聚铭安全隔离与信息交换系统技术白皮书

聚铭网络科技有限公司

2026 年 03 月

目录

声明

在本文中如无特别说明，聚铭网络均指南京聚铭网络科技有限公司。

JUMING 聚铭图标为聚铭网络的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系聚铭网络技术服务部。

联系信息

南京总部：南京市雨花台区软件大道 180 号南京大数据产业基地 7 栋 4 层

电　　话：025-52205520/52205570

传　　真：025-52205565

全国服务热线：400-1158-400

网　　址：www.juminfo.com

产品支持：support@juminfo.com

1. 概述

随着互联网技术的快速发展以及大数据在各行业的广泛应用，信息化建设在带来高效业务协同与数据共享便利的同时，也带来了日益严峻的信息安全挑战。传统网络边界防护体系通常以防火墙为核心，并通过与入侵检测/防御系统（IDPS）、防病毒系统（AV）等安全设备协同部署，以抵御网络攻击并保障系统安全运行。

然而，随着我国数字基础设施的不断完善和数据要素价值的持续提升，单纯依赖防火墙的边界防护模式已难以满足当前数据安全与业务互联的需求，其局限性主要体现在以下方面：

（1）跨安全域数据交换困难

在异构信息系统与不同安全域之间进行数据交换与共享时，传统防火墙难以同时实现高安全隔离与灵活数据共享，导致数据流通效率与安全保障之间难以平衡。

（2）持续通信链路带来的潜在安全风险

防火墙通常需要在高安全域与低安全域之间维持实时通信链路，这种持续连接可能为攻击者提供潜在入侵通道，使未知病毒、恶意代码或新型攻击技术有机会绕过防护系统，对内部网络发起攻击或横向传播。

因此，在数字化与数据共享需求不断提升的背景下，传统边界安全防护体系已难以全面满足安全与互联并重的网络环境需求，亟需引入更高等级的边界防护技术，以保障信息系统的安全、稳定与可靠运行。

安全隔离系统正是在此背景下产生的一种安全边界防护设备。该系统通过构建物理隔离与安全交换机制，在确保不同安全域网络严格隔离的前提下，实现跨网络数据的安全、可控交换。

聚铭安全隔离与信息交换系统是南京聚铭网络科技有限公司基于多年网络安全产品研发与部署经验，面向政府、公安、法院、医疗、交通、教育及企事业单位等行业应用场景设计开发的多业务、高性能安全隔离产品。产品能够满足行业用户对网络边界安全隔离与数据安全交换的需求，实现不同安全域之间数据的安全传输、隔离防护与可控共享。

2. 隔离网闸

2.1. 技术原理

聚铭安全隔离与信息交换系统在内外网络之间承担“安全摆渡”的角色，通过专用通道控制机制实现不同安全域之间的数据安全交换。传统网闸的数据通道控制主要依赖电子开关或基于存储介质的读写控制方式，数据交换通常采用“存储—转发”机制，即数据先写入缓冲区，再由另一端读取并发送至目标网络。因此，系统整体性能在一定程度上受限于开关响应速度和总线带宽。

其中，电子开关在通道切换过程中受器件性能限制，存在一定延时；而基于 IDE 或 SCSI 等存储介质控制方式，则受到总线标准带宽限制，在高性能数据交换场景下难以满足需求。

为突破上述技术瓶颈，聚铭安全隔离与信息交换系统采用先进的物理隔离通道控制技术。该技术通过专用硬件通道实现内外网络之间的数据摆渡，从物理层面彻底阻断内外网的直接通信连接，避免 TCP/IP 等网络协议的直接交互。

系统采用双主机隔离架构，由内端机和外端机两套独立处理系统组成，分别连接内网与外网，并通过 DTP 隔离通道进行数据交换。数据在传输过程中会剥离原有网络协议及附加信息，以原始数据形式通过隔离通道传输，并在目标端根据自定义协议重新封装为网络数据包，从而消除潜在的不安全连接信息。

同时，系统运行在专用安全操作系统及嵌入式控制程序之上，对所有跨网数据进行严格验证与策略控制，仅允许符合安全策略的数据进行交换。通过物理隔离架构、专用通信机制与多层安全控制，系统在保障内外网络彻底隔离的前提下，实现跨安全域数据的安全、可控交换。

2.2. 系统架构

聚铭安全隔离与信息交换系统的硬件结构如图 2.2-1 所示。由此可见，系统由外网控制单元、内网控制单元和 DTP 高速隔离通道三部分组成。DTP 高速隔离通道扮演了“摆渡船”控制的角色，将内外网从物理上分开，达到安全隔离的目的。

图 2.2-1　硬件结构示意图

隔离网闸在内外网之间扮演着一种类似“信息摆渡船”的角色：数据如同货物，内网与外网分处河的两岸，而摆渡船在运输过程中不会同时与两岸接触。基于这一原理，网闸实现了内外网的物理隔离——它不会同时连接内网和外网，从而在根本上阻断任何直接的网络连接。

如图 2.2-2 所示，隔离网闸的系统结构由内网处理单元、外网处理单元和隔离与交换控制单元三部分组成，每个单元均设有独立的数据缓存区，用于暂存待交换的数据。整个数据交换过程需经过两次“摆渡”才能完成：

第一次摆渡：隔离交换控制单元与内网处理单元建立连接，同时断开与外网处理单元。此时，内网中需要交换的数据被写入内网数据缓存区，同时处理器读取来自外网的数据（该数据已在上一次摆渡中存入缓存），完成内网侧的数据写入与外网侧数据的读取。

第二次摆渡：隔离交换控制单元转而与外网处理单元建立连接，断开与内网处理单元。外网中需要交换的数据被写入外网数据缓存区，同时处理器读取来自内网的数据（第一次摆渡中存入缓存），完成外网侧的数据写入与内网侧数据的读取。

通过这种交替连接、分时交换的方式，网闸确保内外网之间始终没有直接的物理或逻辑连接，任何时刻只有一端与隔离交换单元通信，从而彻底消除了基于网络协议的攻击可能。

聚铭安全隔离与信息交换系统采用领先的物理隔离通道控制系统，能够在电路层面切断内外网之间的数据链路层连接，仅允许经过严格检查的应用层数据进行适度交换。这一设计既保证了可信任网络的高度安全性，又实现了与不可信任网络之间高速、可靠的信息传输。

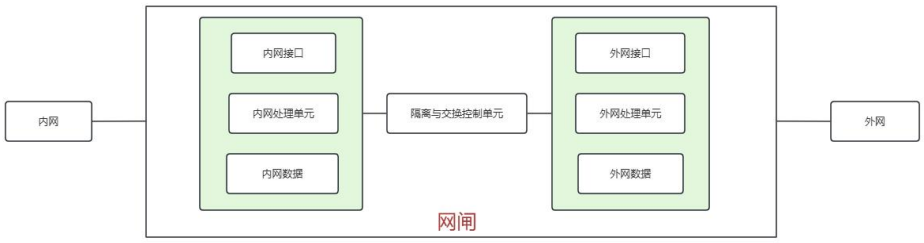


图 2.2-2　硬件结构示意图

聚铭安全隔离与信息交换系统对应用数据的处理流程如图 2.2-3 所示。

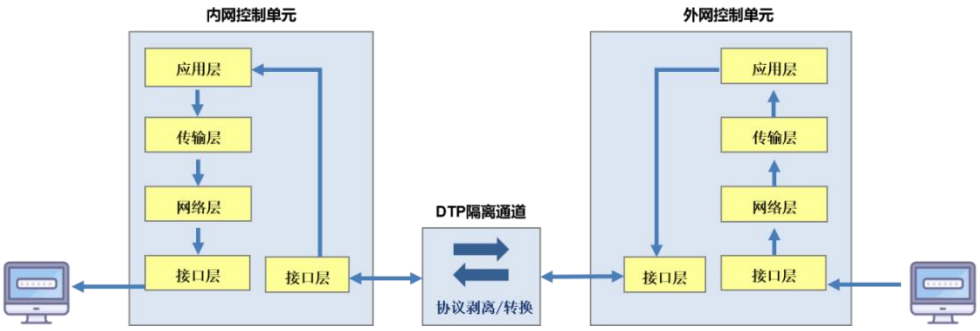


图 2.2-3　处理应用数据示意图

内网控制单元和外网控制单元分别部署于内端机和外端机上，二者各自构成内网与外网的物理边界，同时也是网络协议的终结点。所有穿越网闸的应用层信息首先从 TCP/IP 协议包中被完整剥离，还原为裸数据；随后，这些裸数据通过专用硬件接口及自定义的安全通信协议，被传输至数据通道控制系统。数据通道控制系统对接收到的数据进行深度解析、安全过滤与协议重组等处理，再将其转发至对端；数据抵达目标端后，重新封装为标准通信协议（如 TCP/IP 包格式），最终交付给内网或外网的应用系统。

在整个过程中，内网与外网之间仅交换纯粹的應用数据，所有网络协议信息与控制指令均被阻断，从而彻底消除了基于网络协议漏洞的攻击风险，确保了跨网数据交换的纯洁性、安全性与可靠性。数据通道控制系统采用 xxx 公司自主开发的 DTP 专用硬件设备，并运行自定义的安全通信协议，与内端机、外端机建立专属连接。由于系统本身无法通过任何标准网络协议直接访问，因此能够有效抵御来自内外网络的攻击，保障自身安全。

3. 核心功能

聚铭安全隔离与信息交换系统采用先进的高性能多核硬件架构，搭载拥有自主知识产权的多核多线程并行安全操作系统，配备接口丰富的硬件平台，支持映射、网关、透明、路由等多种部署模式，能够最大限度地兼容用户现有网络架构与环境，实现灵活全面的应用场景覆盖。

产品集文件同步、数据库同步、文件交换审批、音视频交换、安全浏览、工业控制等功能模块于一体，在确保内外网物理隔离的同时，为业务系统提供高效便捷的数据交换服务。通过集成 FTP 访问、数据库访问、HTTP/HTTPS、TCP/UDP 等应用代理，网闸彻底阻断内外网之间的直接通信，禁止建立任何 TCP 连接，仅在应用层进行协议过滤和代理请求，从而有效保护内部网络免受攻击。

图 3-1　核心功能示意图

3.1. 文件同步

聚铭安全隔离与信息交换系统内置文件同步模块，可满足内网与外网服务器之间的自动文件同步需求，无需开放任何连通内外网两侧的网络通道和端口，在保证绝对安全的前提下，通过纯数据摆渡实现。文件同步请求由网闸主动发起，无需安装任何第三方插件，兼容 Windows、Linux 及国产银河麒麟、统信 UOS 等操作系统平台。

配合网闸先进的防病毒引擎和海量病毒特征库，能够精准识别并清除夹杂在文件中的流行木马和顽固病毒。

基于语义分析引擎，深度识别文件内容，全方位的立体保护用户的关键数据，避免机密文件泄露和经济损失。

图 3.1　文件同步示意图

功能特点：

- 基于 FTP、SMB、NFS、FTPS、SFTP 等文件传输协议自动文件共享同步
- 自定义文件传输方向，如内到外、外到内或双向同步等
- 丰富的同步模式，如全量同步、增量同步等
- 基于先进的防病毒和语义分析引擎，实现病毒木马查杀和内容过滤
- 丰富的同步设置，如同步大小区间限制、小文件优先同步、文件并发传输、文件优先级同步
- 实时或定时的文件自动传输
- 详细的文件传输事件记录

3.2. 文件交换

文件交换模块是解决内外网物理隔离的场景中，实现各部门、人员之间的文件便捷发送，且无需建立内外网之间的 TCP/IP 网络连接，确保安全。采用创新性的“文件投递”模式进行文件交换，用户操作采用类似“快递寄件”的方式，只需登录客户端选择发件人、收件人等信息，文件即可精准送达。文件送达进度可视，文件送达审批等多项高级功能。

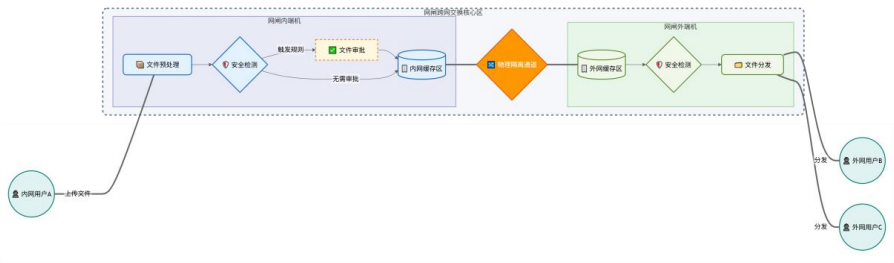


图 3.2　文件交换流程图

功能特点：

- 提供专用文件交换客户端，支持 Windows、统信 UOS、银河麒麟等主流操作系统
- 内置组织架构和用户组列表
- 对接 AD 域服务器，自动获取域用户，实现 AD 域账户的身份鉴别
- 一对一、一对多、多对一的文件发送/接收
- 客户端自动启动、文件自动接收
- 传输加密，断点续传
- 文件审批
- 详细的文件发送/接收等事件记录

3.3. 数据库同步

聚铭安全隔离与信息交换系统内置数据库同步模块，可满足内网与外网服务器之间的数据库同步需求，无需开放任何连通内外网两侧的网络通道和端口，在保证绝对安全的前提下，通过纯数据摆渡实现。数据库同步请求由网闸主动发起，无需安装任何第三方插件，支持 Mysql、SQL Server、ORACLE 等主流数据库及国产数据库。

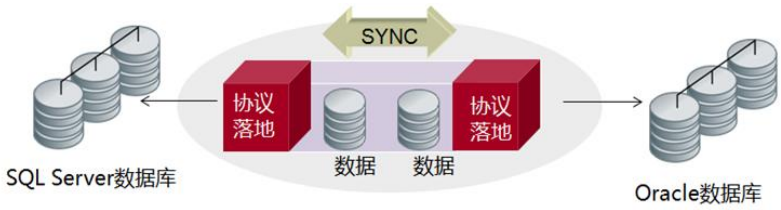


图 3.3　数据库异构同步示意图

功能特点：

- 兼容主流数据库及国产数据库
- 自定义传输方向，如内到外、外到内或双向同步等
- 丰富的同步模式，如全量同步、增量同步等
- 类视图管理，可灵活选择同步的表、字段、主键等
- 灵活的数据冲突策略
- 实时或定时的数据自动同步

- 视图同步模式，支持原视图到目的表同步
- 同步中无目的表自动创建目的表
- 同构及异构数据库自适应
- 详细的数据同步事件记录

3.4. 音视频交换

聚铭安全隔离与信息交换系统交换模块，通过对视频协议进行深度解析，严格区分视频数据流和控制信令流，根据策略配置可以控制视频数据的单向传输。并通过被动或者主动探测，对接入点身份进行审查，对未通过审查的对象一律丢弃，保证视频数据交换的安全可靠。

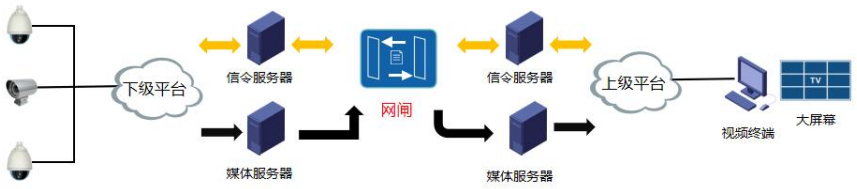


图 3.4　音视频交换示意图

功能特点：

- GB28181(SIP)、GB35114、RTSP 等主流视频协议
- H.263、H.264、M-JEPG、MPEG4 等视频编码
- 视频信令指令的控制，支持信令和媒体服务器分离场景
- 内置丰富的视频厂商协议，海康、大华、H3C、天视、星望、科达、天久、互信互通、先进视讯视频等主流视频厂商
- 策略级日志开关，日志内容精确到 IP 地址、SIP 编号、平台信息、信令内容和请求时间
- 支持 TCP、UDP 信令和码流
- 视频接入服务器、视频接入用户认证

3.5. 安全浏览

安全浏览模块主要用于内外网物理隔离的同时，提供内部网络对外部网络的 Web 网页浏览服务。

功能特点：

- 自定义 HTTP/HTTPS 指令级黑白名单和 URL 地址过滤
- 基于会话级的内容过滤策略，允许不同会话采用不同的内容访问控制策略
- 对访问源地址、目的地址、源端口、目的端目、域名进行访问控制

3.6. 工业控制

聚铭安全隔离与信息交换系统用于工业网络，特别是工业生产网与管理网之间物理隔离时，工业控制模块具备对工控协议的深度解析和指令过滤，以保护 SCADA、DCS、PLC 等工控系统免受来自外部的网络攻击，并实现工业数据的采集和上传。

功能特点：

- OPC 动态端口及读写控制
- 内置丰富的工控协议的识别和控制过滤
- 区分读写操作，黑白名单可单独针对写操作
- 监控协议动作和参数
- 策略级日志开关，详细记录策略的时间、IP、端口、协议、命令、参数、结果
- 策略级运行时间控制，在指定时间内放行

3.7. 数据库安全访问

数据库安全访问模块常用于客户端和数据库服务器之间的访问服务，用于处理客户端访问数据库服务器时的所有请求。通过代理访问，确保应用程序不必跟踪与数据库层相关的任何内容。基于对 SQL 协议的深度解析，可以对 SQL 语句进行过滤。

功能特点：

- 内置常见的 SQL 操作过滤
- 可自定义 SQL 语句黑白名单
- 内置白名单策略，如源 IP 白名单、账号白名单、数据库白名单、表白名

单

3.8. FTP 安全访问

FTP 安全访问模块常用于客户端和 FTP 服务器之间的访问服务，用于处理客户端访问 FTP 服务器时的所有请求。通过代理访问，确保应用程序不必跟踪与数据库层相关的任何内容。基于对 FTP 协议的深度解析，可对 FTP 指令进行过滤。

4. 其他功能

4.1. TCP 单向通信

深度解析 TCP 协议数据，采用截断 TCP 连接的方法，剥离数据包中的 TCP 报文头，实现将内网的纯数据发送到外网，且只允许应用层不带任何数据的 TCP 包的控制信息传输到内网，保护内网关键信息系统的安全性，同时符合电力系统规定支持 1 Bit 返回模式进行数据验证的需求。

4.2. 组播应用

网闸内置组播功能，广泛适用于广电等音视频场景，通过使用 IP 组播技术来分发数据，解决了单播情况下数据的重复拷贝及带宽的重复占用，从本质上解决了广播方式下带宽资源的浪费。

4.3. 自定义通信

通过内置的协议自定义模块，用户可以灵活定义业务相关的通信协议。

如自定义一项 HTTP/HTTPS 业务通信协议，接受来自内网客户端的访问请求，并经安全策略认证通过后，代理模块向安全策略指定的位于 Internet（外网）上的服务器发起加密请求，并将服务器返回结果解密后传送至内网客户端。网闸的代理模块与服务器的通信经过加密处理，可有效防止网络窃听，同时网闸代理模块只与特定的服务器交换信息，可有效防止内网对外部非法 Web 网站的访问。

4.4. NTP 代理

NTP 代理模块主要用于内外网物理隔离的情况下，内部服务器或终端不具备公网访问能力，为避免内网系统时钟的误差，则可通过网闸 NTP 代理模块为内网提供时钟校准服务。同时阻断一切 TCP/IP 网络连接，确保内网安全。

4.5. 高可用

系统采用技术领先的高可靠软硬件设计，支持双电源冗余、链路聚合、双机热备等，可预防网络或者硬件出现单点故障的情况，保障业务的连续性。

4.6. 集群组

网闸内置集群功能模块，我们在设计网络架构时，可以在网络关键位置部署多台（每组最大 16 台）隔离网闸设备，组成负载均衡集群组，以提升网络的性能和可靠性。

多台网闸设备相连组成一个负载均衡集群组，基于 VRRP 协议，共同维护一个 ViP（虚拟地址）。ViP 会随机挂载到集群中的网闸上，提供相同或相似的网络服务，每台网闸系统内置负载均衡模块，负责根据已配置均衡策略(Random)\轮询 (RoundRobin)\最少连接数(Leastconn)\源 IP(source) 等随机将用户请求在网闸负载均衡集群中的分发，为用户提供服务，并对网闸可用性的维护。

4.7. 病毒查杀和入侵防御

聚铭安全隔离与信息交换系统内嵌防病毒模块和实时入侵检测模块，提供病毒防护和查杀功能。可对 BasicAttack、 SMTP、FTP、DNS、DOS/DDOS 攻击、PortScan 等入侵行为进行实时检测。并产生相关日志和告警，实时通知系统管理员。

4.8. 安全控制

通过接口、IP 地址、端口、服务等五元组策略，控制 IP 包转发流向，从而在路由映射的场景下，访问控制更契合场景，更加灵活。

4.9. 防暴力破解

系统支持防暴力破解机制，账户错误登录次数达到预设阈值上限，则被锁定；账户在预设时间内未做出任何操作行为，则账户自动退出登录。

可以设置登录 IP 次数限制，该功能可以设置一个用户名或一台客户端登录

系统的最大重试次数。

每一个用户名登录系统的最大重试次数默认为五次。当超过五次时，将被锁定，锁定时长默认为 5 分钟，并产生审计记录。

4.10. 状态监视

网闸具备液晶显示屏，可分别显示内外网机 IP 地址、CPU 使用率和内存使用率等整机信息，液晶面板可操控重启、关机、恢复出厂设置等，具有设备异常监测报警功能。此外，系统采用 Web 全中文图形可视化管理界面，内置图形化实时监控功能，可对 CPU、内存、硬盘、服务状态、链路状态等信息进行动态监视。

4.11. 身份鉴别

- 支持客户端认证与 WEB 认证；
- 支持用户名/口令和 USB-KEY 组合的双因子认证方式；
- 支持登录错误到达上限，强制锁定登录页面；
- 支持一定时间未操作系统强制登出；

4.12. 用户管理

系统采用三权分立管理模式，可对系统管理员、系统安全员、系审计员等角色进行不同授权管理，符合等级保护 2.0 要求。

4.13. 安全审计

可实时监测和记录系统运行状态、网络流量情况、安全事件信息、数据交换行为及用户操作记录进行细粒度审计，满足用户审计、事后溯源等需求。

支持备份功能，可指定备份策略，对系统的业务模块、配置文件、审计日志等分别进行备份和恢复，并提供导入、导出和查询功能。

支持标准的 SYSLOG/SNMP 协议，支持将日志分发到远程日志服务器存储。

5. 部署模式

5.1. 映射模式

映射模式用于连接不同的网络环境，聚铭安全隔离与信息交换系统可以实现DNAT（目标地址转换）和SNAT（源地址转换）。该模式下内部网络主机访问外部网络时，其源IP地址被转换，可以很好的起到隐藏内网结构，提升内网安全，同时具有节约IP地址资源的作用。

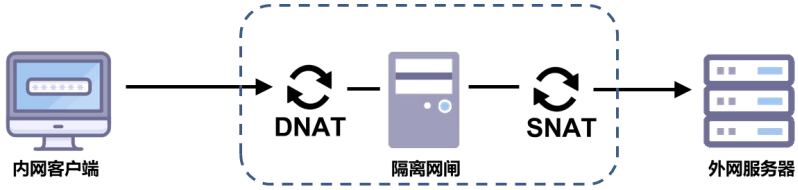


图5.1 映射模式部署示意图

5.2. 网关模式

网关模式下，使用网闸的出口IP地址替换内部网络的源地址向外部网络发送数据；当外部网络的响应数据请求返回到网闸后，网闸再将目的地址替换为内部网络的源地址。网关模式处理基于NAT技术，能够对外隐藏内部网络信息，进一步增强了对内部网络的安全防护。

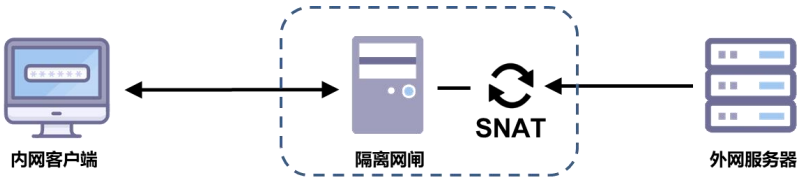


图5.2 网关模式部署示意图

5.3. 透明模式

如果内外网使用相同网段的IP地址，可以将聚铭安全隔离与信息交换系统应用透明模式，在透明模式下网闸工作在数据链路层，以透明网桥方式接入网络，可以部署到网络的网关位置或各部门的出口位置。无需改动用户网络结构和配置，即插即用如下图所示。

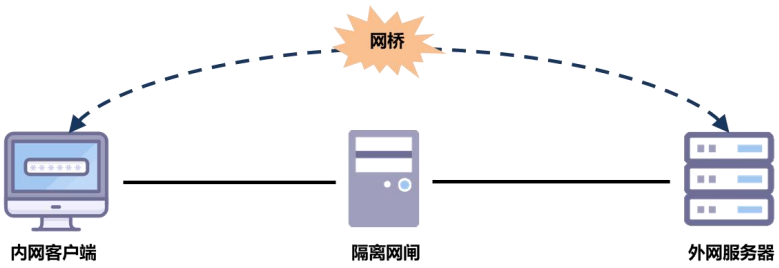


图 5.3　透明模式部署示意图

5.4. 路由模式

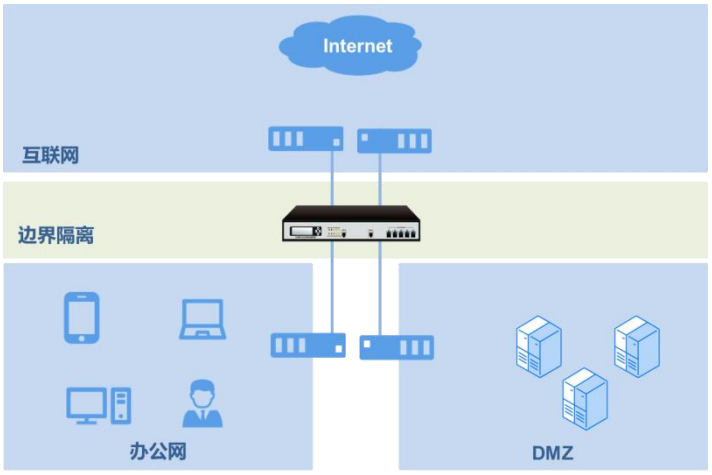
聚铭安全隔离与信息交换系统在路由模式下，将设备串接网络中，可以放于内网的任意子网边界，或与核心交换机相连。可以代替防火墙或路由器，需要为设备配置内网和外网接口的 IP 地址。

图 5.4　路由模式部署示意图

6. 应用场景

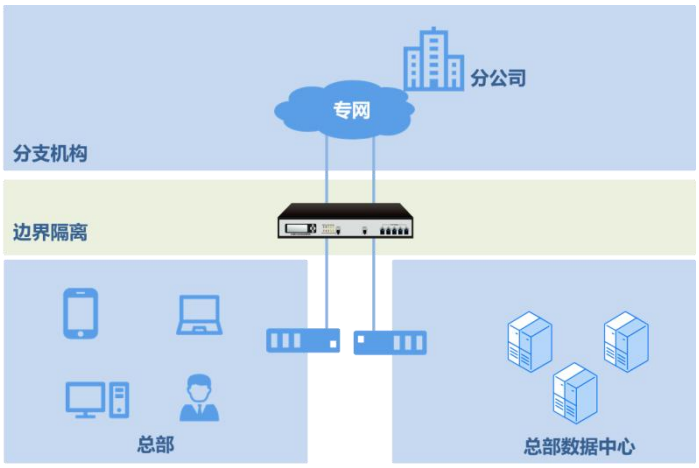
6.1. 内网与互联网边界的安全隔离

网闸部署在企业内网与互联网的边界，可以保护用户内部网络的整体安全。



6.2. 分支机构与总部网络边界的安全隔离

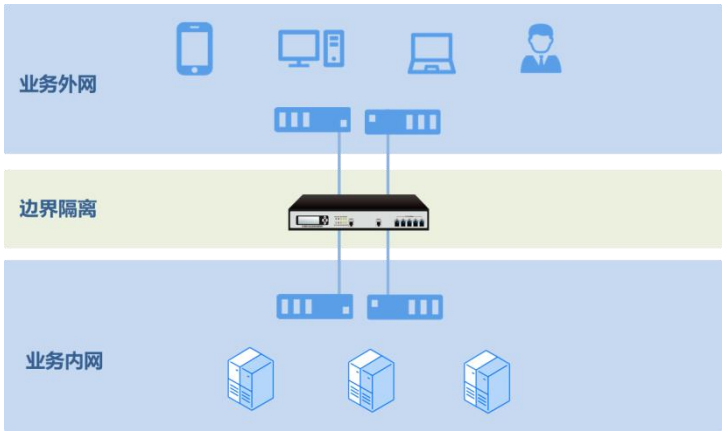
行业用户存在总部网络和分支机构网络的情况，比如国企、政府部门。由于总部网络敏感信息较为集中，安全要求较高，通常和下属分支机构或单位可通过在网络边界部署网闸实现安全隔离与互联互通。



6.3. 核心业务网与办公网之间的安全隔离

通常政府单位或企事业单位的网闸都划分有独立的外网和内网。例如电子政

务面向互联网的业务系统都部署在业务外网上。而数据库等核心设备都置于内网。当业务外网需要访问内部的数据库等资源时，就必须通过隔离网闸来实现数据的安全交换。



6.4. 业务网与业务网之间的安全隔离

大型企事业单位的网络系统可能很庞大，并且按照不同部门、业务、系统的安全等级划分成不同的网络安全区域。这些网络区域间的通信通过部署网闸可以实现安全隔离。