文章编号：1005-8451（2016）10-0059-05

通过互联网访问铁路内网Web Service技术的研究与实现

杨金刚，刘　军，高效松，施卉磊
（哈尔滨铁路局　信息技术所，哈尔滨　150006）

摘　要：文章通过互联网访问铁路内网Web Service技术的研究探索，分析了铁路安全平台的原理和结构，提出了穿越铁路安全平台的一般实现方法，并指出了该方法的不足之处。文章结合哈尔滨铁路局的实际项目，给出了互联网访问内部资源代理程序的实现方法，该代理程序实现了互联网访问路网资源的可配置性及零编程。

关键词：安全平台；Web Service；数字证书；令牌；代理程序
中图分类号：U29：TP393　**文献标识码：**A

Web Service technology applied to access railway Intranet through Internet

YANG Jingang, LIU Jun, GAO Xiaosong, SHI Huilei
(Institute of Information Technology, Harbin Railway Administration, Harbin　150006, China)

Abstract: This article made a research and exploration on Web Service technology to access railway Intranet through Internet, proposed a general method of crossing the railway safety platform through the analysis of the principle and structure of the railway safety platform, pointed out some shortcomings of the method. Based on the actual project of Harbin Railway Administration, an implementation method was given to access the internal resources agent program through Internet. The agent program achieved the configuration and zero programming to access resources of railway Intranet through Internet.

Key words: security platform; Web Service; digital certificate; token; proxy

近几年，为了提升铁路运输服务质量，铁路总公司相继建立了12306互联网售票、95306货运电子商务平台等，为旅客出行和货主货运提供了极大的便利，今后借助互联网来方便公众、提升服务质量的信息系统项目将会越来越多。本文结合哈尔滨铁路局网络电报手机App、职工互动交流平台及微信平台等项目，对通过互联网访问铁路内部资源的技术进行深入研究，就通过互联网穿越网络安全平台调用铁路内部网Web Service的方法进行了详细阐述，指出了一般实现方法的不足，并给出了互联网访问铁路内部资源代理程序的实现方法。

1　铁路计算机网络安全平台概述

铁路计算机网络安全平台（简称：安全平台）是铁路总公司计算机网络安全工程的重要组成部分，是铁路综合计算机内部网络与外部网络（互联网）之间的唯一安全连接通道，其设计目标是建设一个先进的网络安全体系架构，为铁路内部和外部用户提供安全可靠的网络计算和通信环境，规范铁路网络基础设置，形成纵深防御体系，提高网络自身防御攻击能力和网络整体性能，满足日益发展的内外网间应用系统数据传输和安全互访的需求。

安全平台主要由网络系统、访问控制系统、证书管理系统及日志审计系统等组成。其中，访问控制系统是划分铁路内部网络和外部网络的重要边界，是实现应用系统安全访问的基础，它在物理隔离的内、外网络之间建立安全的数据传输通道，对访问者的身份和权限进行查验，确保只有符合条件的授权用户才能访问到受保护的系统资源，同时对访问数据格式的有效性进行校验，它由访问通道子系统、访问控制子系统和配置管理子系统组成，访问控制系统结构如图1所示。

收稿日期：2016-05-06
基金项目：哈尔滨铁路局科研项目课题（KWH2015063）。
作者简介：杨金刚，高级工程师；刘　军，高级工程师。

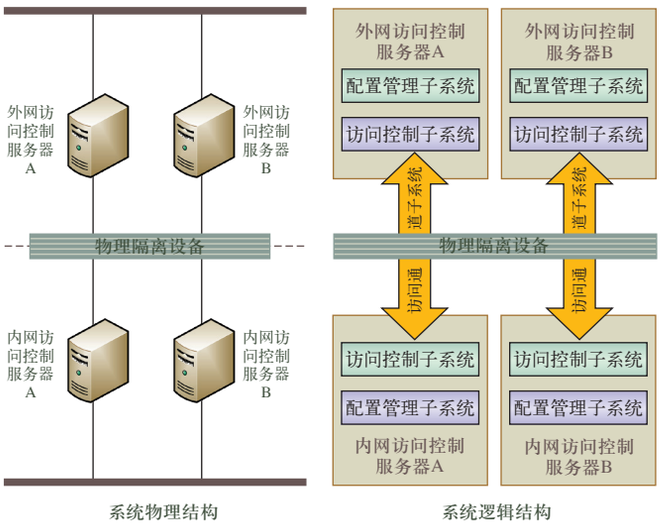

图1　安全平台访问控制系统结构图

1.1　访问控制子系统

主要负责对用户的身份信息及访问权限进行管理，同时进行用户认证及鉴权工作。它提供的服务包括：用户身份认证服务、访问控制服务和单点登录服务。

1.2　访问通道子系统

在物理隔离的铁路内部网络与外部网络之间建立一条安全的数据传输通道，并进一步检查进出数据格式的有效性。它提供的服务包括：正向代理服务和反向代理服务。

1.3　配置管理子系统

对安全代理系统的配置项进行管理，以及对证书库中的证书进行查询。它提供的服务包括：安全代理系统的配置服务和证书库证书的查询服务。

2　互联网访问内网Web Service方法研究

2.1　安全平台访问控制流程

互联网用户通过铁路安全平台访问内部网应用系统的过程如图 2 所示，过程说明见表 1。

2.2　通过互联网访问内部Web Service一般实现方法

2.2.1　物理架构

通过互联网访问内部 Web Service 一般需要 3 类服务器：第 1 类是在互联网或铁路外部服务网隔离区（DMZ）区部署的 Web 应用服务器，用于为互联网用户提供 Web 服务；第 2 类是在铁路外部服务网 DMZ 区部署的外网访问接口服务器，用于部署

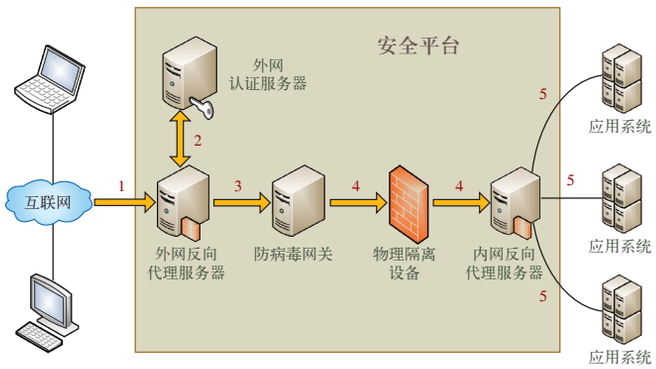

图2　安全平台访问控制流程图

表1　安全平台访问过程控制说明

步骤	说明
1	互联网用户首先要访问内部网应用系统在外网反向代理服务器上映射的互联网域名地址。
2	外网反向代理服务器截获用户访问请求，将其转发至外网认证服务器进行身份认证及授权检查。
3	通过检查后，外网反向代理服务器将访问请求发送到防病毒网关进行病毒扫描。
4	扫描通过后，防病毒网关将访问请求转发到内网反向代理服务器。
5	内网反向代理服务器对访问请求进行必要的协议转换及数据格式有效性检查后，发送到内部网应用系统，应用系统根据业务需求可能进行二次身份认证和鉴权后，返回实际业务数据。

安全平台客户端数字证书、获取安全平台访问令牌（Token）以及为 Web 应用服务器提供内部网 Web Service 的代理方法接口；第 3 类是在铁路内部网部署的 Web Service 接口服务器，用于访问铁路内部网络的业务数据。物理架构如图 3 所示。

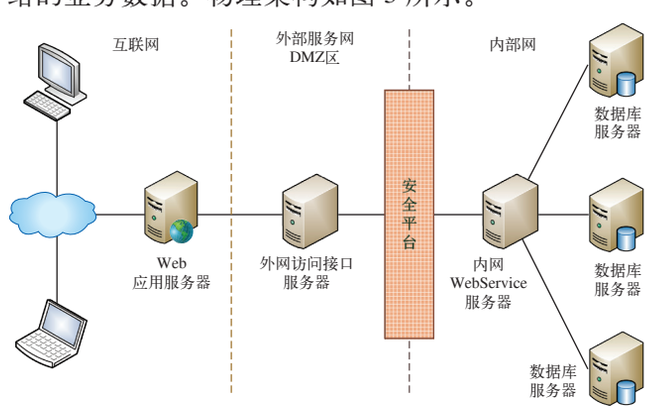

图3　通过互联网访问内部Web Service物理架构图

2.2.2　外网访问接口一般实现方法

本节所阐述的实现方法以 Java 语言为例。

2.2.2.1　创建客户端密钥仓库（KeyStore）

互联网访问内网资源时，安全平台外网认证服务器需要验证客户端数字证书。编写外网访问接口使用 Java KeyStore 密钥仓库，用 Java JDK 提供的

keytool 工具生成密钥仓库并导入证书。导入的 4 个证书分别是：铁路认证中心（CA）根证书、外网访问控制证书、内网访问控制证书以及安全平台配置生成的 PKCS#12 格式客户端证书。

2.2.2.2　获取安全平台访问令牌

安全平台的外网访问控制服务采用的是基于 SSL 协议的 HTTPS 双向认证方式，认证成功后安全平台会为客户端返回具有一定生存时间的访问令牌，持有合法令牌的访问请求可以通过安全平台。

取得安全平台访问令牌的方法是：(1) 进行 SSLSocket 握手，初始化 SSLSocket；(2) 加载 2.2.2.1 生成的 KeyStore 格式的 JKS 文件和口令，返回 SSL 上下文的 SSLSocketFactory 对象；(3) 向 HttpsURLConnection 对象注入 SSLSocketFactory，利用 HttpsURLConnection 对象请求外网认证服务器 URL，解析认证服务器返回内容，获取访问令牌。

2.2.2.3　生成内网Web Service相应的客户端代码

Java JDK 提供了一个工具 wsimport，可以根据 WSDL 生成相应的客户端文件，在项目中使用这些客户端类文件，就可以像调用本地类方法一样调用远程 Web Service 方法。wsimport 工具可以生成由不同语言编写的 Web Service 的 Java 客户端，生成的内网 Web Service 的 Java 客户端类文件和代码文件，导入到项目中即可使用。

2.2.2.4　为Web Service客户端类添加访问令牌

通过 2.2.2.3 生成的客户端在访问内网 Web Service 时，必须在 SOAP 头部插入采用 2.2.2.2 获取的令牌信息，否则将不能通过安全平台验证。

2.2.3　上述实现方法的不足

利用上述方法实现通过互联网访问内网 Web Service 有两方面不足：(1) 编程工作量大，灵活性差。当内网 Web Service 改动时，如新增接口方法、接口参数更改及调用方式改变，都必须修改外网访问接口程序，重新生成内网 Web Service 代理类，重新发布程序；(2) 可扩展性差，这种方法仅能用于标准的 Web Service，对于用户自己实现的通信协议接口不支持。鉴于以上方法的不足，我们开发了互联网访问内部资源代理程序，实现了仅通过配置项目及内部资源的映射，无需编程即可实现通过互联网对内部资源的访问，并且支持标准的 Web Service、Web API 及用户自定义的通信协议接口。

3　代理程序的设计实现

3.1　代理程序总体架构

代理程序由配置、认证、路由及日志 4 部分组成。配置部分用于配置项目的数字证书、虚拟地址及内部资源映射，以及生成供互联网调用的接口 URL。配置部分采用 Flask 框架用 Python 语言编写，配置项的存储采用 MongoDB 数据库；认证部分用于从配置库中读取数字证书文件及密码，提交安全平台外网认证服务器，获取访问令牌。认证部分用 Java 语言编写；路由部分用于解析互联网请求的 URL，根据项目配置信息，转换成内部资源访问地址，并在内部资源访问请求头部附加令牌信息，然后转发至内部 Web Service 接口服务器，获取业务数据后响应互联网请求。路由部分还负责根据配置库中令牌生存时间来对认证部分获取的令牌进行缓存。路由部分采用 Flask 框架用 Python 语言编写，与认证部分的通信采用 Thrift 协议进行 RPC 调用；日志部分用于搜集代理程序的调试信息及性能信息，以便于系统排错和性能瓶颈的确定。代理程序总体架构如图 4 所示。

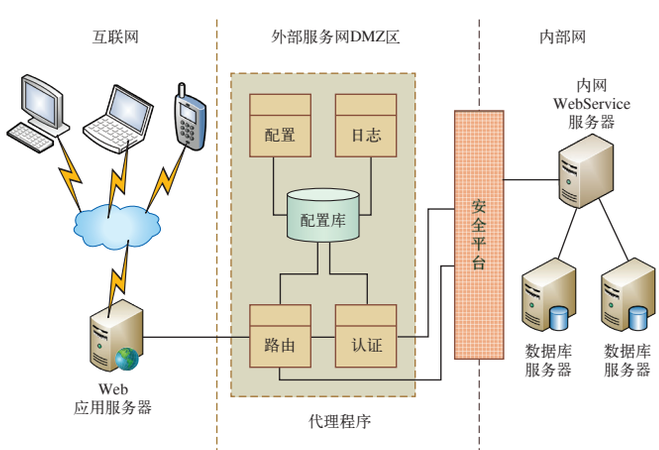

图4　代理程序总体架构图

3.2　配置项设计

代理程序有两类配置项：(1) 项目配置项；(2) 内部资源映射配置项。两者是 One-To-Many 关系，一个项目可包含多个内部资源映射，配置项存储在 MongoDB 数据库中，项目配置完成后，系统自动形成互联网调用的接口 URL。下面以哈尔滨铁路局网

络电报手机 APP 项目为例阐述配置项设计。

3.2.1 项目配置项

下面是项目配置项的一个实例，JSON 格式，各数据域含义见表 2。

表2 项目配置项各数据域含义

数据域	含义
project	项目名称，唯一值
desc	项目描述
virtual_url	内网应用系统在外网反向代理服务器上映射的域名地址
cer_file	安全平台生成的客户端数字证书
cer_pwd	客户端数字证书的口令
token_cache_minutes	访问令牌缓存时间（分钟）

```
{
    "project" : " wldb_app",
    "desc" : "网络电报互联网访问及手机客户端",
    "virtual_url" : "http://xxxx.xxxx-railway.com.cn:8123/mapping/wldb/",
    "cer_file" : "wldb.jks",
    "cer_pwd" : "test123",
    "token_cache_minutes" : 15
}
```

3.2.2 内部资源映射配置项

下面是内部资源映射配置项的一个实例，JSON 格式，各数据域含义见表 3。

表3 内部资源映射配置项各数据域含义

数据域	含义
project	所属项目名称
desc	内部资源描述
inner_url	内部资源访问相对地址
content_type	请求响应的数据格式，包括xml, json, text三种格式
char_set	请求响应字符集
params	请求参数集合，为JSON数组
params.name	请求参数的名称
params.type	请求参数的数据类型，包括string, int, decimal三种类型
params.seq	请求参数的顺位

```
{
    "project" : " wldb_app",
    "desc" : " 获取最新的 N 条网络电报 ",
    "inner_url" : " WebServices/TSApiService.asmx/GetTelegraphListTopN",
    "content_type" : "xml",
    "char_set" : "UTF-8",
    "params" : [
        {"name" : "dw_code", "type" : "string", "seq" :1},
        {"name" : "n", "type" : "int", "seq" :2}
    ]
}
```

3.2.3 外部接口URL格式

代理程序的配置部分根据项目及内部资源映射配置，自动为每个内部资源生成互联网访问接口 URL，外部系统通过调用接口 URL，实现内部资源的访问。接口 URL 格式：

http://[agent_ip]:[port]/[project]/[inner_url]。

[agent_ip]：运行代理程序服务器 IP 地址；

[port]：运行代理程序服务端口；

[project]：项目名称；

[inner_url]：内部资源的相对访问地址。

3.3 路由时序设计

路由部分由路由解析、路由转发、配置读取以及认证部分 Thrift 客户端 4 个模块组成，具体路由时序设计如图 5 所示。

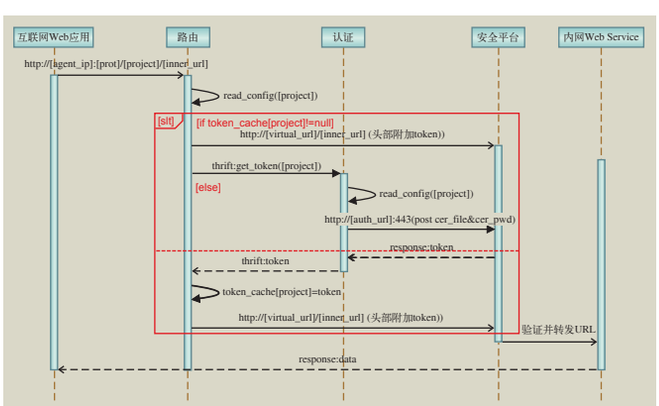

图5 代理程序路由时序图

3.4 认证设计

为了提高性能，认证与路由之间内部通信没有使用 HTTP 协议，而是使用了基于 Thrift 的 RPC 协议。Thrift 是一个跨语言的服务部署框架，2007 年由 Facebook 开发，2008 年成为 Apache 开源项目。认证部分 Thrift 服务端采用 Java 语言编写，路由部分使用 Python 语言编写 Thrift 客户端。Thrift 服务端代码略。

3.5 日志设计

代理程序有两类日志：(1) 错误日志，记录程序运行中出现的错误信息，便于分析产生错误原因及定位出错位置；(2) 性能日志，记录认证及路由过程消耗的时间，便于确定程序性能瓶颈。认证部分日志工具采用了开源日志组件 Log4j，路由部分日志工具使用 Python 自带的 Logging 日志模块。代理程序日志分析统一使用了 Python 语言自行编写的分析工具。

4 结束语

本文主要研究了通过互联网访问铁路内部资源的原理及一般实现方法，并详细阐述了穿越安全平台代理程序的设计思路。随着互联网访问铁路内部网资源项目的逐渐增多，代理程序实现的无需编程及灵活配置的优势将日益显现，如今代理程序已经作为哈尔滨铁路局网络电报手机 APP 及数字哈局等项目的基础设施，发挥着重要的作用。

参考文献：

[1] Deepak Vohra . Java 7 JAX-WS Web Services[M]. Birmingham: Packt Publishing, 2012.

[2] Kristina Chodorow. MongoDB 权威指南 [M]. 2 版 . 北京 : 人民邮电出版社，2014.

[3] 李 亮，尹逊政，孟 军 . 基于安全平台裁决的 ATO 系统冗余设计与实现 [J]. 铁路计算机应用，2014，23 (2) : 32-35.

[4] Miguel Grinberg . Flask Web 开发 : 基于 Python 的 Web 应用开发实战 [M]. 北京 : 人民邮电出版社，2015.

[5] 廖天成，王 博，何化石 . 运输全过程管理系统中列车运行图数据接口的设计与实现 [J]. 铁路计算机应用，2013，22 (2) : 24-26.

责任编辑 王 浩

(上接 P64)

(3) 自定义函数

自定义函数是设计者自己定义的一组脚本函数。脚本编辑器中提供的系统定义函数无法满足制作需求时，设计者可以根据需求自行编写调用函数。

自定义函数一般在控件属性的脚本（例如：鼠标点击）中写入命令，脚本中可写入的命令和触发函数命令一样，在此不再赘述。

VRP 交互功能设计的过程为：在创建模型级别下的相机中创建好所需的数个相机；在时间轴级别下设置好所需的时间轴；在初级页面、高级页面下设置好所需的控件、对话框。先新建完成系统函数写入所需命令语句，双击 Exe 文件后呈现模型、场景及其控件、对话框，然后逐一在各个模型、控件脚本中写入各种命令实现所需功能。脚本命令有：切换相机，实现所在模型、场景和其它模型、场景的相互切换；显示隐藏物体、控件等，实现切换相机后所需物体、控件的显示和不需物体、控件的隐藏；顺序、倒序播放时间轴，实现顺序拆分、组装模型；设置定时器等。简而言之，机车模拟驾驶训练系统的交互功能设计就是设计者在场景中各模型、控件脚本中各种命令按逻辑思维顺序写入、调用的过程。

5 结束语

本文主要对基于 VRP 的虚拟场景漫游系统的构建与实现进行了研究，总结了机车模拟驾驶训练系统的开发过程和技术，该系统实现了场景较为复杂的机车驾驶及其在三维场景的行驶，可以较好地培养司机学习机车驾驶的安全操作规程和应急处理能力。当然，本文用于机车行驶的操作仅限于鼠标、键盘，今后将在这一方面继续完善，对机车的外部操作将使用电控制动控制器 (大闸)、停放制动按钮、脚踏沙阀等实际机车设备，力求操作者在机车驾驶中有更真实可信的体验。

参考文献：

[1] 赵 青，李欣亮 . 基于 3DSMAX 的虚拟现实建模技术研究 [J]. 电子技术与软件工程，2016 (2).

[2] 刘广文 . 基于虚拟现实技术的机车驾驶模拟演练系统的研究与实现 [J]. 铁路计算机应用，2016，25 (4) : 55-57.

[3] 范书恒，宋亚夺 . 基于虚拟现实技术的车站站场建模关键问题的研究 [J]. 铁路计算机应用，2015，24 (6) : 14-16.

[4] 张 菁，张天驰，陈怀友 . 虚拟现实技术及应用 [M]. 北京 : 清华大学出版社，2011 : 1-4.

责任编辑 王 浩