计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2022,31(8):133−139 [doi: 10.15888/j.cnki.csa.008599]

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

气象业务流可信交互架构①

鲍磊磊[1], 吴锐涛[1], 胡　伟[2], 林　应[1]

[1](南通市气象局, 南通 226001)
[2](北京网御星云信息科技有限公司, 北京 100089)
通信作者: 鲍磊磊, E-mail: 10920561@qq.com

摘　要: 在不同安全等级的网络中, 由于缺乏标准的气象信息传输机制, 数据难以有效安全交互. 结合多样的业务应用需求, 基于“2+1”模型结构, 设计了物理隔离网络间的气象业务数据流可信交互框架体系, 部署在气象内网和其他网络的 DMZ 区, 跨区域实现数据安全传输和共享. 文中首先介绍了可信交互的体系架构, 然后结合具体气象业务需求开展了应用研究, 最后进行了系统功能、性能和安全测试, 并对可信交互架构的传输瓶颈和带宽利用率进行了分析. 该研究对应用可信交互架构提高异构网络间数据流的传输效率具有指导意义.

关键词: 可信交互; ASIC; TCP/IP 协议; SSL 加密

引用格式: 鲍磊磊,吴锐涛,胡伟,林应.气象业务流可信交互架构.计算机系统应用,2022,31(8):133–139. http://www.c-s-a.org.cn/1003-3254/8599.html

Trusted Interaction Architecture for Meteorological Service Streams

BAO Lei-Lei[1], WU Rui-Tao[1], HU Wei[2], LIN Ying[1]

[1](Nantong Meteorological Bureau, Nantong 226001, China)
[2](Beijing Leadsec Technology Co. Ltd., Beijing 100089, China)

Abstract: Effective and safe data interaction across networks of different security levels is difficult due to the lack of a standard meteorological information transmission mechanism. Considering the diverse service application requirements, this study draws on the “2+1” model structure to design the architecture of the trusted interaction of meteorological service data streams across physically isolated networks. This architecture is then deployed in the demilitarized zones (DMZ) of the meteorological intranet and other networks to achieve safe data transmission and sharing across regions. After the trusted interaction architecture is outlined, application research is conducted according to specific meteorological service requirements. Finally, system function, performance, and security tests are carried out, and the transmission bottleneck and bandwidth utilization of the trusted interaction architecture are analyzed. This research can guide the practice of applying a trusted interaction architecture to improve the transmission efficiency of data streams across heterogeneous networks.

Key words: trusted interaction; ASIC; TCP/IP protocol; SSL encryption

随着气象预报、预警和服务业务的拓展, 越来越多的信息系统需要在互联网部署针对性的应用, 例如突发事件预警、航空气象服务系统等. 这些系统的数据库大都在气象内网, 但是同时又要和互联网进行业务流交互[1–3]. 如果在外网再开发一套支撑互联网应用的系统不仅增加了开发成本, 造成硬件资源的浪费, 同时将业务应用部署在信息外网会带来信息发布、网络和数据等安全隐患[4–6]. 因此, 如何在保障系统安全的基础上, 针对气象业务应用, 设计出一套可信交互架构, 实现异构网络间的高效访问和数据同步, 优化气象业

① 基金项目: 江苏省气象局青年基金 (KQ202124)
收稿时间: 2021-10-26; 修改时间: 2021-11-29; 采用时间: 2021-12-08; csa 在线出版时间: 2022-05-30

务流传输机制, 成为气象信息化和网络安全业务的重要研究难题.

1 体系架构设计

1.1 硬件架构

气象业务流可信交互系统的硬件架构如图 1 所示.

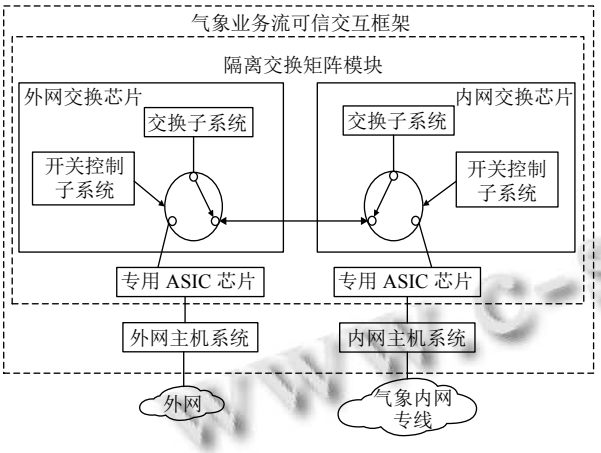

图 1 可信交互系统硬件架构

采用“2+1”模型结构设计, “2”是内网和外网两个主机系统, “1”是指一个隔离交换矩阵模块. 内、外主机系统的作用是: 获取数据包、拆解 TCP/IP 协议和安全检测. 隔离交换矩阵基于内、外网双通道设计, 每个通道由专用 ASIC 芯片和交换芯片组成. 其中, 交换芯片由交换子系统和开关控制子系统构成, 实现对数据流的安全交换和临时缓存. 隔离交换矩阵模块通过开关控制子系统控制开关左右摆动, 实现内、外网交换芯片完成两次同步摆渡过程[7].

第 1 次摆渡是: 内、外网交换芯片交换子系统彼此之间断开连接, 通过开关控制子系统建立各自主机系统、专用 ASIC 芯片和交换子系统三者之间的连接, 各自主机系统通过专用 ASIC 芯片将数据块封装成私有协议数据包写入交换子系统或反向读取交换子系统缓存数据.

第 2 次摆渡是: 内、外网交换芯片通过开关控制子系统断开各自交换子系统和 ASIC 芯片的连接, 交换子系统彼此之间建立连接, 实现数据交换.

两次摆渡过程, 内、外网都不会直接物理连接, 另外专用 ASIC 芯片内部固化了多线程并行处理程序, 自动完成数据块自有协议的封装或拆装, 因此, 内、外网主机系统之间没有基于网络协议的数据交换, 从而保证了内、外网之间的可信交互[8].

1.2 软件架构

可信交互系统软件架构如图 2 所示, 数据包获取后, 标准传输协议被阻断并经网络层和应用层安全检测后, 进行协议重组. 通过系统内核驱动程序和隔离交换控制程序, 实现可信交互系统内部数据流高速全双工交互的基本功能. 采用模块化的设计, 将其封装成系统基本功能模块.

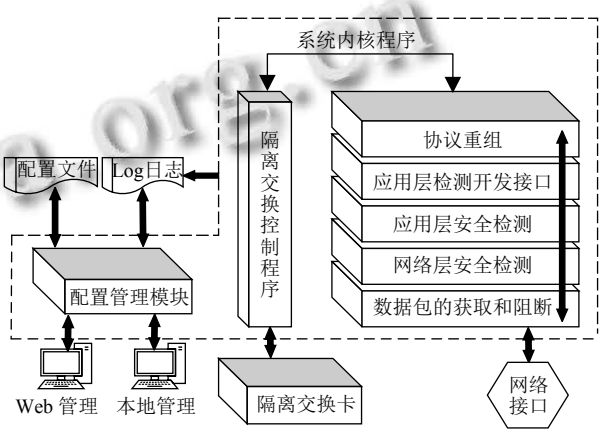

图 2 可信交互系统软件架构

其他功能模块主要分为: 系统模块、访问类和同步类模块 3 类, 都基于系统基本功能模块开发, 如图 3 所示. 其中访问类模块在对 TCP/IP 协议还原的基础上, 对常用的应用层协议进行独立开发, 供用户根据不同的需求选用. 另外提供非常规端口的用户定制访问和安全通道服务.

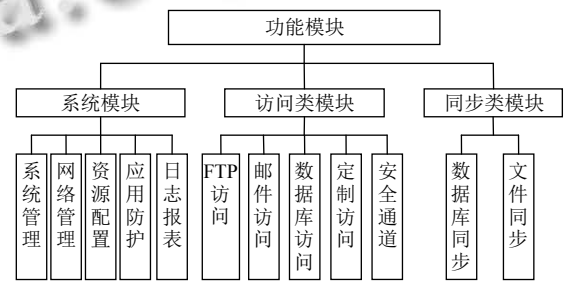

图 3 软件功能模块

1.3 关键技术

为提升系统的性能, 实现多源异构网络下的气象业务流高速交互, 基于专业集成电路 (ASIC) 芯片进行编程开发, 实现了以下核心技术应用.

多网隔离技术: 为解决气象内网需要同时与多个外网建立业务流可信交互的需求, 通过 ASIC 芯片的某

一或多个固化通道建立内网主机系统的某一网口与外网主机系统的某一或多个网口的对应关系, 从而实现一对一或一对多的网络隔离交换. 外网主机系统自身的多个网口禁止互访[9].

协议处理技术: 为解决通用协议和私有协议之间线性转换. 隔离交换矩阵模块上的 ASIC 安全隔离芯片通过硬件固化处理程序实现通用协议数据块和自有协议格式数据包之间的相互转换.

双摆渡传输技术: 为解决内、外网交换子系统之间或交换子系统与主机系统之间的双向数据高效交换. 通过开关控制系统和 ASIC 芯片实现两次摆渡传输过程.

并行处理技术: 为解决多网络接入时, 气象业务流摆渡过程中存在带宽瓶颈问题. 隔离交换矩阵模块上的 ASIC 安全隔离芯片采用了多线程并行处理技术, 提供了多个安全通道供内、外网之间的数据流交互.

链路聚合技术: 为解决外网与内网多对一访问时, 外网主机系统与内网数据传输过程中的带宽瓶颈问题. 通过主机系统的链路聚合技术将多个物理链路聚合成为一个逻辑链路进行数据交互[10].

2 可信交互结构的典型应用

2.1 气象业务流交互需求

气象信息网络主要分为: 气象业务内网、电子政务网、互联网和物联网 4 类. 各类气象业务信息系统主要部署气象业务内网 (简称内网), 并通过可信交互框架与电子政务网、互联网或物联网 (统称外网) 进行业务流交互. 在“云+端”的模式下, 采用智能手机、计算机等终端实现自动气象站维修、数据采集、移动巡检、计量检定、预警信息发布等业务. 以市局为中心节点, 气象业务流可信交互应用架构如图 4 所示.

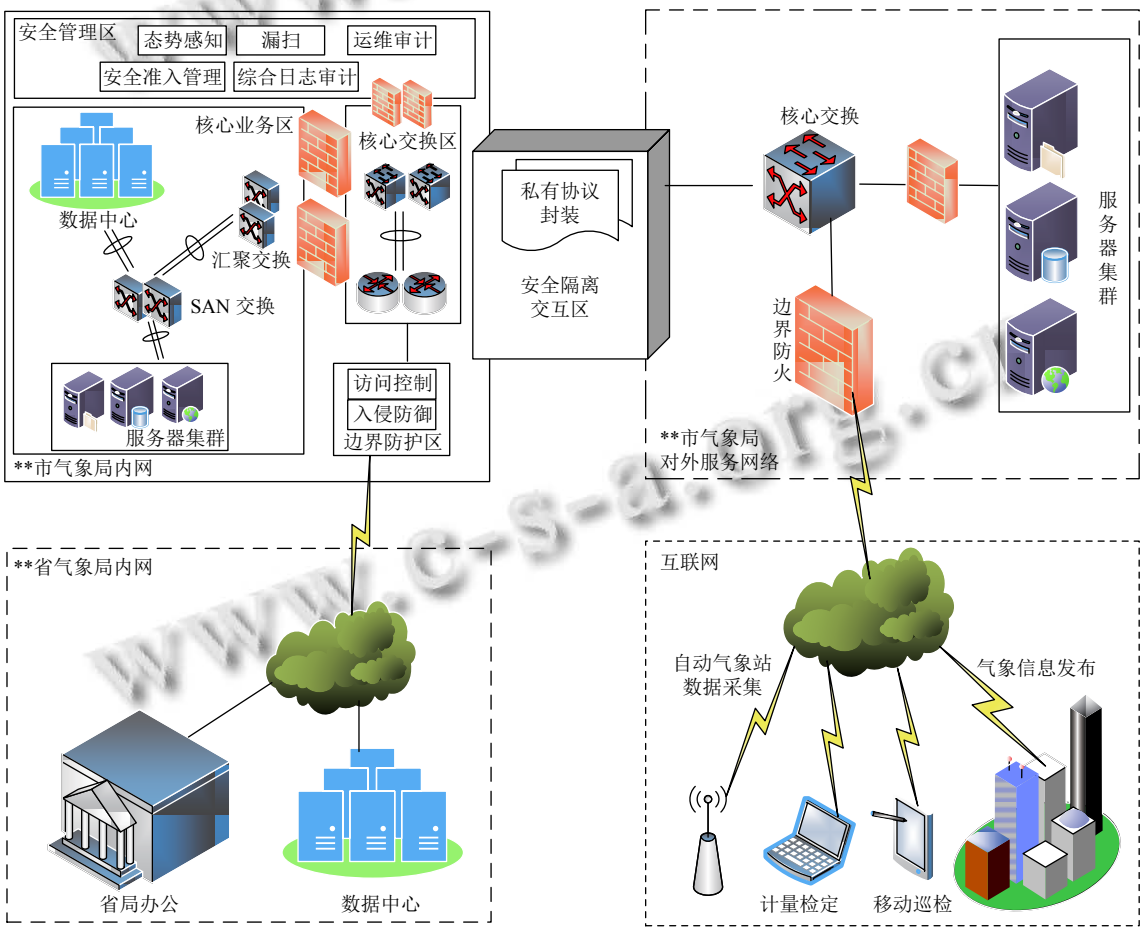

图 4 气象业务流可信交互应用架构

通过梳理, 主要的交互类应用可以分为以下两类:

(1) 访问类应用: 按照访问方向分为单向访问和双向访问两大类, 单向访问又分为内网访问外网和外网访问内网两种, 具体的应急需求如表 1 所示.

表 1 单向业务访问需求表

访问源	访问目的	具体应用
内网业务系统	公网短信接口	发送气象预警信息
	公网邮箱接口	发送气象服务邮件
	公网微博接口	发布气象服务微博
	公网传真接口	发布气象服务传真
	公网地图接口	GIS地图同步更新
外网业务系统	内网数据库	区域自动站巡检服务
	内网数据库	自动站计量检定系统
	内网数据库	自动站数据传输服务
	内网FTP服务端	气象内网数据获取
	内网业务系统	业务系统访问
	内网文件服务	文件共享应用

双向访问即: 内网需要访问外网的同时, 外网也要访问内网的业务, 通过梳理, 具体应用需求如表 2 所示.

表 2 双向业务访问需求表

具体应用	访问源	访问目的
公网气象GPS警报服务	内网气象警报服务端应用程序	外网GPS气象警报客户端
	外网GPS气象警报客户端	内网气象警报服务端应用程序和数据库
气象微信公众号预警信息推送服务	内网应用发布程序	外网气象微信公众服务程序
	外网气象微信公众服务程序	内网服务器应用程序

(2) 同步类应用: 分为气象监测、预报、服务和预警类文件同步和气象业务数据库同步两大类.

2.2 访问类可信交互架构

以内网访问外网的单向访问为例, 发起访问方为客户端, 被访问方为服务端, 整个气象业务流传输路径如图 5. 客户端按照标准的网络通信协议即 TCP/IP 协议 7 层体系通过内网发起访问请求, 在可信交互架构的内网侧经标准协议到私有协议转换后通过隔离交互矩阵将发起的请求传输到外网侧, 在外网侧再经私有协议到标准协议转换后将请求通过外网传送给服务端, 服务器收到客户端的请求后响应并处理. 至此, 完成一次单向的访问过程.

2.3 同步类可信交互架构

典型的气象业务流同步有文件同步和数据库同步两种方式, 他们的同步原理类似, 均通过在内、外网服务器中部署同步客户端软件, 源服务器为同步发送端, 目的服务器为同步接收端. 由客户端软件建立待同步的两台服务器之间的气象业务流交互, 整个数据传输全程采取 SSL 加密, 以确保数据同步的高安全性. 业务文件同步的流程如图 6, 气象数据库同步的流程如图 7.

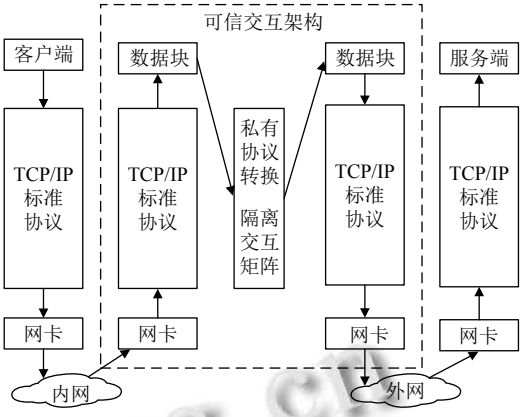

图 5 单向访问类功能示意图

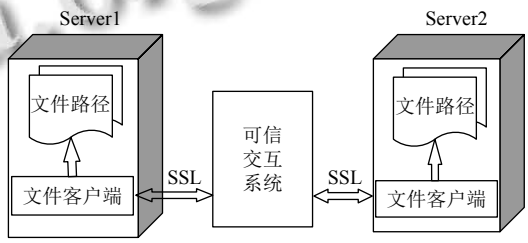

图 6 文件流同步类流程图

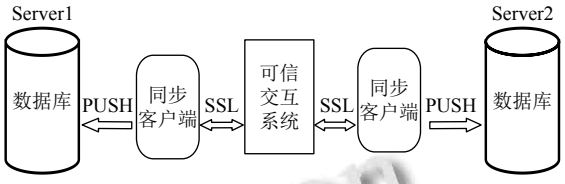

图 7 数据库同步流程图

2.4 同步客户端设计

(1) 功能设计: 同步客户端支持 Windows 和 Linux 多种系统版本, 在应用场景上支持单源多目的、多源单目的和多源多目的的实际应用环境, 支持单线程和多线程并发传输方式, 被传输的气象业务数据需经过内置的安全策略进行格式检查、内容过滤和病毒检测, 确保数据在同步过程中的数据类型匹配、数据冲突检测以及数据容错控制. 提供断点续传功能, 避免系统在断电断网过程中数据丢失; 设计采用增量传输方式, 减轻因网络带宽原因造成的传输压力. 客户端的功能框图如图 8.

图 8 中, 文件同步客户端支持常规 Office、可执行、压缩、图片、视频等多种文件传输, 同时能限制传输文件的格式, 有效放行或阻止特定格式的文件传输; 数据库同步客户端支持包括 SQL Server、Oracle、Sybase、DB2 等主流数据库中同种或异种数据库增量或全表同步传输.

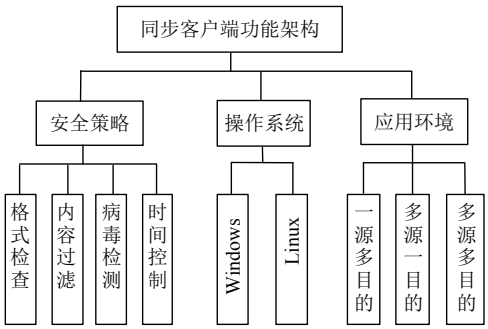

图 8 同步客户端功能框图

(2) 同步机制: 同步客户端软件部署在内、外网服务器上, 通过实时监控的机制监听发送端产生的数据变化, 并通过证书认证机制与可信交互架构建立连接, 将变化的气象数据流写到接收端. 如图 9 所示.

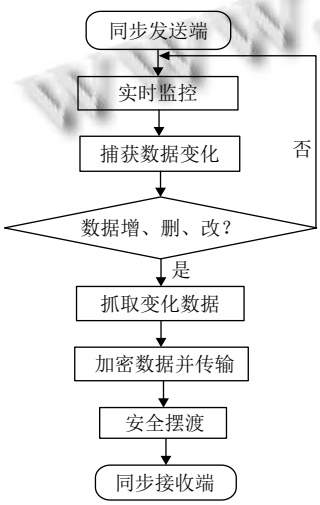

图 9 同步客户端同步机制

文件同步客户端, 采用实时监控文件的 open、close 状态, 第一时间捕获变化的文件. 数据库同步客户端的具体实现是由同步客户端在数据库中建立一个临时 data 表, 用于保存待同步任务的数据, 当所有任务的数据同步完成时, data 表中的临时数据就会自动清除, 等待下一个时刻查询待同步数据, 如此反复循环. 同步客户端展示实时同步的日志, 自动查询每个任务在临时数据表中的数据, 避免数据积压.

3 系统测试

3.1 功能测试

为验证该可信交互架构的访问类和同步类应用的有效性和实用性. 依据气象业务流可信交互需求, 通过配置可信交互架构的软件功能模块实现气象业务流交互, 常用的配置包括源 IP 地址、目的 IP 地址、可信交互入口、出口地址和服务端口, 常用的访问类模块有 FTP、邮件、数据库访问模块, 用户可以选择定制访问或安全通道模块自定义服务端口. 本测试以文件同步和数据库同步应用为例, 选择安全通道模块下普通模式的配置方式, 在同步客户端下配置待同步的任务进行测试, 文件同步功能测试结果如图 10 所示, 数据库同步功能测试结果如图 11 所示.

图 10 文件同步功能测试

图 11 数据库同步功能测试

3.2 性能测试

(1) 测试环境

基于可信交互架构的典型业务应用: 智慧航空气象保障服务系统的网络环境, 在气象内网和电子政务网交互气象数据的两端分别新建文件同步任务以及数

据库同步任务, 在文件传输任务的两端服务器创建对应的文件夹作为数据传输的源和目标路径目录, 在数据库同步任务的两端服务器创建相同的数据库系统和测试表. 内、外网两端的网络环境带宽均为 1 Gb/s.

(2) 测试方案

步骤 1. 预先规划好内网终端 Server1 和电子政务网终端 Server2 的真实 IP; 终端对应在可信交互出、入口的虚拟 IP 和测试端口.

步骤 2. 在终端 Server1 和终端 Server2 都安装同步客户端软件、时间测量软件和时间同步软件, 时间同步软件连接到标准时间服务器, 确保两端服务器的时间一致.

步骤 3. 按照第 2.3 节图 6 和图 7 进行物理连接, 并设置 Server1 为客户端模式, Server2 为服务端模式, 在交互设备配置业务流传输通道, 在两端的同步客户端软件上创建同步任务.

步骤 4. 启动气象业务流同步任务, 传输任务可以根据测试需要适当增加, 选择合适时间进行压力测试.

实际业务中为了网络安全, 端口默认关闭, 需在硬件防火墙上设置访问控制策略, 系统防火墙上分别配置端口的入栈或出栈策略.

(3) 测量结果及分析:

如表 3 所示. 并发数 100 和 200 是文件逐一传输, 传输的文件数量越多, 传输的速率越慢, 而对于并发数 300 和 400, 是将 300 和 400 个文件各自压缩成 1 个数据包进行传输测试, 因此传输速率相对较快. 经过业务环境的真实测量, 可以得出结论: 传输文件的数量与系统的传输速率成反比, 传输文件的大小并不影响系统的传输速率.

表 3 文件同步的测量结果

并发数	文件大小 (MB)	传输速率 (MB/s)	传输时间 (s)	传输通过率 (%)
100	948.34	105.4	9	100
200	1 898.38	99.9	19	100
300	3 072	105.9	29	100
400	4 075.52	107.3	38	100

以上测量结论对于判断可信交互架构的网络瓶颈和估计带宽利用率是非常有用的. 在实际应用中, 对于时效性要求不高的文件, 可以采用批处理程序将待传输的文件进行打包后传输, 传输采用增量传输的方式, 可以有效提高气象业务流的传输速率.

在异构网络两端的数据库上分别创建数据表 test1 和 test2, test1 插入 10 000 条记录, test2 插入 100 000 条记录. 并发数以数据表的记录数为单位, 由于结构化数据库本身的单个数据记录的大小很小, 因此将每秒通过交互架构的记录数作为测量指标更有意义. 经过 10 000 和 100 000 条记录的传输测试, 得到如表 4 的测试结果.

表 4 数据库同步的测量结果

并发数 (记录)	传输速率 (条/s)	传输时间 (s)	传输通过率 (%)
10 000	833	12	100
100 000	237	422	100

由第 2.4 节数据库同步客户端的设计机制: 同步任务启动后, 数据库中建立一个临时 data 表, 用于保存待同步任务的数据, 为了保证数据传输的稳定性, data 表每次最多只能完成 5 条数据插入, 即使传输速度很快, 数据也会存在排队等待时间, 此等待时间即为业务流传输的瓶颈. 通过 3 个月以上的实际业务运行得出结论: 正常情况下, 系统不会出现数据拥堵, 但受限于系统本身吞吐率和并发数等性能指标, 为追求传输的稳定性, data 表的缓存设计是有上限的, 可以通过定期清理或定期重启同步客户端软件释放缓存. 另外经常关注 data 表的数据排队情况, 对于业务流交互架构系统的运维有着重要的意义.

3.3 安全测试

采用网络安全攻防演练的模式, 基于网络层和应用层选取几种常用的网络攻击进行模拟攻击, 统计该可信交互架构的拦截率, 并与下一代防火墙的拦截率进行对比统计, 防火墙匹配访问控制策略、病毒和 IPS 特征库, 并升级特征库到最新版本. 测试结果如表 5.

表 5 系统安全测试结果 (%)

攻击类型	防火墙拦截率	可信交互架构拦截率
DDoS攻击	100	100
密码暴力破解	100	100
SQL注入	100	100
蠕虫病毒	100	100
扫描攻击	100	100

基于测试统计, 下一代防火墙设备对于基于网络层的攻击绝大部分可以拦截, 对基于应用层的攻击拦截需要匹配访问控制策略、最新的特征库基本才能实现 100% 的拦截; 可信交互架构对于各种基于网络层和应用层的模拟攻击实现了 100% 的拦截, 节省了下一代防火墙升级特征库的费用, 采用可信交互架构与多种安全防护设备联动可以达到更好的安全防护效果.

4 总结

气象业务流可信交互架构采用“2+1”模型结构设计, 实现了气象数据流在异构网络下的安全传输, 为气象信息系统提供便捷、安全的交互环境. 本文梳理了内、外网物理隔离后常见业务应用需求, 对访问类和同步类交互架构、同步客户端的功能和机制进行了详细分析, 最后结合具体业务应用开展功能、性能和安全测试研究, 测试结果表明: 传输文件的大小不会影响系统的传输速率; 待同步文件的数量与系统的传输速率成反比, 待同步数据库表的记录数和系统传输速率成反比. 压缩文件的传输结果表明: 可信交互架构的带宽利用率达到 80% 以上.

参考文献

1 黄姗姗, 蒋厚明, 胡牧, 等. 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. [doi: 10.15888/j.cnki.csa.007083]

2 林潇, 吴怡. 智能防御的私有云打印系统. 计算机系统应用, 2021, 30(7): 102–109. [doi: 10.15888/j.cnki.csa.007983]

3 王亚静. 电子政务网络安全隔离与数据交换技术的分析与研究 [硕士学位论文]. 西安: 长安大学, 2016.

4 吴缇. 基于物理隔离网闸的银行文件安全传输系统的设计与实现 [硕士学位论文]. 成都: 电子科技大学, 2013.

5 王婷, 顾海霞, 吴锵. 网闸技术在核电厂实时信息监控系统中的应用与改进. 测控技术, 2017, 36(9): 151–154. [doi: 10.19708/j.ckjs.2017.09.036]

6 钮卿. 双网隔离环境两级应用移动平台的设计与优化. 计算机系统应用, 2019, 28(2): 87–93. [doi: 10.15888/j.cnki.csa.006764]

7 于华楠, 武云瑞, 胡绪超. 正向隔离网闸在电力系统中的应用. 计算机与数字工程, 2014, 42(10): 1817–1818, 1847. [doi: 10.3969/j.issn1672-9722.2014.10.015]

8 李旋, 顾建新, 李毅. 网络安全专用产品网闸性能测试方法. 计算机系统应用, 2019, 28(1): 233–238. [doi: 10.15888/j.cnki.csa.006725]

9 曹旭东, 张实. 基于 FPGA 的高速网闸交换卡的设计. 科学技术与工程, 2013, 13(22): 6610–6615.

10 联想网御科技 (北京) 有限公司. 产品白皮书: 联想网御 SIS-3000 系列安全隔离与信息交换系统. https://wenku.baidu.com/view/ee808f38541810a6f524ccbff121dd36a22dc430.html. [2021-08-20].

(校对责编: 孙君艳)