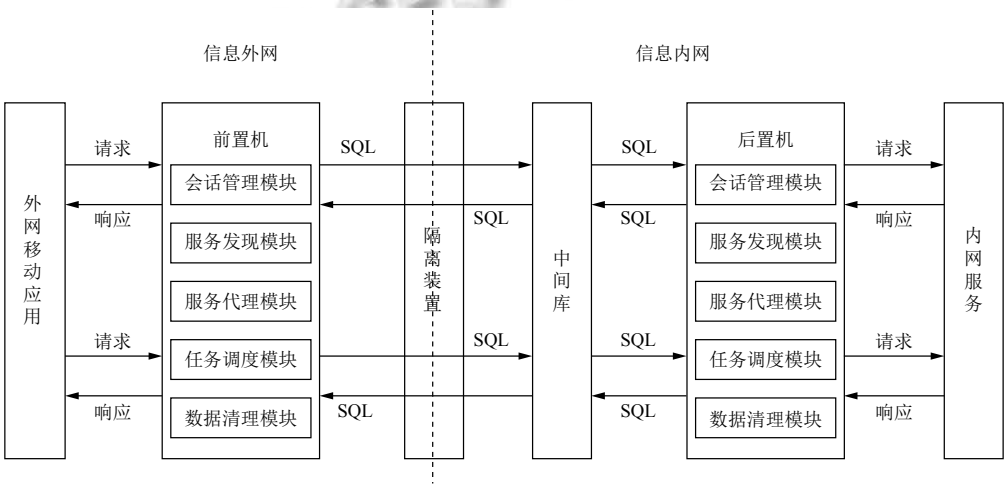

图 2 移动接入网关功能架构图

前置机基于多路复用高性能 IO 通信框架实现[8], 负责发布面向移动终端的代理服务, 解析移动终端请求, 并按一定格式序列化保存到中间库, 然后异步等待响应结果返回给移动终端. 同时提供白名单、内容过滤、请求分发、并发控制、负载均衡策略适配等功能.

后置机通过轮询等方式提取中间库中的请求数据, 并反序列化成相应的请求对象, 然后调用目标服务获取响应, 并将得到的响应结果保存到中间库, 同时提供对目标服务的性能监控、日志统计、异常分析等功能.

移动接入网关中间库, 作为前置机和后置机数据交互的中介, 通过内存表设计方案提高数据访问效率和负载能力. 前置机、后置机采用对等设计, 即采用相同的设计架构, 实现双向通信.

将移动接入网关作为企业对外的统一入口, 提供会话共享、服务代理等功能; 对请求的数据进行签名、校验、协议转换、压缩并进行安全过滤[9]; 并在互联网移动终端与后端业务系统间建立安全数据通道, 实现重要业务数据的全文加密传输和业务安全交互.

信息内网、信息外网穿透服务单节点支持多用户并发, 可独立部署, 支持集群部署, 支持在不停机的情况下通过服务发现模块动态向集群中添加节点, 并自行均衡分配任务给各节点, 使新加入的节点处于服务状态, 动态扩展, 分摊并发压力, 具有较强的横向可扩展性和一定的智能性.

2.2 高可信交互框架

目前大多公司信息内网和信息外网之间架设的物理隔离装置, 只允许 SQL 语句从信息外网穿透隔离装置进入信息内网, 正常的 HTTP 请求无法从信息外网到达信息内网[10]. 然而实际应用中存在大量信息内网和外网之间进行 Web 服务访问的应用场景[11], 因此迫切需要一种能够实现信息内网和信息外网互联互通的解决方案.

因此, 项目组研究实现了高性能、低延迟信息内外网数据穿透技术, 并提供数据跨网双向通信和业务流行为控制. 以互联网移动应用访问内网业务系统为例, 给出具体的信息流转结构图如图 3 所示.

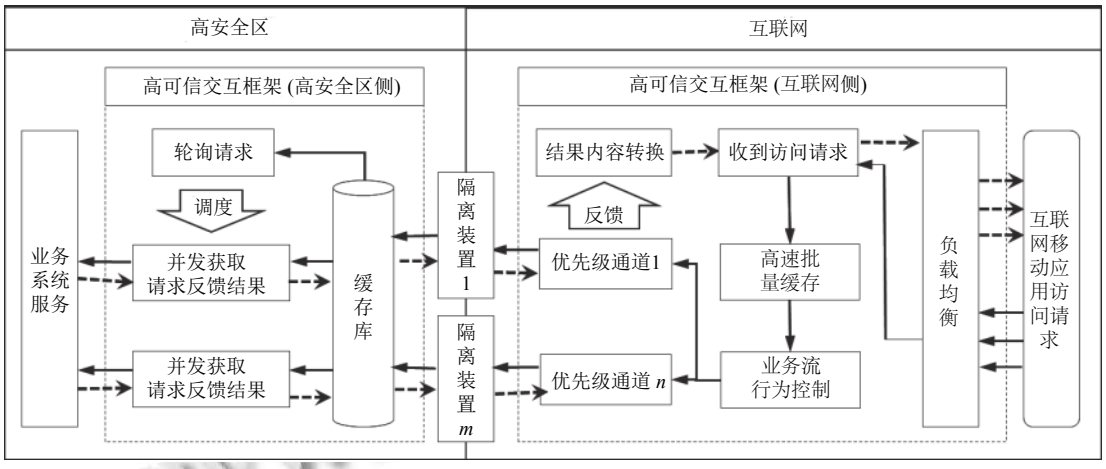

图 3 高可信交互框架功能层级图

当互联网移动应用主动发起 HTTP 请求时, 请求通过负载均衡后先发送到前置机. 对于合法请求, 前置机创建会话, 并检测是否存在可用后置机节点, 如果存在则批量缓存请求并内容转换, 将请求通过优先级通道, 附加消息相关信息后转换为 SQL 语句并通过部署于互联网和高安全区之间的隔离装置写入到中间库, 如果不存在则直接将失败信息发送给互联网移动应用.

后置机轮询中间库获取 SQL 请求信息, 解析后发送到真实的内网业务应用系统, 并等待响应信息; 内网业务应用服务返回响应信息后, 后置机将响应信息按照与前置机相同机制转换为 SQL 语句写入到中间库; 前置机轮询中间库获取响应信息, 并将响应信息发送给互联网移动应用, 实现 HTTP 请求从外网到内网的穿透.

这一框架既能使互联网移动应用发出的请求穿透隔离装置访问内网业务应用系统, 也能将内网业务应用系统发出的请求发送到互联网移动应用. 将信息内网的服务选择性的“暴露”出来, 实现透明访问. 当内

网服务需要向外网服务“推送”数据时, 能够实现逆向访问.

面向网络隔离架构的业务流行为控制的高可信交互框架, 在网络安全防护要求下控制业务流行为, 可通过访问转换为任何接入的业务应用系统提供通信和数据的可行传输服务.

3 实例结果及分析

为了验证该框架的有效性和实用性, 将其应用于电力行业移动信息化, 在移动互联网技术基础上, 通过掌上终端、服务器、个人计算机等多平台的信息交互, 实现配网抢修、移动巡检、用电采集等业务. 这些业务对应的业务系统只能部署在电网信息内网, 与之对应的移动应用均位于互联网, 一线员工在移动终端上工作, 通过该面向网络隔离架构的业务流行为控制交互框架与内网业务系统进行数据传输和通信.

以配网抢修业务为例, 在电网信息内网部署前置机服务器 (8 核 16 GB) 和中间库 (16 核 32 GB), 在信息外网部署后置机服务器 (8 核 16 GB), 中间库和后置机之间加装隔离装置 (8 核 16 GB), 并在中间库中配置配网抢修业务系统地址, 在移动终端 (Android8.0) 配置被隔离装置映射后服务地址, 移动终端通过网关访问真实的内网服务, 以此连通内网业务服务和互联网终端. 当配网抢修终端在现场采集到信息, 先发送给前置机, 经由前置机写入中间库, 后置机轮询中间库, 提取信息并发送给业务系统. 根据各个使用现场的业务内容和访问量, 测试查询、工单下载、图片资源信息同步业务和三种业务混合工作分别在 200、300 和 500 并发数下的响应时间和事物通过率, 实验数据如表 1 所示.

由表 1 中数据可以看出, 移动运维的查询业务、工单下载业务、图片资源信息同步和 3 种操作混合业务, 在并发量为 200、300 和 500 时的平均响应时间均在 0.2 秒以内; 且事务完全通过, 无一失败. 文献[4]中也给出了文本消息传输的及时性和稳定性的实验结果, 如表 2 所示, 尽管业务并发量和业务内容不相同, 本文所述方法在响应时间和事物通过率方面仍然具有一定的优势.

引入移动接入网关作为隔离装置, 在内网业务系统和互联网移动终端之间搭建面向网络隔离架构的业务流行为控制高可信交互框架, 并没有增加业务实际响应时间; 当并发访问量过大时, 网关能动态扩展前后置机节点, 并自行均衡负载到各节点. 当交互的数据中包含用户名密码等信息时, 前后置机会分别进行加解密操作, 保证信息的安全性.

表 1 不同业务高并发时响应时间记录表

测试项	并发数	平均响应时间 (s)	TPS(笔/s)	事物通过率 (%)
查询	200	0.073	2049.823	100
	300	0.139	2062.225	100
	500	0.181	2096.508	100
工单下载	200	0.027	1507.039	100
	300	0.094	1976.119	100
	500	0.144	1983.134	100
图片资源信息同步	200	0.060	3250.934	100
	300	0.098	2908.775	100
	500	0.137	2759.230	100
混合业务: 查询 33%; 工单下载 33%; 图片资源信息同步 33%	200	0.063	775.569	100
		0.068	714.583	100
		0.059	822.086	100
	300	0.100	733.247	100
		0.105	687.351	100
		0.101	706.731	100
	500	0.142	681.987	100
		0.153	619.997	100
		0.145	647.539	100

表 2 文本消息传输的及时性与稳定性[4]

总消息数 (条)	并发数 (个)	总时长 (秒)	成功率 (%)
1000	10	1.65	100
2000	10	2.01	100
3000	50	2.49	100
10 000	100	4.23	99.65

该框架的创新与实现, 使得大型企业开展互联网移动应用建设时, 业务系统仍可保留在高安全区, 部署方式不变, 互联网移动应用可复用内网已有的业务系统, 提高了资源的利用率, 降低了互联网移动应用部署的复杂度和难度, 有效保障了系统安全. 通过移动终端统一接入, 统一安全防护, 推动了移动应用微服务、微应用化, 降低应用系统间的耦合度[9], 最终缩短移动应用的开发周期. 引入高性能、低延迟信息内外网数据穿透技术, 拓展和丰富移动外网安全防护解决方案.

参考文献

1 徐震, 刘韧, 余爱民, 等. 智能电网中的移动应用安全技术. 电力系统自动化, 2012, 36(16): 82–87.

2 陈云蛟, 沈龙, 周甜. 内网信息安全体系研究. 软件导刊, 2014, 13(6): 130–131.

3 张敬伦, 张永生, 高丽琴. 基于内网数据安全防护引擎的安全架构设计. 通信技术, 2017, 50(1): 158–161. [doi: 10.3969/j.issn.1002-0802.2017.01.027]
4 曾望志, 祝永晋, 于广荣, 等. 电力内外网隔离环境即时消息安全传输的研究与实现. 江苏科技信息, 2017, (31): 45–47. [doi: 10.3969/j.issn.1004-7530.2017.31.016]
5 叶水勇, 吴斌, 陈清萍, 等. 信息内外网边界安全监测系统的设计与实施. 电力与能源, 2019, 40(1): 59–62.
6 管小娟, 何高峰, 周诚, 等. 智能电网信息内外网边界安全监测模型研究. 电力信息与通信技术, 2016, 14(4): 66–69.
7 郭仁超, 徐玉韬. 内外网数据安全交换技术在电网企业的应用研究. 电力大数据, 2018, 21(2): 61–66.
8 张华鲁, 贾玮, 张天兵, 等. 电力企业移动信息化实施方案. 电信科学, 2017, 33(2): 154–162.
9 羡慧竹. 基于物联网的智能网关系统研究与实现[硕士学位论文]. 北京: 北京工业大学, 2014.
10 刘金锁. 基于单向隔离技术的电力内外网信息安全交互平台研究. 电力信息化, 2010, 8(8): 37–40. [doi: 10.3969/j.issn.1672-4844.2010.08.010]
11 孟威, 乔林, 刘颖, 等. 基于电力企业移动办公的内外网数据交互. 2017 智能电网发展研讨会论文集. 北京. 2017. 480–482, 531.