中数国科安全隔离与信息单向导入系统产品白皮书

（中数国科集团）

【中数国科】

■ 文档编号	■ 密　　级
■ 版本编号	■ 日　　期
■ 撰 写 人	■ 批 准 人

■ 版权声明

目录

一、前言

自上世纪 90 年代以来，信息技术迅猛发展，人们的生活、工作方式发生了巨大变革，信息网络的大规模应用极大提高了办公效率。经过多年建设，我国已建成相当规模的数字化网络。随着网络的不断普及，网络信息安全问题成为威胁国家和政府安全的重大隐患。经过对安全问题的不断认识和了解，党和政府已将信息安全建设提到相当高的程度，并加强针对涉密信息的防护。

2000 年以来安全隔离技术作为一项新兴的网络安全技术，在保障国家信息安全，尤其是政府、军队及重点行业等信息系统安全建设方面发挥了重要的作用。2000 年 1 月国家保密局在《计算机信息系统国际联网保密管理规定》中规定，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相联接，必须实行物理隔离。2007 年 3 月国家保密局和国务院信息化工作办公室在《电子政务保密管理指南》中规定，涉密网络不能与互联网直接连通；若非涉密网络与互联网是逻辑隔离的，则采用单向网闸隔离涉密网络与非涉密网络，保证涉密数据不从高密级网络流向低密级网络。在涉密网络中允许低密数据传输到高密网络，但不允许高密数据传输到低密网络。

防火墙、入侵检测类产品虽然能够满足一些安全需求，却无法解决涉密网络间的保护问题。对于涉密网络，需要防止任何泄密的可能，实现低密级网络向密级网络单向导入数据成为一个亟待解决问题。

中数国科集团在安全实验室经过大量实验论证后，认为光纤传输在实现单向控制方面可以满足隔离的要求。光纤传输利用发光端为源、感光端为目的，进行信息单向无反馈传输，具有传输效率高、稳定性高，以及经济实用的特点。经过公司多年的实践经验，研发

出中数国科安全隔离与信息单向导入系统产品。

二、产品概述

中数国科安全隔离与信息单向导入系统（以下简称“单向光闸”）是由中数国科集团自主研发、具有自主知识版权的单向导入产品。其基于“2+1”的硬件架构，由外网处理单元、内网处理单元与光单向传输单元组成，提供文件交换、数据库同步、邮件转发、组播中继、访问控制、数据内容审查、安全管理通信等功能，并有着业务双重防护、稳定、高可用等特点。

单向光闸硬件架构上采用物理单向传输。外网处理单元、内网处理单元采用特殊安全电路设计，具有极高的稳定性与可靠性。光单向传输单元包括专用安全传输控制硬件和定制光发送模块、光接收模块，光发送模块只具有单一的数据发送功能，光接收模块只具有单一的数据接收功能。光发送模块和光接收模块之间通过单向光纤连接，此单向光纤是连接外网处理单元、内网处理单元之间唯一的通道，在物理上达到数据流向的单向无反馈。信息只能由一个安全域向另一个安全域传输，并保证反方向无任何信息传输或反馈。

单向光闸软件架构结合传统安全隔离的“摆渡+代理”技术。外网处理单元连接数据发送方，内网处理单元连接数据接收方。外网处理单元收取发送方数据，将数据发送方网络信息流剥离协议，处理后的数据通过光单向传输单元、以单向发送的方式导入到内网处理单元，内网处理单元将数据重新封装后，发送至内网数据接收方，或在设备中实现备份。在保障信息单向传输的同时，最大限度实现信息的实时传输和安全可控。下面以信息流由外网到内网图示为例，说明了通过单向光闸的信息传输过程。

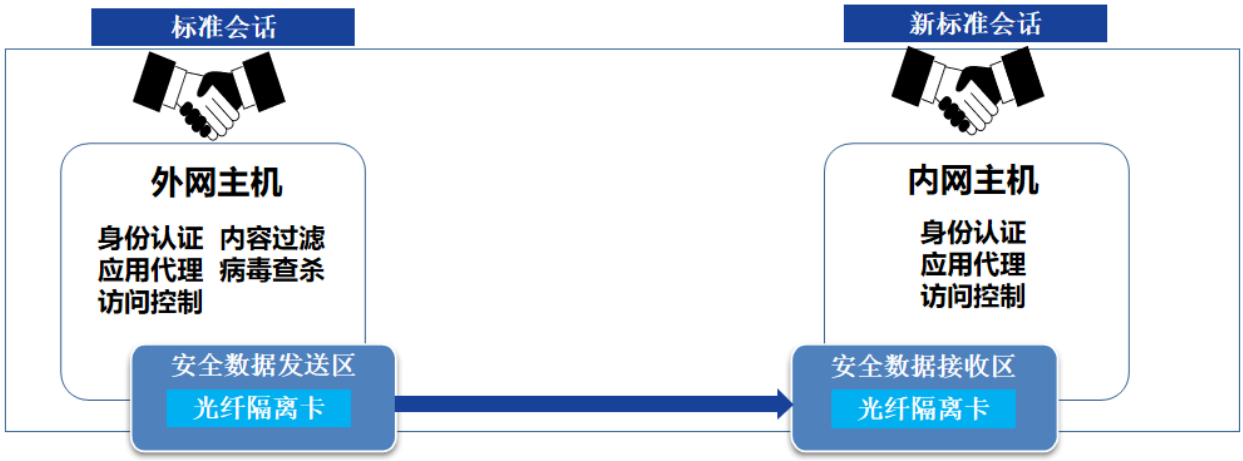

图 1 单向光闸信息传输过程

三、产品功能

单向光闸的主要功能特点就是在保证两个网络隔离的情况下，做指定的单向数据安全传输。单向光闸基于单向传输部件，结合传统安全隔离网闸的“摆渡+代理”技术，实现文件交换、数据库同步、邮件转发、组播中继、访问控制、数据内容审查等功能。在保证单向数据传输的同时，实现数据的实时、准确、可控传输。

3.1. 信息交换

中数国科安全隔离与信息单向导入系统的基于信息交换的工作模式，即由外网处理单元接收来自外网业务系统的发送数据请求，内网处理单元负责接收来自外网处理单元的信息，并将信息提交至内网业务系统的目标服务器。

TCP/UDP 应用层：通过系统内部的 TCP/UDP 代理处理模块，单向光闸能够实现代理外网客户端发送的 TCP/UDP 会话，并将应用层数据进行白名单格式的检查。对于符合规则的应用数据单向传输至内网处理单元，对于不符合白名单规则的会话将日志报警并断开会

话。内网处理单元对于从外网处理单元发送过来的数据根据任务号可发送给相应的服务器。

通用文件信息交换：通过系统内置的 FTP、NFS、SMB 文件交换模块，中数国科安全隔离与信息单向导入系统能够实现主动到外网服务器抓取文件并向内网的服务器上传文件。管理员可设置文件传输完成后是否删除源文件。

专用文件信息交换：通过系统内置的专用文件传输模块，中数国科安全隔离与信息单向导入系统能够实现外网向内网进行私有文件的安全、单向传输。客户机通过管理控制台分配的账号，使用专用协议文件客户端软件上传或下载文件。每个账号均有自己的私有目录空间，另外系统提供一个公共空间以供所有用户使用。

邮件中继：系统内置 SMTP、POP3、IMAP 邮件代理引擎，实现外网邮件服务器将邮件转发至光闸的外网处理单元，经过内容检查及单向摆渡后，内网处理单元会将邮件发送至客户内网邮件服务器中，从而实现外网邮件服务器到内网邮件服务器的中继转发。

数据库单向同步：通过系统内置或外置的数据库同步模块，光闸可实现外网向内网的单向数据库同步。数据库单向同步支持的类型包括：Oracle、Sqlserver、Mysql、Db2、Sybase、Postgresql 等国际主流数据库，同时也支持人大金仓、达梦等国产数据库的同步。支持异构数据库之间的同步，并支持按条件过滤。

组播单向代理：系统通过内置的组播代理，支持多种模式的组播单向代理传输。

光网联动：单向光闸系统支持与双向网闸进行联动，应用场景如视频环境：双向网闸传输双向信令，在光闸中传输单向视频流。

3.2. 访问控制

中数国科安全隔离与信息单向导入系统具有强大的访问控制力，包括如下几点：

网络访问控制：单向光闸可实现链路层、网络层、传输层访问控制，通过灵活组合网

络对象，制定与实际需求完全吻合的访问控制策略。

访问用户控制：单向光闸可实现定制、绑定哪些用户可以访问系统，对发送和接收数据流的主体进行身份鉴别，防止非法数据访问。

管理访问控制：单向光闸可通过订制访问策略，精细地控制“谁”（网络对象）、“能够”（允许或禁止）访问系统。管理控制台以人性化的人机交互界面协助管理员轻松实现管理目标。

3.3. 数据内容审查

单向光闸对接收的数据、文件进行安全性检查：对单向导入的数据内容进行病毒扫描阻断含病毒数据的导入；对单向导入的数据内容进行关键字检查，阻断非法数据的导入。确保只有符合保密、安全策略的数据、文件才被允许单向传输至内网处理单元。

3.4. 文件校验二次传输

由于单向光闸数据传输具有单向无反馈的特性，实时单向传输的数据可能出现部分丢失的情况，外网处理单元发送数据后无法判断内网处理单元接收的文件是否正确。中数国科安全隔离与信息单向导入系统采用独特的冗余数据算法，提供了传输记录的校验功能。管理员可根据时间、文件名进行筛选，导出接收记录，在外网处理单元导入记录并进行校验。当发现文件丢失或文件错误的情况，系统同时提供重传功能，最大限度地保证了数据的完整性。

3.5. 业务双重防护机制

中数国科安全隔离与信息单向导入系统采用双重安全防护机制：白名单和防病毒引擎

系统的内网处理单元、外网处理单元以白名单方式接受网络请求、建立、终止会话。所有的客户网络请求无法直接穿透单向光闸进入内网，只有经过安全检查、被允许的客户业务数据或文件才能被传输，否则将被视为无效数据，直接删除并丢弃，因此单向光闸能够隔离各种未知的安全风险。同时，单向光闸内嵌防病毒引擎，能够实时检测、阻绝已知的各种病毒与入侵，并在控制台示警，帮助管理员在最短时间内做出响应。

3.6. 安全的管理通信

中数国科安全隔离与信息单向导入系统只允许用户通过专用的独立管理控制端口进行管理，并可设置允许进行管理的设备地址。授权管理员经过身份鉴别后，采用多因素鉴别、加密方式建立与设备的连接。通信端口不接受任何管理请求，避免了管理信息的旁入可能。产品提供有设备初始化、备份恢复、自动备份等功能。

3.7. 权限分配方式

中数国科安全隔离与信息单向导入系统采取系统管理员、安全管理员与安全审计员角色分立的权限分配模式，各管理员之间权限互不交叉。系统也提供用户角色分配权限的策略，使用户管理更加方便且易于理解。

3.8. 日志审计功能

中数国科安全隔离与信息单向导入系统提供强大的日志和审计功能。单向光闸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。日志内容完整记录并保存系统设定、通信控制、内容检查、连接限制、系统告警等各类日志告警信息。审计模块可使管理员以多种方式进行查询、审计。

系统具有各种日志信息的导入、导出、备份等功能，保证了日志信息的安全性与易用性。

3.9. 高可用性功能

中数国科安全隔离与信息单向导入系统提供双机热备功能。两台单向光闸设备可组成热备机组，机组内单向光闸设备有主设备与备用设备之分，设备间相互检测状态并同步访问策略，当主设备发生故障，从备用设备启动并自动变为主光闸设备，同时以声音与告警信息示警。如下图所示：

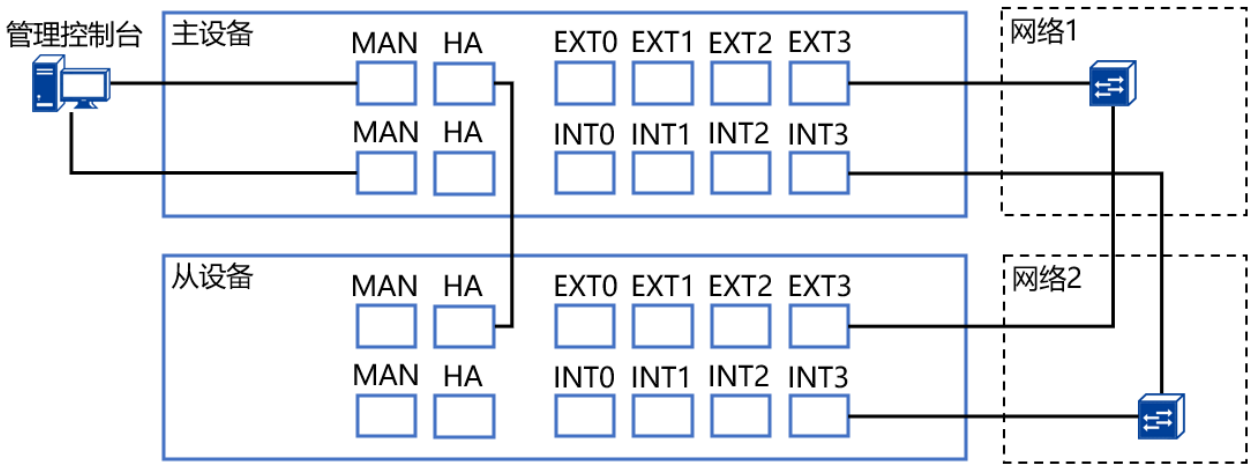

图 2 单向光闸双机热备

四、产品亮点

4.1. 可靠隔离

中数国科安全隔离与信息单向导入系统具有物理隔离、协议隔离、应用隔离、内容隔离、风险隔离的亮点功能。

物理单向：中数国科安全隔离与信息单向导入系统由内网处理单元、外网处理单元和

光单向传输单元三个物理部分组成。光单向传输单元采用发光器、单向光纤、接收器实现物理单向。

协议隔离：中数国科安全隔离与信息单向导入系统的内网处理单元、外网处理单元均采用了我司具有自主知识产权的安全操作系统，各自独立完成网络协议的终止。使内外网业务系统无法直接建立通用协议会话，从而阻断以共有协议为载体的风险传递。

应用隔离：中数国科安全隔离与信息单向导入系统采用应用解码技术，客户传输的应用数据经过模块编码验证，只有符合白名单编码规则的数据才可被传输至内网处理单元。

内容隔离：外网处理单元在将数据传输至内网处理单元之前，会将待传输的数据进行内容检查与病毒查杀，不符合安全规定的数据会被直接删除，只有合法的数据才被允许交换至内网处理单元，从而保证了数据内容的安全性。

风险隔离：中数国科安全隔离与信息单向导入系统支持白名单机制+防病毒双重防护机制。白名单仅允许用户许可的应用数据通过，防范了未知的安全风险；系统集成的防病毒模块可扩展多种常规安全防护引擎。双重防护机制在最大程度上实现了风险隔离，保证了数据传输的安全性。

4.2. 多类型访问控制

中数国科安全隔离与信息单向导入系统不仅具有强大的访问控制力，同时更支持多种应用类型的传输访问控制，如自定义应用、适配协议、邮件传输、组播代理等。

自定义应用：支持基于 TCP/UDP 应用单向传输控制，类型支持 TCP、UDP、DBSYNC。

视频传输：支持 RTMP 视频协议数据传输控制，也可配合数据交换平台产品使用 SIP 视频协议，提高设备传输性能。

邮件传输：支持控制应用层指令，如指定邮件传输的用户名、邮件地址；可以对邮件正文、附件格式等进行指定过滤。过滤条件更细粒化。

组播代理：支持 ASM、SSM、SFM 多种组播方式及多任务组播代理。

4.3. 数据内容审查规则多

数据内容审查支持多种审查规则，如白名单规则、关键字检查、文件类型检查、病毒检查等。

白名单规则：数据流代理应用规范可由管理员设定，只有负责设定的数据规范才可以被传输。数据规范包括以下三种类型。

- ASCII 类型数据格式表示；
- 十六进制数据类型格式表示；
- 正则表达式数据格式表示；

关键字检查：单向光闸的外网处理单元可依据管理员设定的涉密或不健康的信息进行过滤，将过滤到关键字的信息摈弃并记录日志告警。

文件类型检查：单向光闸的内外网处理单元可将指定的可能产生危险的文件类型过滤删除并且记录日志告警。

病毒检查：单向光闸的外网处理单元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，系统会将病毒文件删除，并记录日志告警。

4.4. 系统多重防护安全性高

中数国科安全隔离与信息单向导入系统采用具有自主知识产权的安全操作系统。操作

系统存储于 ROM 中，无法被恶意修改，具有极高的安全性。系统内置高性能安全引擎，可防止 Dos 和 DDos、缓冲区溢出、恶意编码、应用层洪水等攻击。并且系统的内网处理单元、外网处理单元能够在特定的时间自动清理缓存中的文件碎片、修复文件系统错误，保证单向光闸对文件的访问效率。

中数国科安全隔离与信息单向导入系统采用光单向传输单元进行信息传输，业务数据通过应用隔离等措施使外网网络数据及有害数据信息无法进入内网。单向光闸采用双重全防护机制，白名单的防护机制保护客户业务系统免于遭受各种已知安全风险及未知安全隐患，内嵌的防病毒引擎为用户提供第二层保护，识别已发现的各种病毒和入侵时示警并记录日志。

4.5. 独有 RSMP 实现高吞吐

中数国科安全隔离与信息单向导入系统的内、外网处理单元采用中数国科独有的复杂对称多处理（RSMP）技术，在一台单向光闸设备内集成多各处理模块，成倍提升处理能力，使单向光闸具有高性能。

4.6. 专用硬件设计高可靠

中数国科安全隔离与信息单向导入系统在硬件结构上采用专用安全主板设计，进一步提高了隔离系统的可靠性，使单向光闸设备可在超重负荷的环境下长期稳定运行。在实施中，配合双机热备的部署方式可使系统抵抗灾难性成倍提高。

五、应用场景

5.1. 不动产行业场景

《自然资源部办公厅关于完善信息平台网络运维环境推进不动产登记信息共享集成有关工作的通知》（以下简称通知）明确要求：“互联网与政务外网之间通过双向网闸、政务外网与业务内网之间通过单向网闸和离线摆渡方式实现数据互通”，有效避免信息共享、系统对接、上线运行等关键环节出现数据流失、外泄等事件发生。不动产中心需与政务外网或直接与互联网进行互联。简化方便办理流程，方便了企业及群众，但是也带来诸如病毒入侵、黑客攻击的风险。

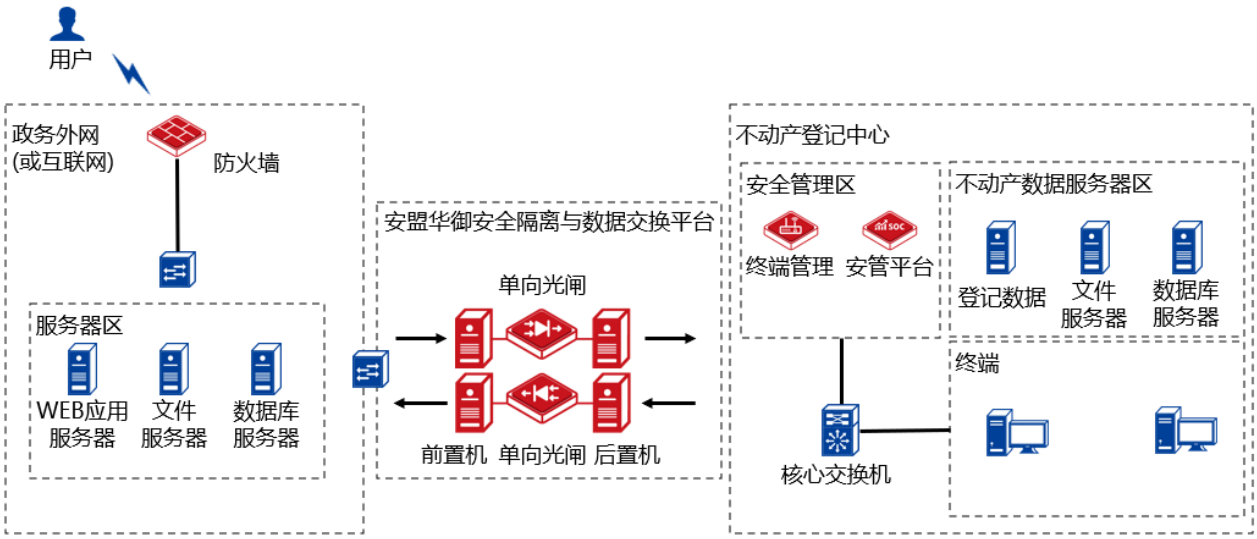

图 3 不动产行业案例

在不动产登记中心边界处部署两套中数国科安全隔离与信息单向导入系统，实现数据单向导入和导出。两条独立单向通道，互不干涉，数据无法从原路返回，保证数据单向无反馈传输。屏蔽来自互联网的攻击及入侵的威胁，实现不动产登记中心网络安全。

5.2. 法院行业场景

■ 文件交换场景

现有法院系统是由安全要求极高的法院业务专网的移动服务内网平台和外网受理平台组成，两个平台之间需要实时传输业务请求与回复。移动服务平台的法院业务专网内部审批系统与部署于移动互联网端的外部受理系统进行实时数据交互、协同办公，就必须互联，此举易造成感染病毒、木马攻击、敏感信息外泄等安全事件。

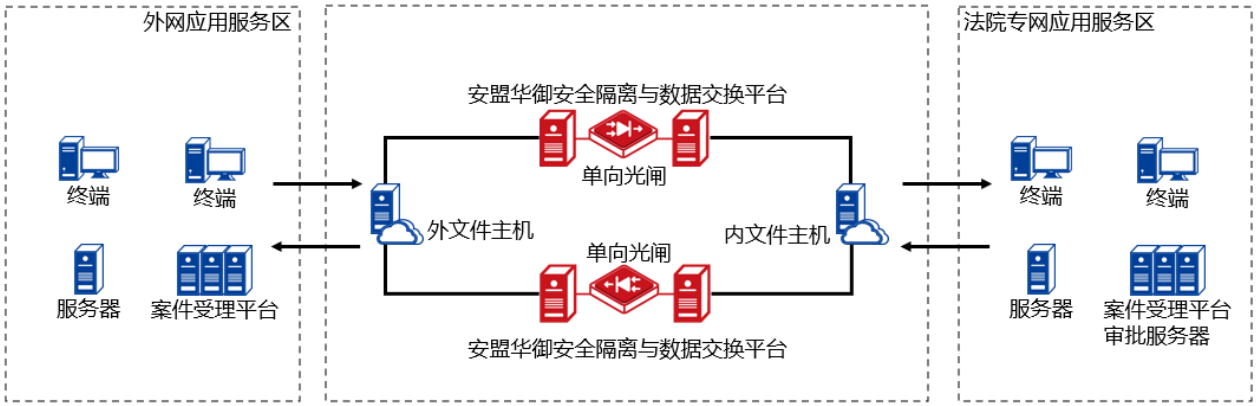

图 4 案例拓扑

■ 数据库同步场景

单向光闸系统包括两台单向光闸设备，出向光闸负责主动从内网前置数据库服务器上抓取数据记录，以单向光信号的方式同步到外网后置数据库服务器指定数据表。入向光闸负责主动从外网后置数据库服务器上抓取数据记录，以单向光信号的方式同步到内网前置数据库服务器指定数据表。

5.3. 电子政务行业场景

在 2000 年 1 月颁布的《计算机信息系统国际互联网保密管理规定》和 2002 年第 17 号文件《国家信息化领导小组关于我国电子政务建设指导意见》中，明确指出为保护重要数

据和应用系统的安全，要保证政府部门内部的计算机信息系统与互联网或其他公共信息网络之间的隔离。如图所示，我们在电子政务外网和政务内网非涉密区部署单向光闸，起到了网络隔离的效果，在业务方面实现数据从政务外网向政务内网非涉密区单向参数，而且单向光闸严格采用基于单向光导技术的隔离交换技术来实现，满足政策合规方面的要求。同时，单向光闸内置文件和数据库同步模块，无须向两侧的服务器安装任何插件，实现从源端主动抓取数据，向目的端主动推送数据，从而保证业务系统的安全性。

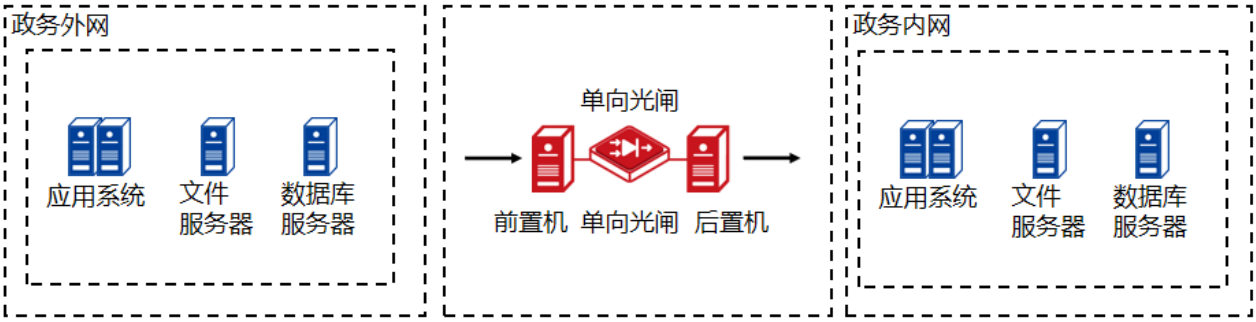

图 5 案例拓扑