

DOI: 10.13955/j.yzyj.2021.03.05.04

Nginx 在四川邮政安全对外服务网关中的应用探讨

田宏, 李子木

(中国邮政集团有限公司四川省信息技术局, 四川 成都 610015)

摘 要: 随着互联网应用的普及, 如何解决信息网络安全与业务对互联网应用需求的矛盾成为邮政技术人员必须面对的问题。以四川邮政安全对外服务网关建设为例, 通过对 Nginx 服务器的二次开发, 同时结合 HTTPS 协议, 使其具备安全管控功能, 并提出了具体的技术架构方案, 以促进邮政安全系统建设工作, 为解决网络安全和业务发展矛盾提供解决思路。

关键词: 信息安全; 反向代理; 访问控制; HTTPS 协议

中图分类号: F61 **文献标识码:** A

随着互联网的持续发展, 人类社会已经在互联网上建立了庞大的生态经济。从商品销售到用户出行, 人们的生活已经同互联网紧密结合在一起。邮政业务现在也离不开互联网。当前邮政的互联网业务已经完成了产品和服务的交易闭环、服务内容的升级与飞速发展。业务飞速发展的同时也带来了数据被劫持或泄露的安全风险。纵观当前整个互联网企业, 用户数据泄露、流量劫持、网页篡改等安全事件频发, 这些安全事件往往给个人和公司带来非常大的经济损失和社会影响。因此, 如何解决好安全同发展的矛盾已成为邮政技术人员必须破解的难题。

四川邮政服务网关依托于 Nginx 软件的强大功能进行建设。Nginx 是一个以高性能、高并发著称的 HTTP 服务器, 它支持 HTTP 反向代理、TCP 代理、负载均衡、HTTP 缓存及 Web 开发等, 更为重要的是 Nginx 软件支持二次开发, 以增强软件自身的功能。Nginx 只通过简单配置无法满足四川邮政

服务网关对安全的需求, 只有通过对 Nginx 进行模块开发和定制才能满足相关需求。

1 四川邮政系统安全存在的问题

为解决互联网网络安全问题, 除使用防火墙统一解决网络层安全外, 用户身份认证、访问控制权限管理、数据加密及防数据篡改等都由各个应用系统自行实现。这种方式主要存在如下问题。

一是各个系统自建网络安全功能, 由于各个系统的设计和开发人员各异, 安全方案可能也存在较大差别, 对安全建设的质量无法较好监管, 也不利于邮政运维对系统安全的统一把控。

二是各个系统单独建设网络接入安全功能, 会对接入方造成使用障碍。如使用两套系统需要使用两套安全认证方式或者认证凭证。

三是从系统架构角度讲 (也是最关键的一方面), 各个系统单独建设安全功能, 不利于企业安全能力的提升, 还会导致系统功能和程序模块缠绕

作者简介: 田宏 (1977 ~), 男, 四川成都人, 主要从事软件开发研究; 李子木 (1990 ~), 男, 四川成都人, 硕士, 工程师, 主要从事信息系统维护研究。

收稿日期: 2021-03-19

纠缠。目前的企业系统建设,无论中台还是微服务,都强调系统的单一职责,要把与本系统业务不相关的功能分离出去。对那些所有系统都需要但与自身业务逻辑不相关的功能要做好服务下沉工作,即把共性抽取出来形成单独的服务。让各个业务系统专注于自身业务功能的开发,而这些公共服务独立出来后由专门人员负责设计开发,做到分工明确,各自在负责领域深耕发展。

2 对外服务安全网关项目建设目标

为了解决系统安全建设过程中的问题,四川邮政启动了对外服务安全网关的建设工作。通过项目建设,解决本省系统通过互联网对第三方提供程序接口和软件系统的安全控制,提供邮政系统在互联网的安全反向代理功能。

2.1 提供安全访问保障

安全网关对互联网统一提供 HTTPS 服务, HTTPS 采用双向认证方式。为需要接入邮政系统的每一个第三方提供一个唯一的自签证书或者第三方认证证书。需要访问邮政系统者必须提供邮政颁发的证书。HTTPS 具有以下优点:一是借助 HTTPS 协议本身安全特性来对数据进行加密,防止敏感数据的泄露。二是完成第三方的身份认证问题,防止系统被非授权的其他人员访问。三是保证数据的完整性,防止数据在互联网传输过程中被他人篡改。

2.2 提供访问控制和权限管理

安全网关对授权用户进行访问控制,网关基于访问用户、权限分配,设置细粒度访问控制策略,采用动态反向代理方式,达到非法用户不能访问、合法用户不能越权访问的目的。安全网关主要是通过 Nginx 进行权限控制和反向代理工作。Nginx 作为反向代理服务器具备如下优势。

2.2.1 响应更快

响应速度表现在两个方面:一方面,在正常情况下,单次请求会得到更快的响应;另一方面,在高峰期如有数以万计的并发请求,Nginx 可比其他 Web 服务器更快地响应请求。

2.2.2 高扩展性,跨平台

Nginx 的设计极具扩展性,是由多个不同功能、不同层次、不同类型且耦合度极低的模块组成。因

此,当对某一个模块修复 Bug 或进行升级时,可以专注于模块自身,无需在意其他,而且在 HTTP 模块中,还设计了 HTTP 过滤器模块。一个正常的 HTTP 模块在处理完请求后,会有一串 HTTP 过滤器模块对请求的结果进行再处理。当开发一个新的 HTTP 模块时,不但可以使用诸如 HTTP 核心模块、events 模块、log 模块等不同层次或者不同类型的模块,还可以原封不动地复用大量已有的 HTTP 过滤器模块。这种低耦合度的优秀设计,造就了 Nginx 庞大的第三方模块,而公开的第三方模块也如官方发布的模块一样容易使用。Nginx 的模块都是嵌入到二进制文件中执行的,无论官方发布的模块还是第三方模块都是如此。这使得第三方模块一样具备极其优秀的性能,充分利用 Nginx 的高并发特性,因此许多高流量的网站都倾向于开发符合自己业务特性的定制模块。

2.2.3 高可靠性,宕机率低

高可靠性是选择 Nginx 的最基本条件,很多家高流量网站都在核心服务器上大规模使用 Nginx。Nginx 的高可靠性来自其核心框架代码的优秀设计以及模块设计的简单性。另外,官方提供的常用模块都非常稳定,每个 worker 进程相对独立, master 进程在 1 个 worker 进程出错时可以快速“拉起”新的 worker 子进程提供服务。

2.2.4 低内存消耗

一般情况下,10 000 个非活跃的 HTTP Keep-Alive 连接在 Nginx 中仅消耗 2.5MB 内存,这是 Nginx 支持高并发连接的基础。

2.2.5 单机支持 10 万以上并发连接

这是 Nginx 一个非常重要的特性。随着互联网的迅猛发展和互联网用户数量的成倍增长,各大公司、网站都需要应付海量并发请求,一个能够在峰值期顶住 10 万以上并发请求的 Server,无疑会得到大家的青睐。理论上,Nginx 支持的并发连接上限取决于内存,10 万远未封顶。能够及时处理更多的并发请求,与业务特点紧密相关。

2.2.6 热部署

master 管理进程与 worker 工作进程的分离设计,使得 Nginx 能够提供热部署功能,即可以在 7×24 小时不间断服务的前提下,升级 Nginx 的可执行文件,同时支持不停止服务即可更新配置项、

更换日志文件等功能。

四川邮政安全网关的权限控制正是依托于 Nginx 的高扩展性，在 Nginx 的 HTTP 文请求访问阶段加入自己开发的权限控制代码，通过匹配 HTTPS 中证书 ID 来控制接入方的访问权限。

2.3 提供统一的接入安全管理

安全网关提供统一的安全功能和互联网接入端口，邮政内部的各个系统无需单独实现互联网的安全接入。该方式不但能减轻各个业务系统的开发要求，做到业务功能沉淀积累，还避免了各个系统都建安全接入功能导致各自为政的情况，为后期安全管理扫清障碍。统一的安全管理功能提供了统一管理接入邮政系统的用户、统一发放管理数字证书等功能，有助于安全规定的落实。

3 对外服务安全网关项目技术介绍

Nginx 是一款非常优秀的反向代理工具，支持请求分发、负载均衡以及缓存等非常实用的功能。在请求处理上，Nginx 采用 epoll 模型，这是一种基于事件监听的模型，因此具备非常高效的请求处理效率。同时，Nginx 还支持多种语言的再次开发功能。基于其性能和开发两方面优势的考虑，四川

邮政对外服务网关的转发核心部分选用 Nginx 来实现。

HTTPS 是安全套接字层超文本传输协议，为了数据传输的安全，HTTPS 在 HTTP 的基础上加入了 SSL/TLS 协议，依靠证书来验证服务器的身份，并为浏览器和服务器之间的通信加密。HTTPS 协议是由 SSL/TLS+HTTP 协议构建的可进行加密传输、身份认证的网络协议，要比 HTTP 协议安全。HTTPS 协议的主要作用分为两种：一种是建立一个信息安全通道，保证数据传输的安全；另一种就是确认网站的真实性。四川邮政对外服务网关提供的服务使用 HTTPS 协议。

4 对外服务安全网关项目技术架构

整个系统的数据处理流程是：通过部署在邮政 DMZ 区中的 Nginx 服务器对外提供 HTTPS 服务。Nginx 服务器根据 HTTPS 协议中证书的 ID 与 Redis 中存储的该 ID 权限数据进行匹配，确定其权限。对通过权限认证的数据请求，Nginx 会转发到对应的后台业务系统。权限数据是后台管理人员配置的权限，通过 Web 服务器中的同步程序经过格式转换同步到 Redis。系统技术架构见图 1。系统

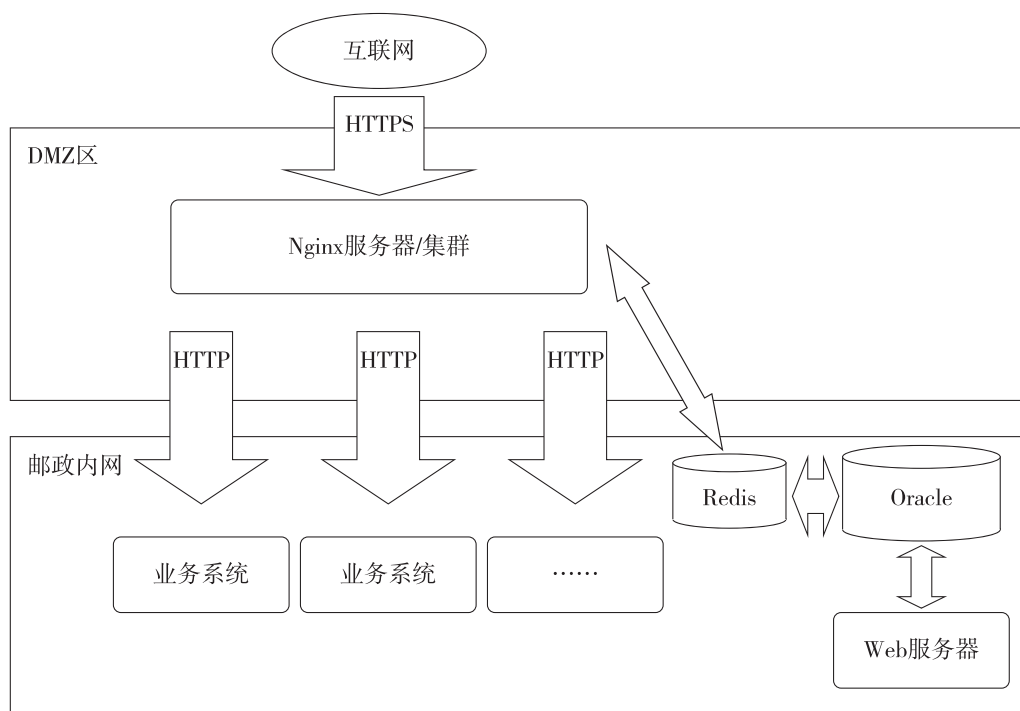


图 1 系统技术架构图

共有四个模块，具体如下。

Nginx 服务器/集群：该模块为核心模块，提供对外的安全接入。当前先提供双向 HTTPS 服务，后期可以考虑提供 SFTP 和 SSH 等其他服务。要接入邮政服务的第三方必须事先获取邮政提供的数字证书，该证书为一对一证书。证书可以是邮政自签名证书或第三方签发证书。该模块的另外一个重要功能是根据提供给接入方的证书按照事先制定好的规则提供权限认证和动态反向路由功能，同时完成 HTTPS 报文到 HTTP 报文的转发工作，在发往各个业务系统的 HTTP 头中插入访问者的证书信息，方便业务系统做用户权限认证工作。

Redis：该模块为上一个模块提供访问规则的存储功能。之所以没有让 Nginx 直接读取 Oracle 中的安全访问规则，一是查询需求相对简单，没有复杂查询的情况出现。二是 Oracle 的性能达不到高并发、低延迟的要求。Redis 需要与 Oracle 中的数据进行同步。

Web 服务器：该模块为管理人员提供操作界面，制定安全访问规则，管理第三方接入。

Oracle：该模块为 Web 服务器提供数据储存功能，还要与 Redis 进行数据同步。

5 管理系统功能介绍

系统架构中的 Web 服务器，主要提供权限管理等功能供管理人员使用。同时负责把 Oracle 内权限内容进行格式转换后存入 Redis 中，供 Nginx 调用进行权限控制。系统的主要功能包括：接入系统维护、对外服务系统维护、Ukey 维护、权限管理、同步权限数据。

5.1 接入系统维护

接入系统是指需要对接邮政内部系统的第三方系统。系统提供该接入系统的增改查功能，同时提供冻结等控制功能。

5.2 对外服务系统维护

该功能负责维护需要通过安全网关提供对外服务的系统，需要维护系统的 IP 地址端口号等信息，以便网关进行动态转发。

5.3 Ukey 维护

Ukey 维护即 SSL 的证书维护，系统可以生成相关的自签证书，同时提供证书有效期管理以及启

停证书的维护，避免原生 Nginx 对证书有效期管控只能在证书生成时指定。系统还提供了加密证书的下载功能。

5.4 权限管理

提供接入系统的证书绑定工作，同时指定接入系统访问邮政内部系统的权限控制。

5.5 同步权限数据

当管理人员修改和增加了相关配置，对于影响权限控制的修改，系统会向管理人员发送提示信息。管理人员根据实际情况手动执行该功能，完成 Oracle 到 Redis 的权限数据同步工作。

6 下一步发展计划

系统上线一年多时间，在实际运行中为系统下一步改进积累了大量经验。四川邮政计划启动项目的二期建设工作，从提供业务功能和系统架构优化两方面同时入手进行建设。

6.1 业务功能优化

进一步优化权限管理，提供多任务角色管理功能，权限管理依托角色进行设置。新增邮政内部机构层级和机构柜员权限管理。对邮政内部系统提供系统程序接口，以便其他系统把内部权限控制同网关安全权限控制相结合。同时，研究新的安全认证方式，比如手机扫二维码的安全认证方式，使对外服务网关的安全认证方式更为多样，以适应不同环境的使用需要。

6.2 系统架构优化

新系统将采用 KeepAlived+Lvs+Nginx 技术实现高可用性的集群，把网关需要进行安全控制的数据从 Redis 移到 Nginx 的共享内存中，但需要解决分布式环境中数据一致性问题。

参 考 文 献

- [1] 王力, 汤永全. Nginx 实战 [M]. 北京: 电子工业出版社, 2019
- [2] 虞卫东. 深入浅出 HTTPS 从原理到实战 [M]. 北京: 电子工业出版社, 2018
- [3] 李明江. Nginx Lua 开发实战 [M]. 北京: 机械工业出版社, 2018
- [4] 陶辉. 深入理解 Nginx [M]. 北京: 机械工业出版社, 2013