中数国科安全隔离与信息交换系统产品白皮书

（中数国科集团）

目录

一、概述

随着党和政府积极推进“互联网+政务”工程建设，多数政府单位积极开展信息化建设，但是由于业务的复杂性和计算机技术的不断发展，众多信息系统的开发缺乏整体规划和系统性，不同时期建设的业务系统可能基于不同的操作系统平台和数据库技术。因而在各个系统之间很难有效地实现信息共享和交互，于是就形成了“信息孤岛”的现象。如何利用现有的技术手段解决各个业务系统之间的数据交换，实现各部门数据共享，提高政府办公效率就成了一个急需解决的问题。

2019 年，国家颁布了《信息安全技术 网络安全等级保护基本要求（GB/T22239-2019）》，里面明确提到：“应在网络边界通过通信协议转换或者通信协议隔离等方式进行数据交换，应对进出网络的数据流实现基于应用协议和应用内容的访问控制。”

1.1 产品背景

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，从 1995 年开始，互联网在我国迅速普及，党和政府积极推进全国的数字化进程，使我国的数字化建设取得了突飞猛进的发展，经过多年建设，我国已建成具有相当规模的数字化网络，但随着网络的不断普及，安全问题日益

增多，网络和信息安全问题成为威胁国家和政府安全的重大隐患。随着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一个相当的高度上来，我国互联网建设的重点也从开始的组网、应用开发转移到现在的保障应用安全以及全面的信息监督、控制、管理体系的实现上来，从而构筑我国坚固的信息安全防护体系。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、部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。

安全隔离技术首先出现于国外，最早出现的是物理隔离的概念，以色列首先研发了物理隔离卡，使得一台主机可在两个安全等级不同的区域间来回切换，随后，以色列和美国又出现了基于这种原理的网络隔离产品，在两个网络并不同时连通的情况下进行数据交换与信息共享。目前，各个国家的政府、军队均有采用不同形式的隔离产品保障信息安全。

同样，我国隔离技术也经历类似的发展历程，隔离技术日趋完善与成熟，当前隔离技术主要有如下两种实现方式：

1、“摆渡型”，采用多主机系统，连接内外网的主机内装有物理或电子方式的切换开关，确保内外网络间在同一时刻没有通畅的链路，依靠软件控制在两个网络间实现文件转存。该种隔离技术在实时通信、稳定性、安全性方面都面临巨大的、甚至是难以逾越的技术障碍。

2、“通讯重构型”，采用多主机系统，连接内外网的主机使用专有通信协议进行通讯，从而实现内外部网络的隔离和数据交换，内外网主机实时捕获、分析网络中的数据包，并进行重新封装，此基础上实现安全审查与访问控制。该种隔离技术较好地解决了实时通信的问题，但当今黑客技术发展迅速，入侵行为往往分散成多个伪装成正常业务动作的数据包穿越各种防护设备，抵达目标后进行重组并造成危害，令“通讯重构型”隔离产品无法防范。

电子政务建设的不断深入，更加复杂的业务系统不断被开发，工作效率的提高也带来了更多的安全风险，为了满足电子政务建设不断提升的安全需求，我公司依仗强大的技术力量和独特的安全理念，自主研发出具有更高安全性、更高性能的网闸。

1.2 产品定义

中数国科网闸主要用于各地电子政务建设，下列场合都可使用隔离系统保障业务系统安全：

- 政务外网与政务内网间存在业务往来的接口；
- 行业内纵向上下级信息系统的接口；
- 行业间需要进行业务信息共享、数据交换的接口；

中数国科网闸可在保障信息安全的前提下，在两个不同安全级别的网络区域间进行适量的、可靠的数据交换。

国家保密局对网闸类产品的应用也做了规定，规定网闸可在以下四种网络环境下应用：

1、不同的涉密网络之间；

2、同一涉密网络的不同安全域之间；

3、与 Internet 物理隔离的网络与秘密级涉密网络之间；

4、未与涉密网络连接的网络与 Internet 之间”。

二、产品简介

中数国科安全隔离与信息交换系统由内、外网处理单元和安全数据交换单元组成；主要功能是在保证两个网络隔离的情况下，做特定的数据交换，系统内外网主机间按照指定的周期进行安全数据的摆渡，其数据流转过程类似 U 盘拷贝，也像船只通过船闸的过程，所以安全隔离与信息交换系统被业内形象的简称为“网闸”。

三、系统架构及工作原理

中数国科网闸设备分别由内、外网处理单元与数据交换单元（专用隔离芯片）三部分组成。内、外网处理单元是一台专有的网络安全计算机设备，分别连接于内外网络。内、外网处理单元之间通过专用的隔离芯片进行数据的摆渡传输，其过程类似 U 盘拷贝。当专用隔离芯片与内网联通时与外网电路是断开的，当隔离部件与外网联通时，与内网是断开

的。并在确保网络隔离的前提下实现适度的数据交换；

3.1 系统架构

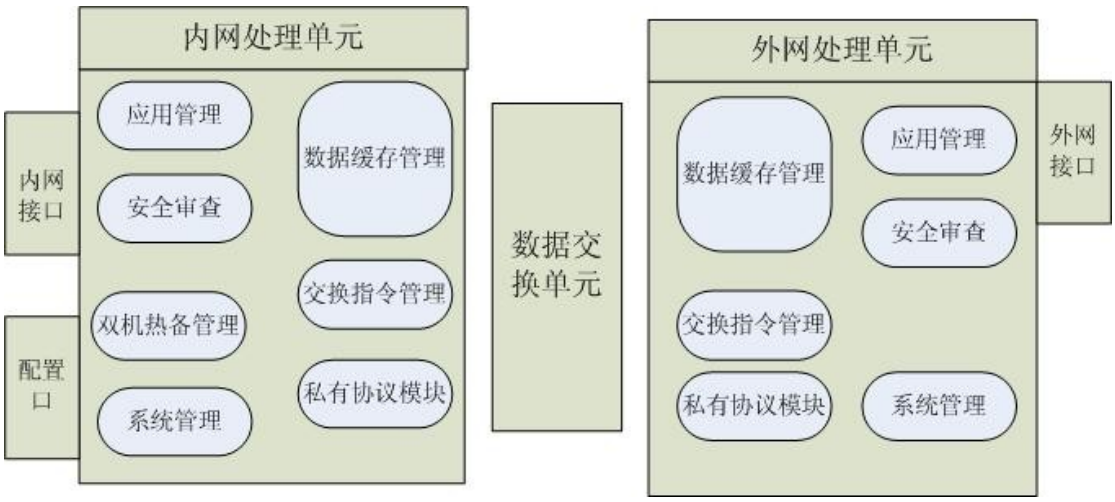
我们知道计算机网络依据物理连接和逻辑连接来实现不同网络之间、不同主机之间、主机与终端之间的信息交换与信息共享。网闸隔离、阻断了网络的所有连接，实际上就是隔离、阻断了网络的连通。网络被隔离、阻断后，两个独立主机系统之间如何进行信息交换？网络只是信息交换的一种方式，而不是信息交换方式的全部。在互联网时代以前，信息照样进行交换，如数据文件复制（拷贝）、数据摆渡，数据镜像，数据反射等等，网闸就是使用数据“摆渡”的方式实现两个网络之间的信息交换。

网络的外部主机系统通过网闸与网络的内部主机系统“连接”起来，网闸将外部主机的TCP/IP 协议全部剥离，将原始数据通过存储介质，以“摆渡”的方式导入到内部主机系统，实现信息的交换。说到“摆渡”，我们会想到在 1957 年前，长江把我国分为南北两部分，京汉铁路的列车只有通过渡轮“摆渡”到粤汉铁路。京汉铁路的铁轨与粤汉铁路的铁轨始终是隔离、阻断的。渡轮和列车不可能同时连接京汉铁路的铁轨，又连接到粤汉铁路的铁轨。当渡轮和列车连接在京汉铁路时，它必然与粤汉铁路断开，反之亦然。与此类似，网闸的专用隔离芯片部分在任意时刻只能与一个处理单元建立非 TCP/IP 协议的数据连接，当它与外部处理单元的主机系统相连接时，它与内部处理单元必须是断开的，反之亦然。

即保证内、外网络不能同时连接在网闸上。网闸的原始数据“摆渡”机制是原始数据通过存储介质的存储（写入）和转发（读出）。

网闸在网络的第七层将数据还原为原始数据文件，然后以“摆渡文件”的形式来传递原始数据。任何形式的数据包、信息传输命令和 TCP/IP 协议都不可能穿透网闸。这同透明桥、混杂模式、IP over USB、代理主机、以及通过开关方式来转发信息包有本质的区别下面以内网与外网之间的安全隔离与信息交换系统为例，说明通过网闸的信息交换过程。

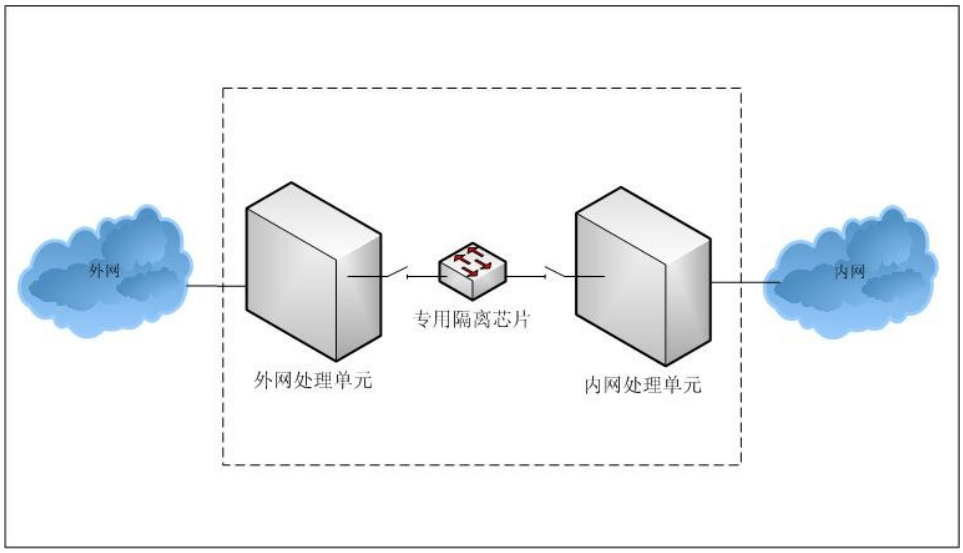
当内网与外网之间无信息交换时，数据交换单元与内网交换单元，数据交换单元与外网处理单元，内网处理单元与外网处理单元之间是完全断开的，即三者之间不存在任何连接，如下图所示。



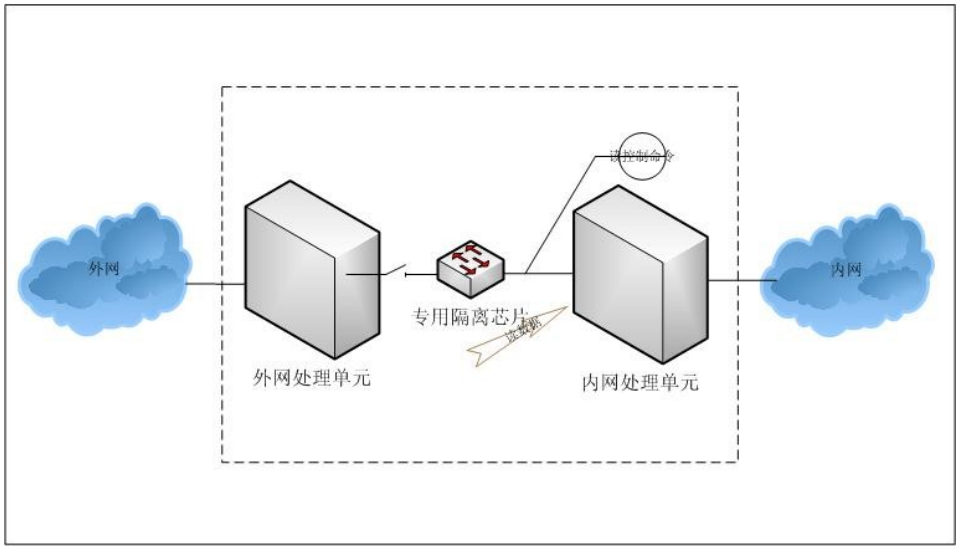
当内网数据需要传输到外网时，内网处理单元会主动向数据交换单元发起非 TCP/IP 协议的数据连接请求，并发出“写”命令，将“读”开关合上，并把所有的协议剥离，将原始数据写入高速缓存。在写入之前，根据不同的应用，还要对数据进行必要的完整性、安

全性检查，如病毒和恶意代码检查等。

在此过程中，外网处理单元与数据交换单元始终处于断开状态，见下图所示。



一旦数据完全写入网闸的存储介质，“读取”开关立即打开，并中断与内网的“写”开关，中断与内网的连接。转而发起对外网处理单元的非 TCP/IP 协议的数据连接请求，当外网处理单元收到请求后，发出“读”命令，将数据交换单元的数据读取到外网处理单元。外网处理单元重新发起 TCP/IP 的会话到达目标服务器，将数据上传交给应用系统，完成了内网到外网的信息交换。详见图 3 所示。



中数国科网闸由内网处理单元、外网处理单元与安全数据交换单元（专用安全通道）组成。内、外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。安全数据交换单元采用专用安全传输控制硬件，通过层层搬运的方式实现信息安全交换，在数据交换的过程中通道在任何时刻都不是直接连通的。安全数据交换单元是隔离系统的内、外网单元之间的唯一数据传输安全通道，只有私有可信数据才被识别，从而杜绝了任何不被识别数据穿透安全传输通道，确保所有通过的数据包只被控制单元识别的合法纯数据。

3.2 工作原理

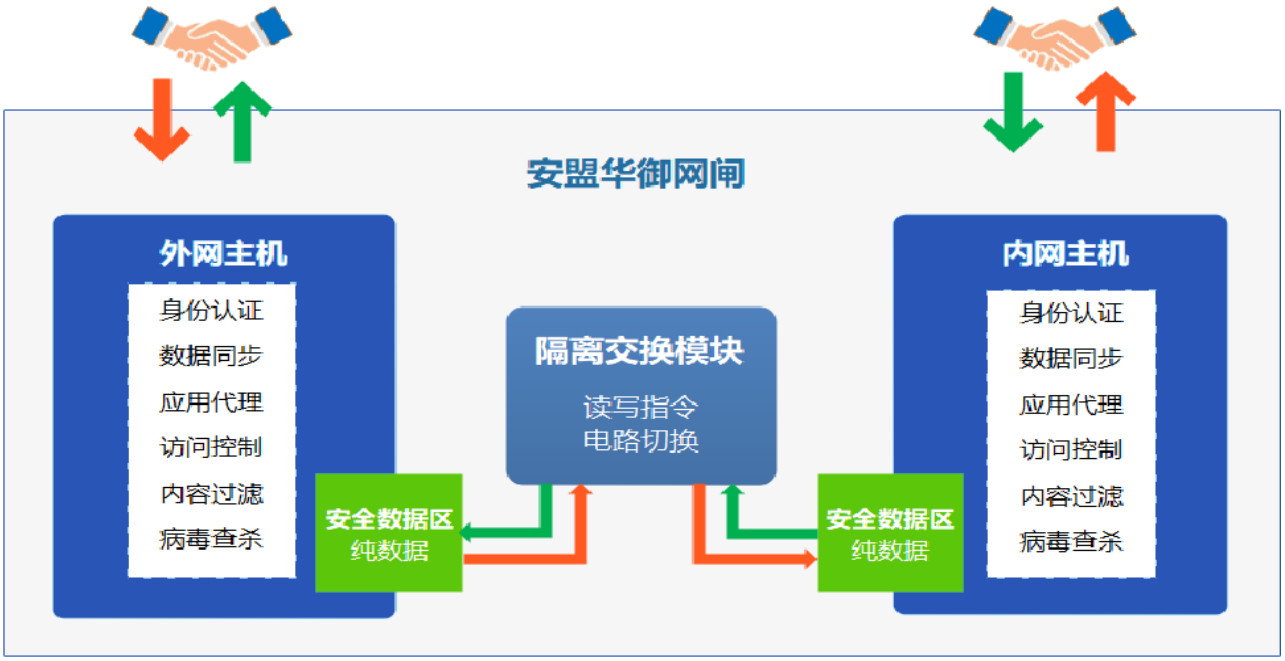
网闸的工作原理是在内、外网处理单元独立完成网络协议终止、内容检查与日志审计，将符合安全策略的数据内容提交至安全数据交换区等待数据交换。安全数据交换单元按

照设定的周期分别由内、外网处理单元的安全数据交换区将数据内容提取并交换至另一端的安全数据下载区，等待用户的读取或传输至指定的计算机上，从而在保证内外网隔离的情况下，实现可靠、高效的安全数据交换，而所有这些复杂的操作均由隔离系统自动完成，用户只需依据自身业务特点定制合适的安全策略既可实现内外网络进行安全数据通信，在保障用户信息系统安全性的同时，最大限度保证客户应用的方便性；同时系统集成防病毒技术及扩展入侵检测技术，形成一套具有多重防护的安全解决方案。

四、关键技术

中数国科网闸对于接收到的任何外部会话连接，首先通过外网主机网络接口将会话终止，然后利用协议解析模块将 TCP/UDP 数据格式打破，并采用专有的封装协议将分解得到的数据打包后通过隔离开关传输到内网主机。在内网主机数据经过一系列安全检查之后，协议解析模块对数据重组，并在内网主机网络接口将重构的会话传送到内部服务器。

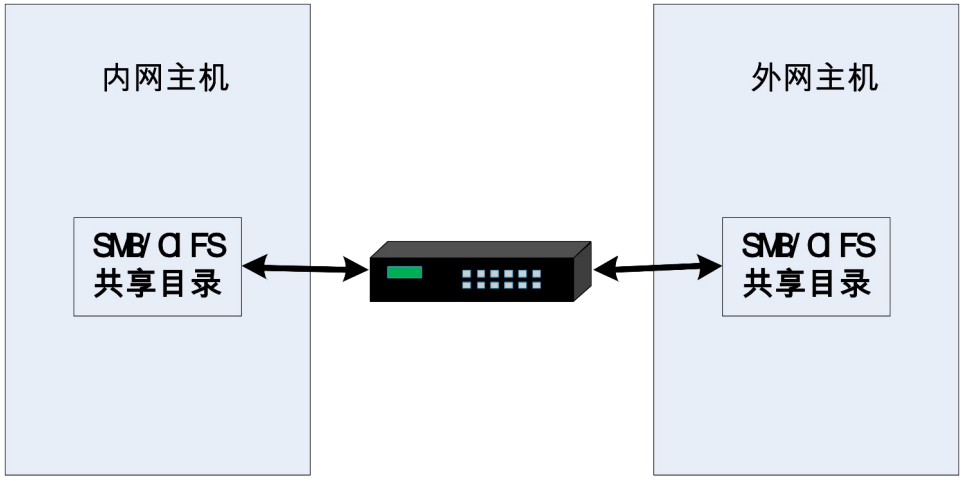
对于从内部到外部的 TCP 连接，中数国科网闸也具有对等的处理方式。事实上中数国科网闸已经将原来直接连通内外网络的 TCP 连接，从逻辑上分解为外网到网闸外网主机的 TCP 连接、外网主机到内网主机的专有封装协议连接、内网到内网主机的 TCP 连接的组合。因此，在添加中数国科网闸之后，可以阻断内外网络之间的 TCP 对话，其结构如图所示：



值得提出的是，中数国科网闸不但在逻辑上终止了 TCP 对话，还从物理上断开了内外网络之间的连接，使得内外网络之间在任何时候都不存在直接的物理层和链路层连接通路。

中数国科网闸技术的关键技术要点如下

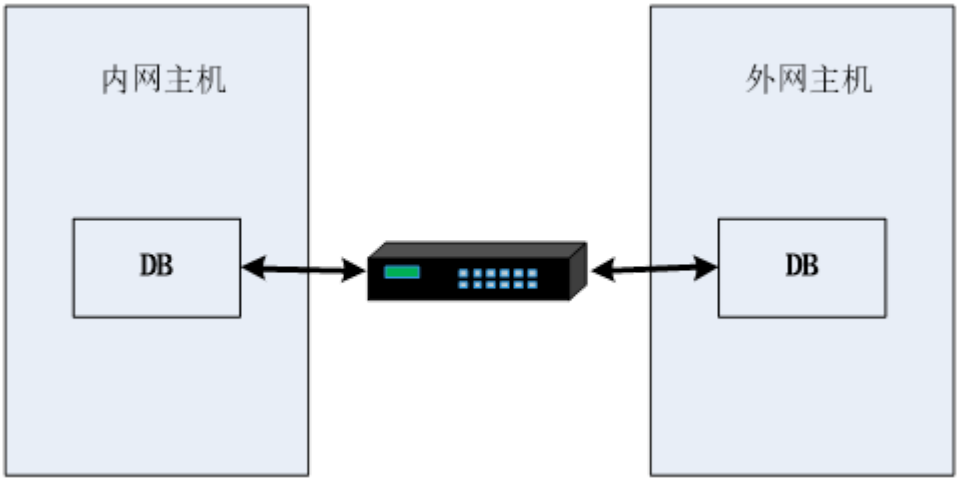
文件交换



网闸主动抓取两侧共享目录中的文件，按设定的规则方向，做定时同步。支持单向

（内到外或外到内）、双向、一对一、一对多、多对一的同步，支持文件后缀名过滤、防病毒功能，支持同步文件备份（即在同侧设定的备份目录下备份将要同步的文件）。

数据库同步



网闸主动抓取两侧数据库信息，按设定的规则方向，做定时同步。支持单向（内到外或外到内）、双向同步，支持同构、异构数据库同步，支持同步插入、同步删除、同步更新。

五、产品功能

网闸在保证内外网隔离的情况下，实现可靠、高效的安全数据交换，而所有这些复杂的操作均由系统自动完成，用户只需依据自身业务特点定制合适的安全策略既可实现内外网络进行安全数据通信，在保障用户信息系统安全性的同时，最大限度保证客户应用的方便性。

网闸主要用于连接两个不同的安全域，实现两个安全域之间应用代理服务、协议转换、信息流访问控制、内容过滤和文件交换、数据库交换等功能。

5.1 业务功能

5.1.1 安全隔离

- **安全隔离**：系统由内网处理单元、外网处理单元及安全数据交换单元三个物理部分组成，安全数据交换单元不同时与内外网处理单元连接。
- **协议隔离**：内、外网单元主机均采用自主研发的安全操作系统，分别独立完成网络协议的终止。内、外网单元之间只能采用专有安全通道进行数据传递，内外网无法直接建立任何的协议会话，从而屏蔽以共同协议为载体的风险传递。
- **应用隔离**：系统采用模块化的应用解码，内、外网单元分别独立完成与客户会话交互、提取安全数据等待数据交换，所以内外网之间不能建立直接的应用会话。
- **内容隔离**：内、外网单元分别将待交换传输的数据进行内容检查与病毒查杀，丢弃不符合安全策略的数据，只有合法的数据才允许交换至另一端，从而保证了数据内容的安全性。
- **风险隔离**：系统以白名单机制运行，仅许可正常的、用户许可的网络应用，防范未知的安全风险。并且系统集成防病毒并可扩展多种常规安全防护引擎，如入侵检测等，可检

测 60000 多种病毒和 4000 多种网络入侵，双重安全机制最大程度上实现了风险隔离。

5.1.2 信息交换

网闸的内、外网处理单元分别负责接收来自所连接网络的访问请求，两模块间没有直接的物理连接，形成一个物理隔断，从而保证可信网和非可信网之间没有数据包的交换，没有网络连接的建立，在此前提下，通过专有硬件实现网络间信息的实时交换。这种交换并不是数据包的转发，而是应用层数据的静态读写操作，因此可信网的用户可以通过网闸放心的访问非可信网的资源，而不必担心可信网的安全受到影响。

- **Web 信息交换模块：**通过系统内部的 Web 处理模块，网闸能够实现内外网间的 Web 数据交互。通过对内外网间 Web 应用进行信息获取、流保持、内容解析、源数据丢弃、审查、数据重建、传递、流发起等系列业务动作，实现内外网间可进行标准的、可控的 HTTP 通信。如针对绝大多数 Web 应用只允许 GET、PUT、POST 三个命令即可，其它动作例如 Delete、Option 等较危险的动作一律阻止；可以禁止 JavaScript 及 ActiveX 等脚本程序以屏蔽其带来的威胁。
- **文件交换模块：**文件同步功能支持 FTP、 SMB、NFS、FTPS、SFTP 等主流文件传输协议，满足绝大多数业务场景需要，同时支持我司自研的私有文件传输协议，传输数据时采用国密算法对数据进行加密，防止恶意数据窃取等行为；文件交换功能通过主动获

取、主动推送的方式将文件安全的交换到另一侧网络，传输文件时无需在网络边界打开端口，防止网络攻击的发生；支持真实文件格式过滤，防止通过修改后缀名的方式绕过安全检查，同时可以结合杀毒模块对文件内容进行安全检查，防止恶意程序进入另一侧网络。

- **邮件交换模块：**通过内外网处理单元的 POP3、SMTP 处理模块，可以允许可信网络用户自如地通过网闸收发来自不可信网络上的电子邮件，也可以允许不可信网络上的用户安全地通过网闸来收发可信网络上的电子邮件。网闸能够在内外网间实现透明的、可审查的、可控的 POP3 和 SMTP 应用，可以指定用户名、密码甚至邮件地址，可以禁止邮件附件功能。
- **数据库交换模块：**数据库信息交换模块包括两部分，一为数据库信息访问交换，一为数据库信息同步，支持主流及国产等多种关系型数据库，通过内置的数据库处理模块，系统内能够控制针对各种数据库的操作，比如 Oracle 数据库，可以设置只允许读取数据（Select），不允许删除数据（Delete）、更新数据（Update）以及删除数据库表（DROP）、新建数据库表（CREATE）等操作；数据库同步功能支持字段级数据同步功能，利用数据库自身的触发器机制，实时将特定的发生变化数据同步到对端，支持 TEXT、BLOB、CLOB 等大字段数据同步，支持内容过滤功能。
- **多媒体模块：**支持 RTSP、RTMP、MMS、HLS、H323、SIP 协议（符合国标 GB/T

28181 与 RFC3261 标准要求）、PSIP（警用数字集群 PDT）等多种音视频交换协议，在指定的通道中绑定流媒体模块后，可以保证通道中传输的数据符合媒体格式；支持视频点播、回放功能；支持同厂家或不同厂家平台之间的级联、互联。

- **工控信息交换模块：**专用安全通道只传输工控生产数据信息，保证了生产内网的绝对安全。生产企业的生产内网需要将生产数据及时传输到办公网络中，同时确保生产内网的绝对安全。支持工控领域常见的 OPC、MODBUS、S7 等多种主流工控协议，并可控制相应的功能码。比如只允许通过 MODBUS 协议读取状态信息，不能发送控制指令等。可应用于冶金系统、电力系统、煤炭、石油、石化、化工、环保等单位的。
- **组播模块：**对于组播应用做不同网络之间的代理，支持组播数据代理，可跨网络进行组播数据转发，支持 PIM 协议的代理，使客户组播应用无缝跨网代理。
- **定制信息交换模块：**对于用户自行研发的标准 TCP/IP 通信协议，可借助我公司提供的定制信息交换模块完成用户协议的安全定制，以用户定制的命令、参数等来解析通信内容，只允许用户特定的协议通过，远比其它产品只进行端口过滤和内容过滤安全的多。

5.1.3 网络访问控制

网闸具有强大的访问控制力，管理员可通过定制访问策略，精细地控制数据的传输方向、内容。管理控制台以人性化的人机接口协助管理员轻松实现管理目标。

- **网络访问控制：**隔离用的内、外网，实现 2~7 层的访问控制，通过灵活组合的网络对象，制定与实际需求完全吻合的访问策略。
- **用户访问控制：**隔离用户的内、外网，实现定制的用户访问控制，可以控制某个用户只可访问某一个应用系统。

5.1.4 数据内容审查

内容检查是指当网闸在准备交换数据之前所进行的安全检查，确保只有符合保密规定、安全策略的数据才可被交换至另一端网络中。

- **动作检查：**网闸的内、外网单元可依据管理员设定的安全策略进行控制，拒绝非授权的操作：如 FTP 的允许下载不允许删除、上传，数据库的只允许查询（SELECT）不允许删除（DELETE）等等，并将所有操作记录到系统日志，对违规的操作生产告警信息。
- **关键字检查：**针对关键字（词）进行检索，按照匹配的原理，对通过网闸传输的数据进行过滤和检查，可以保护网络的各种敏感资源和数据，也保护了可信网络资源。网闸的内、外网单元可依据管理员设定的关键字、涉密、不健康的信息进行过滤，禁止传输违规信息并产生告警。
- **文件类型检查**：网闸的内、外网单元可将指定格式的、可能产生危险的文件类型进行过滤，记录日志并产生告警。

5.1.5 缓存空间及传输数据的管理

中数国科网闸的内、外网单元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，保持文件访问效率。

5.1.6 双重安全防护机制

网闸采用双重安全防护机制，即系统的内、外网处理单元以白名单方式接受网络请求、建立并终止会话。所有的客户网络请求无法穿透系统进入内网，并且只有被允许的网络请求才被响应，能够隔离各种未知的安全风险。

客户的业务数据均需经过安全检查才允许被交换。同时，网闸内置防病毒和入侵检测引擎，能够实时检测、阻绝已知的各种木马、病毒与入侵行为，并在产生告警，以便管理员在最短时间内做出响应。

网闸提供开放、可靠的 API 接口，可与第三方安全技术（如以 PKI 为基础的身份认证技术、安全审计技术等）无缝集成。

5.2 管理功能

5.2.1 安全的管理通信

中数国科安全隔离与信息交换系统只允许从设备的管理控制端口进行管理。在通信端

口不接受任何管理请求。避免了管理信息的旁入可能。管理者与隔离网闸设备采用加密的 HTTPS 协议进行交互。现有各种监听工具无法获取其通信内容，保障了管理信息的安全性。

5.2.2 权限分配

网闸采取系统管理员、安全保密员、安全审计员三种角色分立的权限分配模式。各类用户只能维护本角色的功能作，三员权限分立并相互制约。同时提供用户管理功能，可分配相应的权限给特定用户，使用户管理更加方便且易于理解。

5.2.3 策略配置

网闸采用图形化策略定制方式，即便是初次使用的用户也可依据界面向导，依次制定适应实际网络的交换策略。此外，系统内置的初始策略更是方便了新用户的使用。

5.2.4 日志审计

网闸提供强大的日志和审计功能，日志默认存储在设备中，支持通过 SYSLOG 将日志发送到日志服务器，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、系统告警等各类信息。

审计模块可使管理员以多种方式进行查询、审计，并生成报表。系统具有日志告警信息

的导入、导出、备份等功能，保证了日志告警信息的安全性与易用性。

5.3 高可用性功能

网闸产品针对大型网络的应用提供了负载均衡、双机热备功能，实现系统的稳定可靠运行。通过内置的双机热备系统，连接在同一个网络内的多台网闸设备可以建立双机热备机制，并通过虚拟 IP 统一对外提供服务。从设备不断发出心跳信息侦测主设备状态，一旦主设备出现故障从设备将立即接管并继续提供服务。结合网闸独有的状态检测系统，管理员能够迅速发现设备故障并做出处理。

5.3.1 负载均衡

网闸支持两种方式的负载均衡功能：

- **基于带宽**：采专有均衡算法，将大量的业务请求平均分配到各个安全隔离，从而获得成倍的性能提升，适用于大流量、高负载的应用场合。
- **基于应用**：采用专用设备对各种网络请求进行预分流，将不同的网络应用交由不同的隔离设备处理，不仅实现性能的增长，同时也实现了应用分离与控制，加强安全性和可靠性。

5.3.2 双机设备

网闸提供双机热备功能，两台设备可组成热备组，组内设备有主设备与从设备之分，主、从网闸设备使用心跳检测设备状态，并获取最新的访问策略，当主网闸设备发生故障，从设备会立即开始工作，避免影响用户业务系统正常使用，同时以声音与告警信息示警。如下图所示：

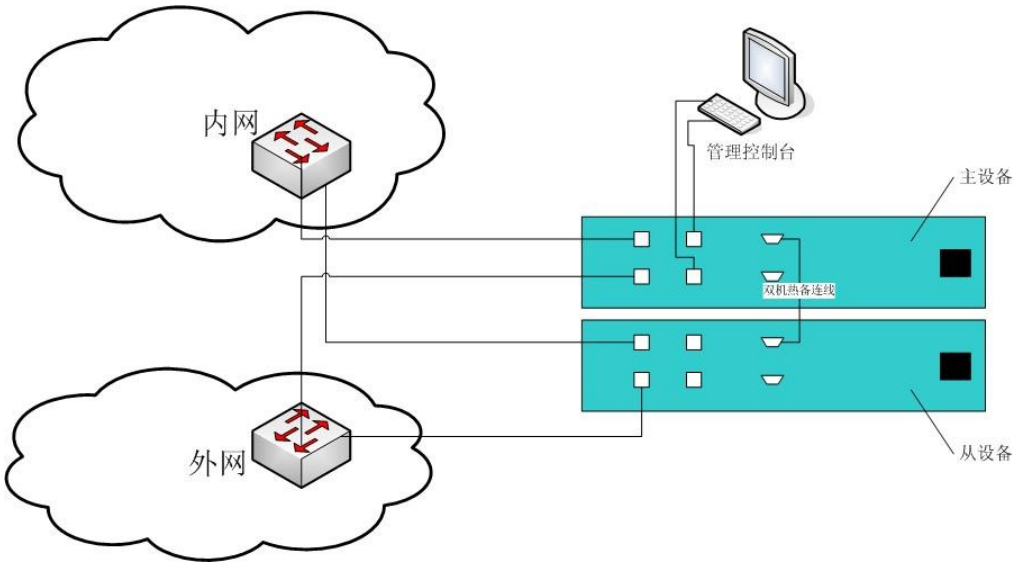


图 3.3 双机热备

5.4 双协议栈支持

网闸支持纯 IPv4，纯 IPv6，IPv6 到 IPv4，IPv4 到 IPv6 等网络环境，支持 NAT6，NAT6to4 功能，可实现混合网络代理功能。

网闸内置的访问控制模块、文件交换模块、数据库同步模块、WEB 代理模块、组播模块全部支持 IPv4、IPv6 双协议。

5.5 VPN

网闸支持 VPN 功能，可实现网络设备、移动终端的安全接入。支持国密 SSL VPN、国密 IPSec VPN，支持 SM1、SM2、SM3、SM4 算法。采用严格的基于国产商用 SM2 算法的身份鉴别机制，支持 CRL\OCSP 等方式查询证书状态，有效防范身份冒用等安全风险。

六、产品优势亮点

6.1 网络适应性强

支持双机热备、链路聚合；支持 IPv4、IPv6 及 IPv4 与 IPv6 混合网络。

6.2 视频兼容广泛

支持 RTSP、SIP、H.323 协议，通过了公安部 GB/T 28181 评测，兼容海康、大华、宇视、科达、新华三、公安一所等主流视频厂商应用。

6.3 数据库支持丰富

支持数据库的代理访问和实时同步功能，既支持 Oracle、SQL Server. MySQL、Sybase 等主流数据库，也支持武汉达梦、人大金仓、优炫等国产数据库。

6.4 系统处理能力强

网闸的内、外网处理单元采用复杂对称多处理（RSMP）技术，在一台网闸设备内集成多各处理模块，提升设备处理能力，使网闸具有很高的性能。

6.5 系统可靠稳定

网闸采用专用安全主板，提高系统的可靠性，使网闸设备可在重负荷的环境下长期稳定

运行。双机热备功能可使系统抵抗损坏时的可靠性成倍提高。

七、应用场景

7.1 医疗行业场景

随着网上医疗的普及，医院的业务内网已不能再封闭，非法连接和入侵攻击时有发生医院需要增加安全防护投入。当前，大部分医院都在参照等保三级进行安全防护建设。

医院网络分为医疗内网和办公外网，医疗内网与外部机构通过专线或 VPN 进行数据交换。由于等级保护的相关标准规定，在办公外网和医疗内网之间部署网闸，保证各安全域的隔离，同时做安全、可控的数据交换；如图所示：

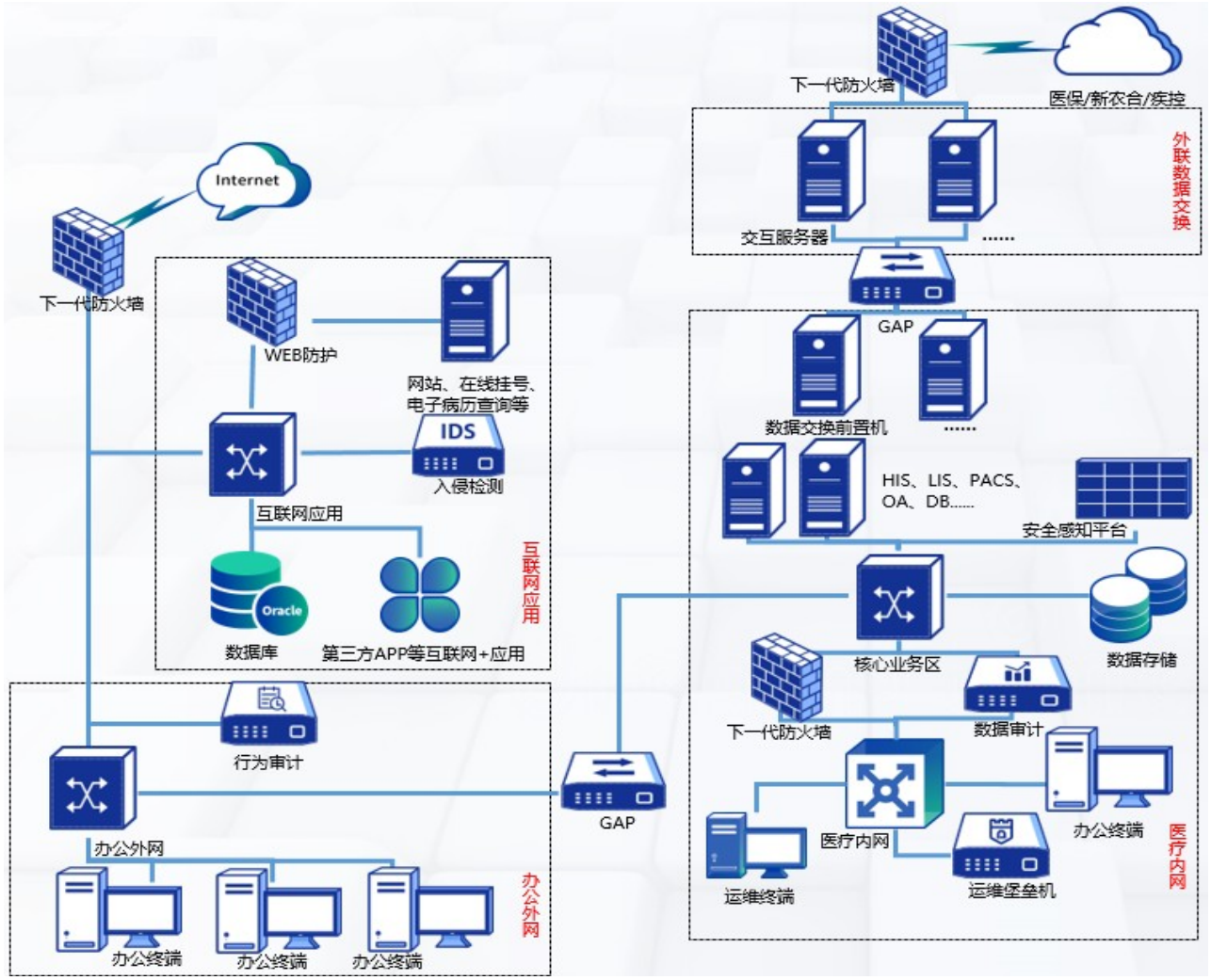


图 5.1 医疗场景拓扑图

网闸能够满足与医院原有网络、系统高效对接，屏蔽前端网络链路方式的多样性，实现各种网络环境的全面接入。

满足《网络安全法》相关要求，同时也满足网络安全等级保护相关要求。

网闸产品结合自身产品的优点针对客户网络环境的特点制定相应的安全策略，以确保内网与外网高安全隔离的同时，实现内网与外网的数据库同步。

7.2 电子政务行业场景

电子政务场景各业务网涉密级别不同，为保证数据安全，一般采用物理隔离方式来保护高级别网络安全，但这导致外网用户无法及时有效的获取信息，无法满足用户对信息交互的需求。

在政务网和外网之间部署安全隔离网闸，只允许与系统相关的数据和信息进入内部网络中。内网与外网在同一时刻不连接，为用户提供安全有效的文件交互、数据库同步、视频交互等信息； 如图所示：

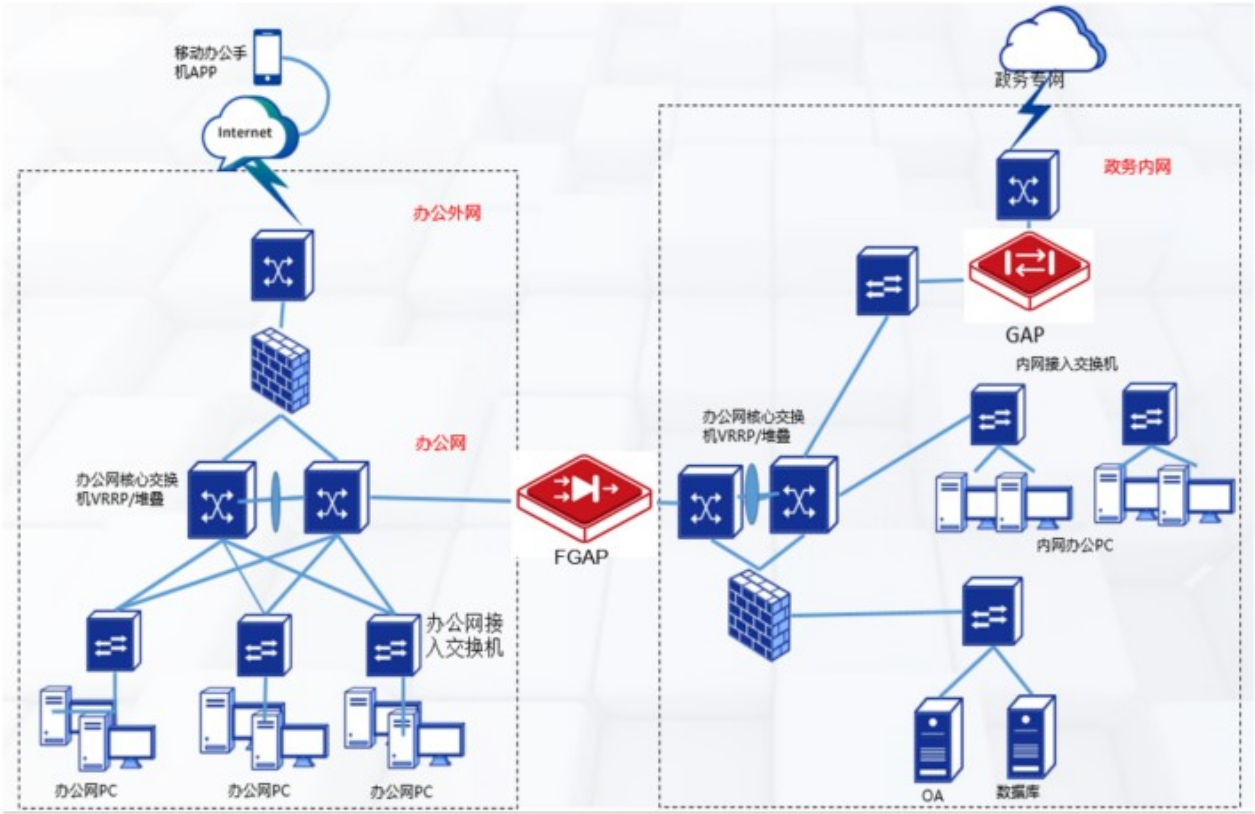


图 5.2 电子政务场景拓扑图

网闸采用高性能服务器架构进行数据处理，最大限度的避免了数据传输过程中的延迟

和卡顿问题。

满足《网络安全法》相关要求，同时也满足网络安全等级保护相关要求。

7.3 公安行业场景

交警集成指挥平台，主要通过信息共享、集成应用和联网运行，实现各类道路交通基础动态信息的逐级汇聚及大范围分析研判，实现跨地域道路交通管理的联网联控。在联网基础上，实现车辆缉查布控、交通违法现场查处和审核入库、交警执法站信息管理、道路交通安全形势研判、勤务管理等方面的应用进行可视化指挥调度。

网闸部署于公安专网与警务通网和视频专网之间，实现网络间高安全隔离和业务数据实时交换，为交警集成指挥平台、视频平台级联、移动警务通等业务应用保驾护航；如图所示：

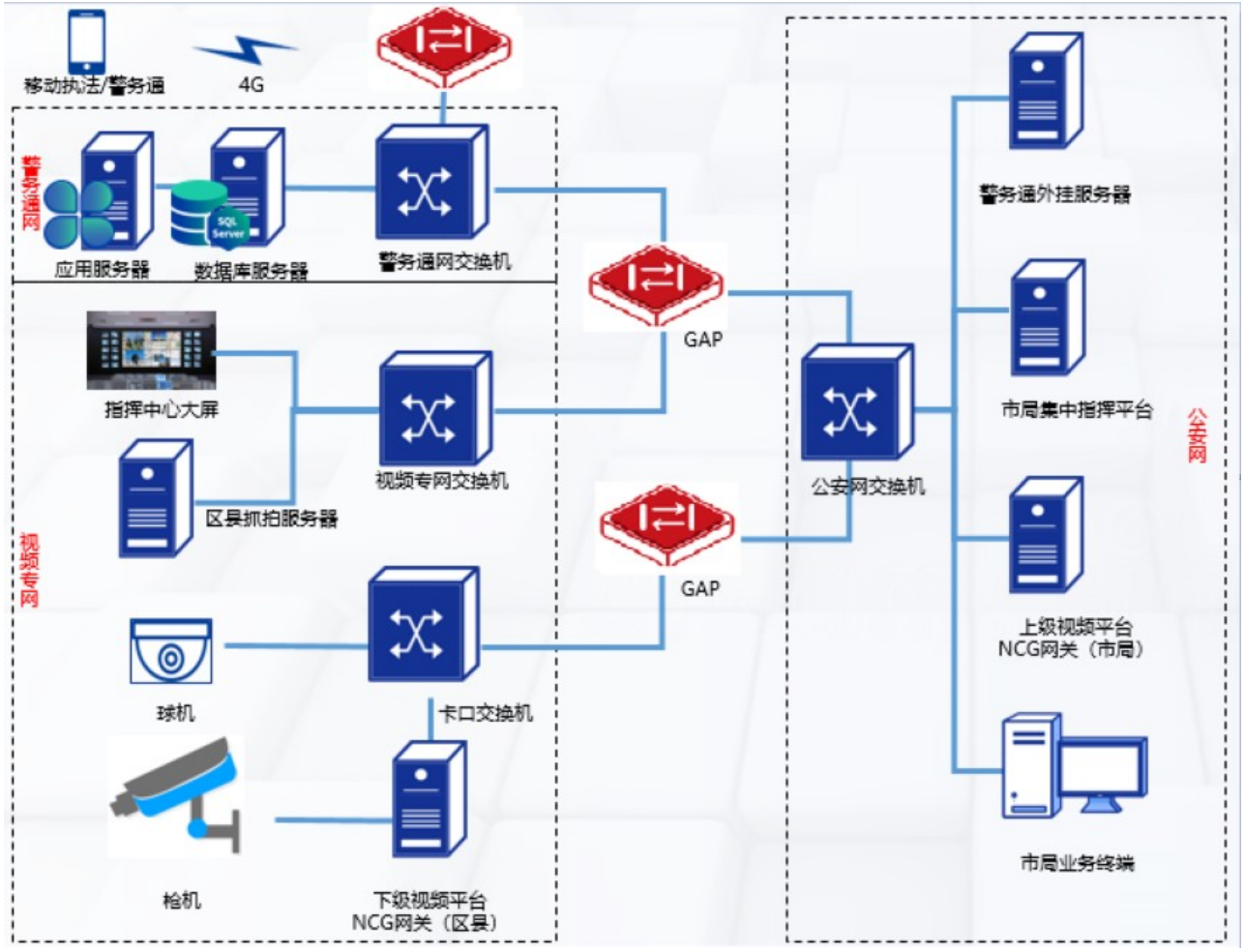


图 5.3 公安场景拓扑图

网闸采用主动交换方式，此方式的特点是对两端的客户网络应用透明，客户数据库服务器不需要做任何转发设置，不需要对数据库进行二次开发，只需要为网闸提供数据库交换的账号即可。

屏蔽勒索病毒及其变种传播到内网业务系统。