中数国科安全隔离与数据交换平台产品白皮书

（中数国科集团）

【中数国科】

■ 文档编号	■ 密　　级
■ 版本编号　V19.1.31	■ 日　　期
■ 撰 写 人　李佳璠	■ 批 准 人

■ 版权声明

目录

一、前言

国家保密局 2000 年 1 月 1 日起颁布实施的《计算机信息系统国际互联网保密管理规定》对国家机要部门使用互联网规定如下：涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其他公共信息网络连接，必须实行“物理隔离”。所谓“物理隔离”是涉密的内部局域网在任何时间都不存在与互联网直接的物理连接，企业的网络安全才能得到真正的保护。

随着互联网的迅速发展，各政府和企事业单位利用互联网开展工作已成为不可逆转的趋势，各个机构都需要在内网和互联网之间进行大量的信息交换，以提升工作效率。从而在网络安全和效率之间产生了巨大的矛盾，而且矛盾日渐扩大化。网络隔离的目的是为了保护内部网络的安全,而网络互连的目的是方便高效地进行数据交换。

在实际工作中，低安全域向高安全域、非密向低密、低密向高密网络信息系统自动上传的数据需求非常强烈，如：各种公文、邮件等向内部涉密网络的自动传递、工作人员在互联网查询到的资料信息向涉密网络的自动传递、涉密监管机构利用自动化工具从互联网端搜集的敏感信息向涉密网络的自动传递等。这些数据种类繁多、数量巨大，如果采用传统光盘摆渡机的形式不仅造成巨大的资源浪费，而且效率低下，相应的人员、系统无法及时得到对应的信息。近年出现的 USB 摆渡机、机械臂摆渡机等，由于天然的低效率，仍然无法解决大数据量实时传输到涉密网络中的客观应用需求；安全隔离设备虽然可以解决数据的实时传输，但是由于计算性能的劣势，使其在启用所有安全策略的情况下，摆渡效率降低并且有出现丢数据的情况。

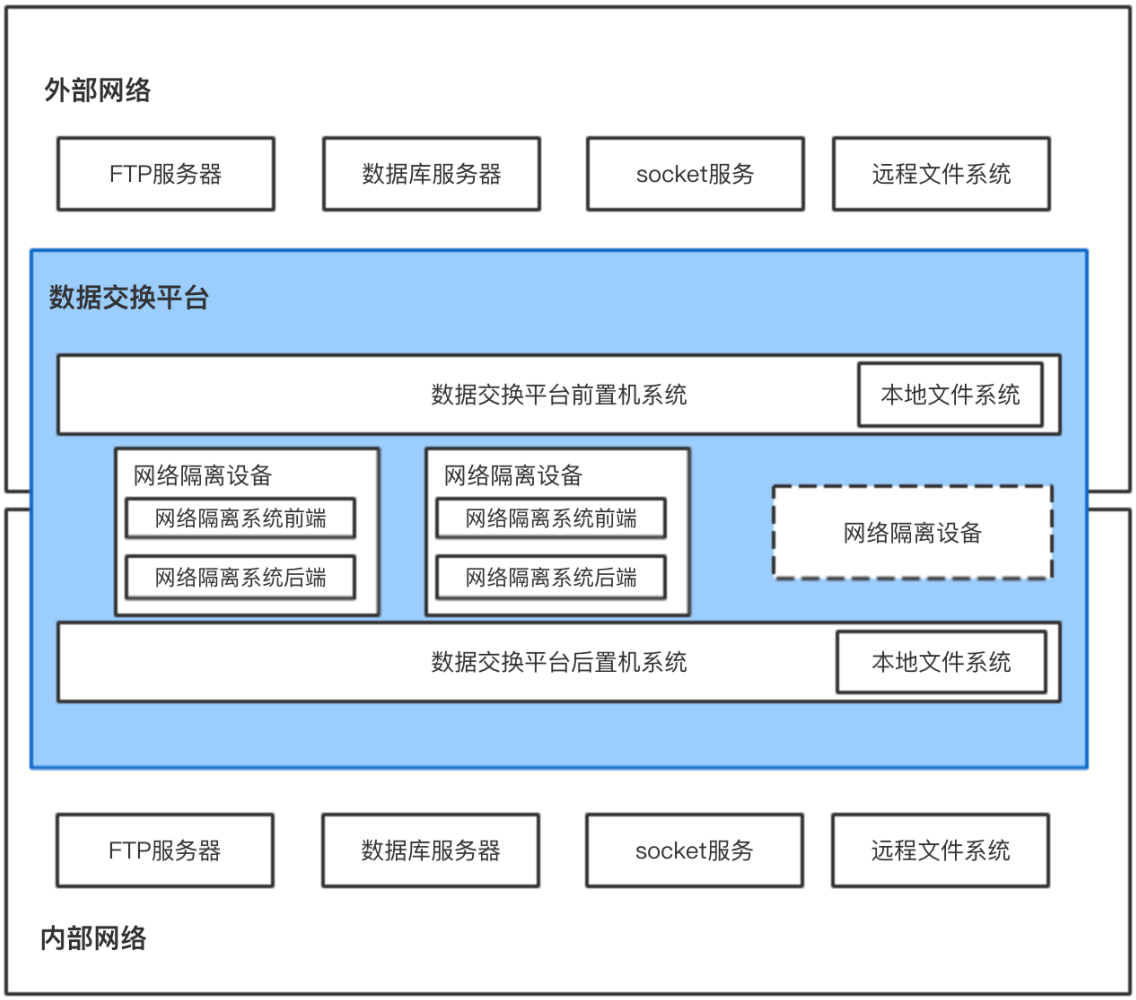
二、产品介绍

2.1. 产品简介

中数国科安全隔离与数据交换平台（以下简称“交换平台”）是由中数国科集团自主研发的、具有自主知识版权的隔离和交换类设备。其由前置机、安全隔离设备（网闸或光闸）、后置机三部分组成，提供文件同步、数据库同步、音视频同步和服务代理等安全防护功能。产品基于策略进行设备认证、格式检查、内容过滤和病毒查杀等防护手段，将数据安全摆渡，实现网间数据的高安全交换。

2.2. 产品组成

数据交换平台采取软件分层的思想设计整个系统，具备伸缩性、可维护性、可扩展性、可重用性和可管理性。数据交换平台从部署方式上，分为前、后置机、网络隔离前、后端共4个子系统。



前置机和后置机在客户的外、内网分别部署，分别与外网、内网的业务网络通信，解决数据的大量、高效、单向、稳定的传输。

前置机与用户计算机或服务器建立可信连接，实现源身份和权限鉴别。获取低安全域中新的待传输文件/数据，进行包括病毒、文件格式等安全检查，并根据设置的安全传输策略进行文件/数据传输任务整合，实现审计及链路监控，最后将待发任务信息通知后置机。

后置机通过身份和权限鉴别，可为指定接收用户推送或提供文件/数据，实现数据的外发。

中间安全隔离设备主要实现用户数据从前置机和后置机之间的数据传输，提高了不同安全域间数据交换的安全性。

三、产品功能

中数国科安全隔离与数据交换平台作为边界隔离数据交换的产品解决方案，其承载的业务数量及数据流量均超越了以往边界隔离数据交换产品，摒弃了隔离设备产品上不应该承担的、具有威胁性的双向数据流代理业务，强化了数据交换功能。

3.1. 数据库同步

中数国科安全隔离与数据交换平台支持数据库抓取及推送功能。自动从外网指定数据库服务器中抓取需要传输的数据库变化信息进行数据库传输。

数据库同步模块实现数据库推送功能，系统根据通道选择决定将信息推送给目标数据库。支持多种主流数据库，包括 Oracle、Mysql、Sqlserver、人大金仓 Kingbase、PostgreSQL、DB2、达梦 DM、南大通用 Gbase、神舟通用 Oscar、MARIADB、优炫 UXDB、Sybase，支持数据库同构、异构传输。

3.2. 文件同步

中数国科安全隔离与数据交换平台支持文件同步功能。由前置机主动发起的文件传输请求（主动模式）或被动接受客户机的文件传输请求（被动模式），从外网中获取需要传输的文件，并根据用户配置决定是否存储到本地，可在文件传输过程中加入完整性校验信息保证文件完整性，然后将文件推送到对应网络指定的文件服务器，或在后置机上建立文件服务，等待对应网络特定业务系统来提取文件。协议支持 FTP、SFTP、SAMBA、SFTP、FTPS、SCP，以及专用私有协议 SUTP 等，支持文件同步任务模式、传输带宽设置等。

3.3. 音视频同步

中数国科安全隔离与数据交换平台文件交换支持音视频传输功能，支持的协议有RTSP、RTMP、HLS、SIP、GB28181、H323、ONVIF。支持基于 TCP 或 UDP 协议的 SIP 代理和平台互联、SIP 视频代理，支持基于 TCP 或 UDP 协议的 GB28181 平台互联，支持 H323 代理和平台互联模式。支持加密传输通道，保障传输的安全性；用户可根据实际情况配置指令级别访问控制。

中数国科安全隔离与数据交换平台还具有 ONVIF 客户端功能，通过模拟摄像头的功能可实现视频流的单向传输，在不同网络安全域间严格单向传输的业务场景中可以满足用户的使用需求，保障视频流传输的安全隔离性。

3.4. 服务代理

中数国科安全隔离与数据交换平台和安全隔离设备之间的服务代理，通过在前置机与后置机之间建立安全传输链路，进行 TCP、UDP 协议的服务代理。传输类型支持单播、广播、组播。支持 HTTP、FTP、POP3、SMTP 多种应用层协议的代理传输，支持对应用层协议传输的深度过滤及病毒查杀功能。

3.5. WEB 服务调用

中数国科安全隔离与数据交换平台提供 WEB 服务调用功能，基于 SOAP 协议实现 WEB 服务代理。在打通 WEB 访问通道同时，对数据进行过滤和控制，保护内部网络信息。WEB 服务调用支持命令级的访问控制，支持对数据内容检查及过滤。

3.6. 内容检查

内容检查是指前置机对接收到的文件和信息进行安全性检查，确保只有符合保密、安全策略的数据、文件才允许被单向传输至后置机。

敏感词检查：前置机可依据管理员设定的涉密或不健康的信息进行过滤，将过滤到敏感词信息拦截并记录日志，支持内置敏感词库及用户自定义敏感词库。

文件类型检查：前置机对可能产生危险的文件真实类型进行检查、过滤、删除并且记录日志。

黑白名单检查：前置机可依据管理员设定黑白名单对文件进行阻断或通过。

3.7. 病毒防护

中数国科安全隔离与数据交换平台的前置机可针对用户上传的文件进行检查，在确保没有病毒的情况下才被转存到安全数据区。当发现病毒后，系统会将病毒文件阻断传输，并记录日志供安全管理员追溯。系统集成了双病毒引擎对文件落地业务进行病毒查杀。提供病毒库升级功能。

3.8. 监控与审计

中数国科安全隔离与数据交换平台提供强大的日志和审计功能。设备内置日志存储空间，支持标准 SYSLOG 日志格式发送到远端日志服务器，为日志审计提供了很好的数据支撑和方便性。日志完整记录了异常行为、管理行为、业务日志等各类信息，能够使管理员以多种方式进行查询、审计。系统具有按日志类型进行导入、导出、备份等功能，保证了日志信息的安全性与易用性。

四、产品亮点

4.1. 数据传输安全性高

中数国科安全隔离与数据交换平台采用专有的安全通道，即在前置机、后置机以及安全隔离设备之间采用私有协议的加密传输，保证数据传输的高安全性。产品设计采用摆渡传输方式，从物理上断开内外网连接。绝大多数基于网络的攻击行为都通过物理层以上的网络链路级（IP、传输层等）攻击回路来进行实施，只要断开内外网络之间的物理连接，包括利用电路和芯片级后门、漏洞在内的所有外部攻击将无能为力。

4.2. 业务交换可控性高

为达到安全可控传输的目的，中数国科安全隔离与数据交换平台在传输过程中结合自身的过滤规则以及安全隔离设备对数据进行检查和过滤，防止非法信息传输；传输的数据经过安全隔离设备检查，是已经完全剥掉所有控制信息的符合格式要求的原始数据文件，因此被认为是安全的，同时交换平台支持双病毒引擎等安全模块，能够有效阻挡病毒文件传播。

中数国科安全隔离与数据交换平台业务传输功能集成了指令级别的访问控制，保证数据的受控交换。

4.3. 传输方式功能全

中数国科安全隔离与数据交换平台具备文件同步、数据库同步、服务代理、音视频代理、WEB 服务调用等功能，交换平台的通道提供流模式和文件落地两种方式，同时支持安

全隔离设备自动向交换平台注册通道，进行数据传输。交换平台支持主动、被动、混合等多种提供服务的方式，能够满足客户各种数据交换场景的需求。此外还支持安全控制功能、审计管理功能、运行监控功能等，功能丰富全面、图形化显示直观，能够为客户提供完善的安全和运维支撑能力。

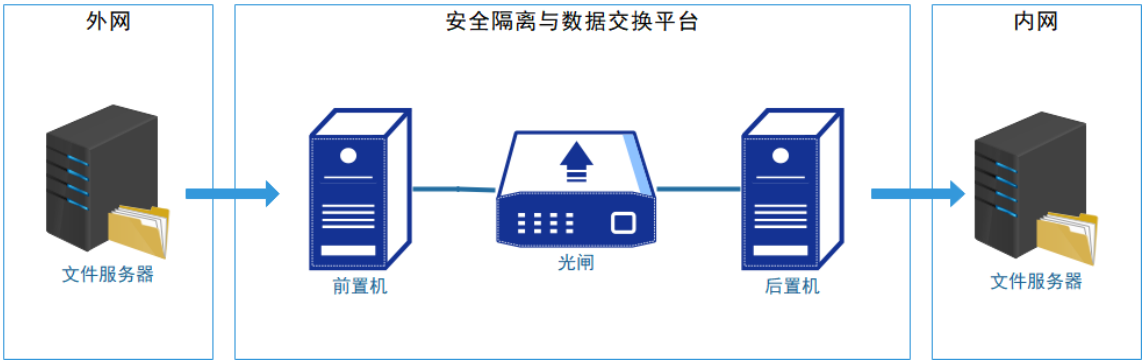
五、部署场景

中数国科安全隔离与数据交换平台通常部署在两个不同的安全域之间，主要用来将低安全域的数据单向传输至高安全域的业务系统中。

低安全域可为低密或非密网络，高安全域通常为业务专网或涉密网络。中数国科安全隔离与数据交换平台实现低安全域向高安全域的可控数据传输。

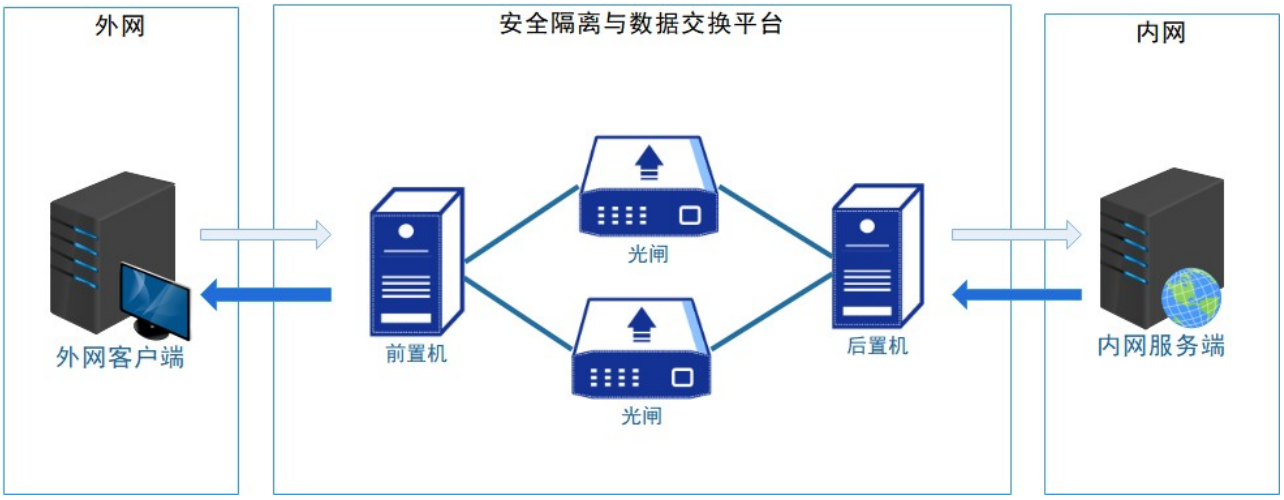
5.1. 单向光闸部署场景

部署场景 1：数据交换平台前置机+单向光闸+后置机



5.2. 双单向光闸部署场景

部署场景 2：数据交换平台前置机+双单向光闸+后置机



5.3. 双向网闸部署场景

部署场景 3：数据交换平台前置机+双向网闸+后置机