

国家电子政务外网标准

GW0205—2014

国家电子政务外网 跨网数据安全交换技术要求与实施指南

Technical Requirements and Implementation Guide

for Secure Data Exchange Across Regional Networks

of The National E-Government Network

2014 – 11-13 发布

2015– 1-1 实施

国家电子政务外网管理中心

目 次

前 言	I
引 言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 技术框架	3
4.1 系统架构	3
4.1.1 跨网数据安全交换系统架构	3
4.1.2 跨网数据安全交换对象和交换方式	3
4.1.3 跨网数据安全交换系统组成	3
4.2 功能结构	3
5 技术要求	4
5.1 功能要求	4
5.1.1 数据库数据交换	4
5.1.2 文件数据交换	5
5.1.3 流媒体数据交换	5
5.1.4 请求命令与响应数据交换	5
5.2 安全要求	5
5.2.1 隔离性要求	5
5.2.2 设备认证要求	6
5.2.3 访问控制要求	6
5.2.4 内容安全要求	6
5.2.5 可用性要求	6
5.2.6 安全管理与审计要求	6
6 实施指南	7
6.1 部署要求	7
6.2 数据交换方案选择	7
6.3 数据交换模式选择	7
6.3.1 数据库数据交换和文件数据交换	7
6.3.2 流媒体数据交换和请求命令与响应数据交换	10
6.4 性能要求	10
6.4.1 数据库数据交换	10
6.4.2 文件数据交换	11
6.4.3 流媒体数据交换	11
6.4.4 请求命令与响应数据交换	11
6.5 管理要求	11
附 录 A（资料性附录） 数据交换需求表	12
附 录 B（资料性附录） 业务配置信息需求表	13
附 录 C（资料性附录） 前置机信息表	15

前 言

为进一步规范国家电子政务外网（以下简称“政务外网”）区域网络隔离和跨网数据安全交换的技术要求，满足各级政务部门业务应用系统跨网数据同步的实际需求，结合政务外网建设实践及跨网数据安全交换系统部署经验，编制政务外网跨网数据安全交换技术要求与实施指南(以下简称“指南”)。

本指南由国家电子政务外网管理中心提出并归口。

本指南主要起草单位：国家电子政务外网管理中心、杭州合众信息技术股份有限公司、北京国保金泰信息安全技术有限公司、北京天行网安信息技术有限责任公司、上海辰锐信息科技有限公司、北京中宇万通科技有限公司。

本指南主要起草人：焦迪、罗海宁、邵国安、周民、吕品、梁智、闵剑、张震宇、李克亮、王伟、史林港、杜华、李志鹏、李天阳、樊志杰、高旭旻。

引 言

为了满足中央、省（自治区、直辖市）、地（市）政务部门跨网数据安全交换的实际需求，特编制本指南，用以规范各级政务外网跨网数据安全交换系统的建设、运行和管理。本指南包括政务外网跨网数据安全交换技术框架、技术要求及实施指南的主要内容，并详细阐述了跨网数据安全交换系统的功能、性能和安全要求。

涉及国家秘密的信息系统和数据与非涉密信息系统和数据之间的跨网交换按国家主管部门的相关规定执行。

国家电子政务外网跨网数据安全交换技术要求与实施指南

1 范围

本指南适用于指导各级政务外网建设运维单位开展跨网数据安全交换系统的建设、运行和管理工作的，主要针对政务外网互联网接入区、公用网络区数据中心内服务器的跨网数据同步与安全交换提出技术要求与实施指南。

其他政务部门物理隔离的局域网之间有数据安全交换需求的可参照使用。

2 规范性引用文件

下列文件中的条款通过本指南的引用而成为本指南的条款。凡是注明日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本指南。凡是不注明日期的引用文件，其最新版本适用于本指南。

GE 17859 计算机信息系统安全保护等级划分准则
GB/T 20269 信息安全技术 信息系统安全管理要求
GB/T 20270 信息安全技术 网络基础安全技术要求
GB/T 20271 信息安全技术 信息系统安全通用技术要求
GB/T 20272 信息安全技术 操作系统安全技术要求
GB/T 20273 信息安全技术 数据库管理系统安全技术要求
GB/T 20279 信息安全技术 网络和终端设备隔离部件安全技术要求
GB/T 20282 信息安全技术 信息系统安全工程管理要求
GB/T 22239 信息安全技术 信息系统安全等级保护基本要求
GB/T 22240 信息安全技术 信息系统安全等级保护定级指南
GB/T 28181 安全防范视频监控联网系统信息传输、交换、控制技术要求
《公安信息通信网边界接入平台安全规范》（公信通[2007]191号）

3 术语和定义

下列术语和定义适用于本指南。

3.1

跨网 Across Regional Networks

政务外网城域网内采用VPN技术逻辑隔离且无协议通信的网络之间，或者是物理隔离的网络之间。

3.2

数据库数据 Database Data

按照数据结构来组织、存储在数据库系统中的数据信息。这里主要指关系型数据库数据，属于结构化数据。

3.3

计算机文件数据 File Data

存储在磁盘、光盘、磁带等长期储存设备上的数据。这里主要指Office文档、文本文档、视频文件、图片文件、图纸文件等，属于非结构化数据。以下简称文件数据。

3.4

请求命令与响应数据 Request and Response Data

基于服务器之间一方发送的请求数据和另一方返回的响应数据所形成的应用交互协议数据，这里主要指应用服务器与数据库服务器之间、应用服务器与文件服务器之间的请求命令与响应数据。

3.5

流媒体数据 Streaming Media Data

采用流式传输的方式在网络中播放的媒体格式数据。

3.6

协议转换 Protocol Conversion

协议的剥离和重建。在所属某一网络的隔离部件一端，把基于网络的公共协议中的应用数据剥离出来，封装为系统专用协议传递至所属其他网络隔离部件的另一端，再将专用协议剥离，并封装成需要的格式。

3.7

信息摆渡 Information Ferry

信息交换的一种方式，物理传输信道只在传输进行时存在。信息传输时，信息先由信息源所在网络一端传输至中间缓存区域，同时物理断开中间缓存区域与信息目的地所在网络的连接；随后在信道上物理断开信息源所在网络与中间缓存区域的连接，接通中间缓存区域与信息目的所在网络的传输信道，将信息传输至信息目的地所在网络。在任一时刻，中间缓存区域只与一端网络相连。

3.8

网闸 Gap

一种信息安全隔离部件，位于两个不同物理网络或安全域之间，通过协议转换的手段，以信息摆渡的方式实现数据交换，且只有被系统明确要求传输的信息可以通过。

3.9

单向光闸 Unilateral Optical Gap

结合网闸技术和光传输技术的一种信息安全隔离部件，其特性是利用光的单向传播特性进行信息传输，确保信息在物理传导上的单向性，同时具有网闸的协议转换手段和信息摆渡方式。

3.10

前置机 Staging Server

跨系统进行数据交换和传输的中间设备，其主要功能有网络通信、数据认证、格式转换及数据缓冲等。

4 技术框架

4.1 系统架构

4.1.1 跨网数据安全交换系统架构

跨网数据安全交换系统是基于网闸和单向光闸技术,综合利用设备认证、格式检查等安全措施实现两个不同网络业务区服务器之间数据同步的平台。系统架构如图1所示:

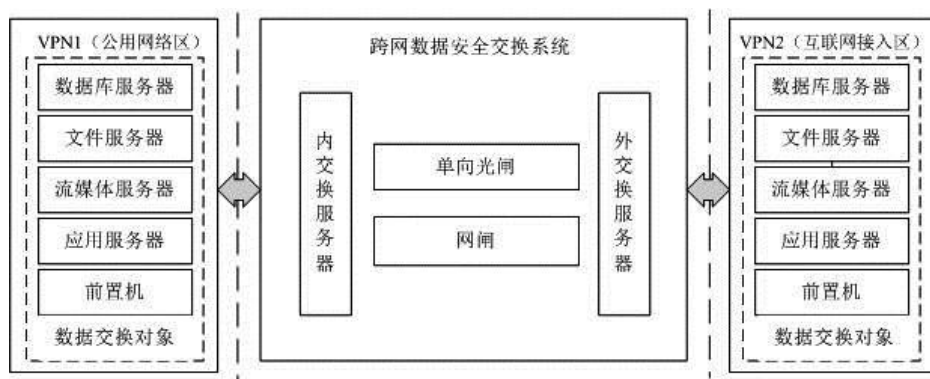


图1 跨网数据安全交换系统架构示意图

4.1.2 跨网数据安全交换对象和交换方式

a) 交换对象

根据交换对象种类的不同,可分为数据库数据、文件数据、流媒体数据、请求命令与响应数据。

b) 交换方式

根据交换数据流向的不同,可分为单向数据传输、双向数据传输。

4.1.3 跨网数据安全交换系统组成

- 单向光闸:通过协议转换,以信息摆渡的方式实现单向数据传输;与内、外交换服务器组成单向传输链路,适用于数据库数据、文件数据交换的单向传输。
- 网闸:通过协议转换,以信息摆渡的方式实现双向数据传输;包括普通网闸和视频网闸,与内外服务器组成双向传输链路,适用于数据库数据、文件数据、请求命令与响应数据和流媒体数据的双向传输。
- 内、外交换服务器:完成数据抽取、数据装载、设备认证、格式检查、内容过滤、安全审计等安全功能。

4.2 功能结构

跨网数据安全交换系统功能结构如图2所示:

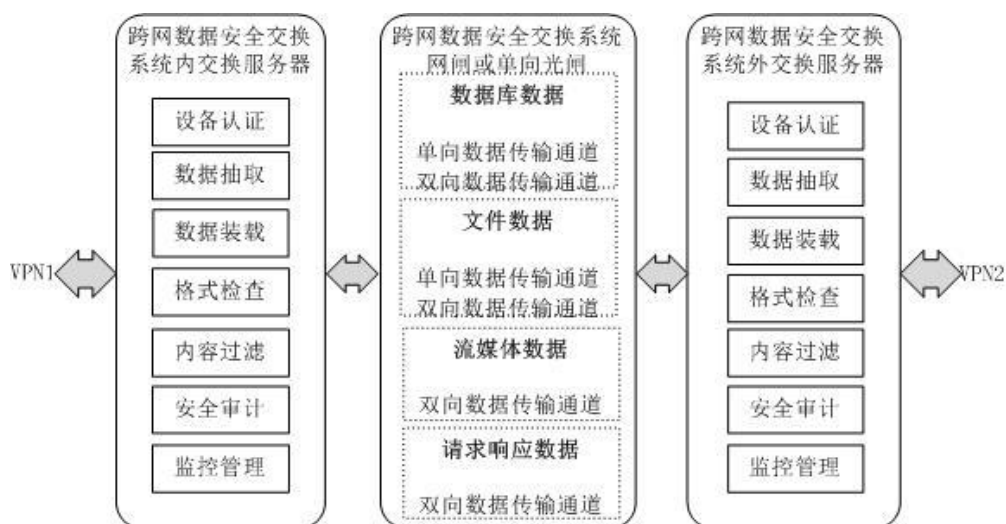


图2 跨网数据安全交换系统功能结构图

网闸和单向光闸通过协议转换，以信息摆渡的方式实现各类数据的双向和单向传输。内、外交换服务器作数据源时完成数据抽取、格式检查、内容过滤、设备认证，作数据目标时完成数据装载、设备认证；外交换服务器应具备向内交换服务器发送监控、报警信息并接受内交换服务器配置指令的功能。

数据库数据、文件数据交换时内、外交换服务器应具备设备认证、数据抽取、数据装载、格式检查、内容过滤、安全审计、监控管理功能。

流媒体数据、请求命令与响应数据交换时内、外交换服务器应具备设备认证、格式检查、内容过滤、安全审计、监控管理功能。

各子模块应具备如下功能：

- 设备认证：基于数字证书、IP 地址绑定等技术对连接跨网数据安全交换系统的设备进行设备身份认证，禁止未认证设备上线；
- 数据抽取：从源端前置机或信息系统抽取待交换的数据库数据、文件数据到跨网数据安全交换系统；
- 数据装载：从跨网数据安全交换系统将数据库数据、文件数据装载到目标端前置机或信息系统；
- 格式检查：对交换对象的格式根据事先定义的规则进行关于范围、长度、类型等检查；
- 内容过滤：对交换对象的内容进行病毒检测、木马过滤；
- 安全审计：提供跨网数据安全交换行为审计、管理员配置管理审计等；
- 监控管理：提供跨网数据安全交换系统运行状态实时监控、交换业务配置管理、交换业务统计分析、安全事件实时报警等。

5 技术要求

5.1 功能要求

5.1.1 数据库数据交换

- 支持主流数据库系统；
- 支持主流操作系统；
- 支持异构数据库之间的数据交换；
- 支持历史数据和增量数据的交换；
- 支持时间戳、视图、触发器、日志等数据抽取模式；
- 支持基于字段值、行、列等条件的数据交换；
- 支持实时、定时的数据交换；

- h) 支持数据库交换的断点续传；
- i) 具备数据传输完整性和一致性检查机制。

5.1.2 文件数据交换

- a) 支持主流文件类型；
- b) 支持主流操作系统；
- c) 支持异构文件系统之间的数据交换；
- d) 支持历史文件、增量文件的数据交换；
- e) 支持 FTP、SMB、共享文件夹等文件数据抽取模式；
- f) 支持基于特定条件的文件数据交换；
- g) 支持实时、定时的文件数据交换；
- h) 支持文件交换的断点续传；
- i) 具备数据传输完整性和一致性检查机制。

5.1.3 流媒体数据交换

- a) 支持主流流媒体数据类型；
- b) 支持主流流媒体协议；
- c) 支持视频控制信令的数据交换；
- d) 支持视频流数据的双向或单向传输。

5.1.4 请求命令与响应数据交换

- a) 支持主流数据库服务协议、文件服务协议、应用服务协议的识别和过滤；
- b) 支持实时请求命令与响应数据交换。

5.2 安全要求

5.2.1 隔离性要求

5.2.1.1 数据库数据交换

- a) 单向数据传输采用单向光闸或网闸作为唯一连接通道，通过协议转换，以信息摆渡的方式实现单向数据交换，同时必须确保数据无反向传输；
- b) 双向数据传输采用网闸作为唯一连接通道，通过协议转换，以信息摆渡的方式实现双向数据交换。

5.2.1.2 文件数据交换

- a) 单向数据传输采用单向光闸或网闸作为唯一连接通道，通过协议转换，以信息摆渡的方式实现单向数据交换，同时必须确保数据无反向传输；
- b) 双向数据传输采用网闸作为唯一连接通道，通过协议转换，以信息摆渡的方式实现双向数据交换。

5.2.1.3 流媒体数据交换

流媒体数据交换采用专用流媒体网闸作为唯一连接通道，通过协议转换，以信息摆渡的方式实现数据交换。

流媒体网闸应具备流媒体协议转换、流媒体控制信令的过滤和检查功能，并适应快速信息摆渡。

5.2.1.4 请求命令与响应数据交换

请求命令与响应数据交换采用网闸作为唯一连接通道，通过协议转换，以信息摆渡的方式实现数据交换，同时必须确保阻断传输层（含）以下的网络协议。使用此类数据交换时，不建议采用前置机方式。

5.2.2 设备认证要求

- a) 应确保非法设备无法通过数据安全交换系统实现数据交换，交换对象应采用 IP 地址绑定、设备数字证书或 SNMP 等方式进行设备认证；
- b) 若采用设备数字证书认证方式，应支持政务外网数字证书。

5.2.3 访问控制要求

- a) 支持通过用户名口令、数字证书方式对系统管理员和操作员进行身份认证，认证支持政务外网数字证书，应通过政务外网现有认证体系进行认证，也可离线认证；
- b) 支持对系统管理员、系统安全员、系统审计员进行不同角色的授权管理。

5.2.4 内容安全要求

5.2.4.1 数据库数据交换

- a) 支持对数据库字段类型、长度等进行安全格式检查；
- b) 支持对数据库字段内容进行关键字过滤；
- c) 支持对数据库大字段内容进行病毒查杀；
- d) 支持不同数据库之间数据交换时格式转换。

5.2.4.2 文件数据交换

- a) 支持对文件类型、长度等进行安全格式检查；
- b) 支持对文件内容进行关键字过滤；
- c) 支持对文件内容进行病毒查杀。

5.2.4.3 流媒体数据交换

支持对不同视频系统的协议进行识别和过滤，支持白名单保护机制。

5.2.4.4 请求命令与响应数据交换

- a) 支持对请求命令与响应的参数类型、长度等进行安全格式检查；
- b) 支持对请求命令与响应内容进行关键字过滤；
- c) 支持对请求命令与响应内容进行病毒查杀。

5.2.5 可用性要求

- a) 单向数据传输系统支持链路冗余，应在一条链路故障时保证单向数据的传输；
- b) 双向数据交换系统支持热备，应在故障时自动切换交换任务到其他运行的双向数据交换系统；
- c) 双向数据交换系统支持负载均衡，应根据负载自动切换交换任务到其他运行的双向数据交换系统。

5.2.6 安全管理与审计要求

- a) 支持实时监控跨网数据安全交换系统业务状态、通道运行状态；
- b) 支持通过图、表等方式展现跨网数据安全交换系统业务相关统计信息，并按不同时间粒度和区间汇总；
- c) 支持对跨网数据安全交换系统的行为、安全事件和交换内容等进行审计；
- d) 支持对系统管理员、系统安全员、系统审计员管理行为进行审计；

- e) 支持安全事件报警功能;
- f) 支持配置文件、审计日志的备份功能,并提供备份数据的导入、导出、查询功能;
- g) 支持接收符合标准 SYSLOG 或 SNMP 接口规范的审计日志;
- h) 支持对审计数据保存大小上限进行动态设置。

6 实施指南

6.1 部署要求

- a) 中央、省、地市分级建设跨网数据安全交换系统,分级部署;
- b) 以局域网方式接入到地市的县级政务外网暂不要求建设交换系统,局域网内的不同安全域可采用防火墙等安全隔离措施进行数据交换。

6.2 数据交换方案选择

- a) 数据交换类型的选择
 - 1) 根据业务需要选择数据交换对象,如数据库数据交换、文件数据交换、流媒体数据交换和请求命令与响应数据交换;
 - 2) 根据业务需要选择数据交换流向,如单向数据交换、双向数据交换;
 - 3) 数据责任主体单位通过填写数据交换需求表(见附录 A)及业务配置信息需求表(见附录 B)来明确业务需求、数据交换方向、交换对象信息等。
- b) 数据传输链路的选择
 - 1) 当存在数据单向传输安全需求,应使用单向数据传输链路,即数据必须严格保证从一侧网络向另一侧网络单向传输且没有反向数据传输;
 - 2) 当两侧网络间数据传输吞吐量大于跨网双向数据传输链路中网闸最大通量时,可建设两条相反方向的单向数据传输链路。
- c) 前置机方式的选择
 - 1) 从数据交换对象划分,数据库数据交换和文件数据交换可采用前置机方式,流媒体数据和请求命令与响应数据可直接交换;
 - 2) 如果跨网数据安全交换系统和数据责任主体单位相同,则不需要采用前置机方式,直接从信息系统中抽取数据进行跨网数据安全交换;
 - 3) 如果跨网数据安全交换系统和数据责任主体单位不同,则需要采用前置机方式,在不同责任主体单位之间放置前置机,有交换需求的部门将数据主动推送到前置机上,由跨网数据安全交换系统从前置机中抽取数据进行跨网数据安全交换。

6.3 数据交换模式选择

6.3.1 数据库数据交换和文件数据交换

根据跨网数据安全交换的信息系统的部署位置、责任主体单位以及前置机部署需求的不同,将跨网数据库数据和文件数据安全交换分为双前置、单前置、无前置三种模式。

6.3.1.1 双前置模式

- a) 适用场景:跨网数据安全交换系统和两端数据(数据库及文件服务器)责任主体为两个不同的单位,则跨网数据安全交换系统两端都面向前置机,将前置机上的数据抽取后装载到另一端的前置机上,与信息系统之间没有直接连接。
- b) 前置机作用:负责对需要进行数据交换的数据库服务器、文件服务器进行设备认证,跨网数据安全交换系统负责对前置机进行设备认证。

- c) 前置机的要求：跨网数据安全交换系统的责任主体单位负责前置机的建设，前置机配置参考附录表C.3。
- d) 数据责任主体单位填写前置机需求表（见附录表C.1），跨网数据安全交换系统责任主体单位根据前置机需求表填写前置机反馈表（见附录表C.2）。

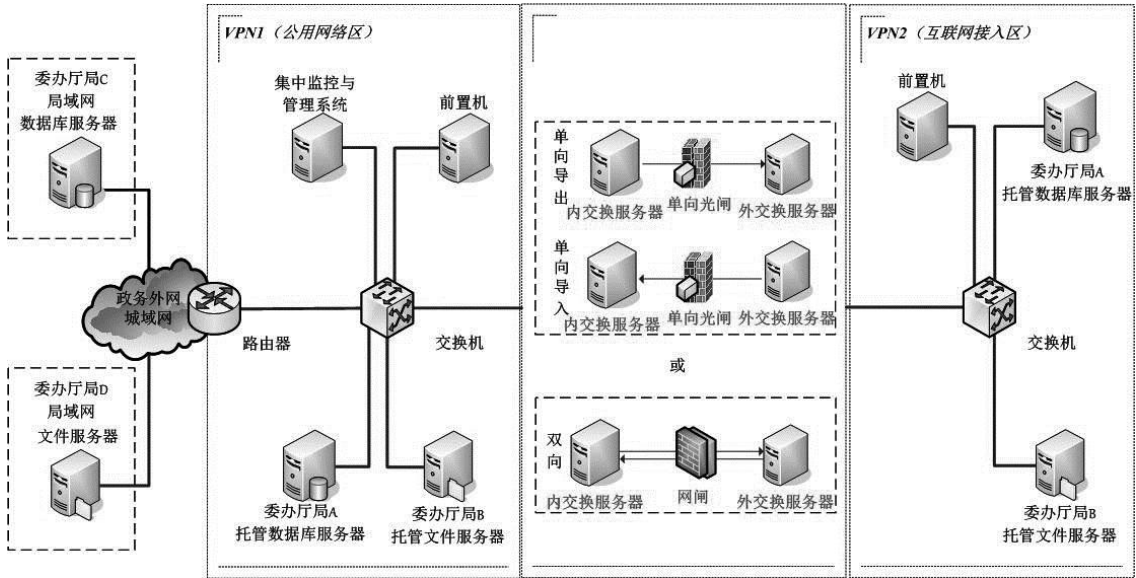


图3 双前置模式示意图

需要进行跨网数据安全交换的部门共用一台前置机，各部门将所需交换的数据主动推送到前置机上，由跨网数据安全交换系统到前置机抽取数据并将数据交换到另一端前置机上，各部门到此端前置机取数据。

业务量需求较小时，可以将前置机功能运行在跨网数据安全交换系统内、外交换服务器上，也可根据业务量实际需求增加前置机。

6.3.1.2 单前置模式

- a) 适用场景：跨网数据安全交换系统与数据（数据库及文件服务器）责任主体单位相同的一端可直接面向信息系统，与数据责任主体单位不同的一端面向前置机，将前置机上的数据抽取后装载到另一端的信息系统中。
- b) 前置机作用：负责对需要进行数据交换的数据库服务器、文件服务器进行设备认证，跨网数据安全交换系统负责对前置机、局域网内的数据库服务器、文件服务器进行设备认证。
- c) 前置机的要求：参照上一节双前置模式中前置机的要求。

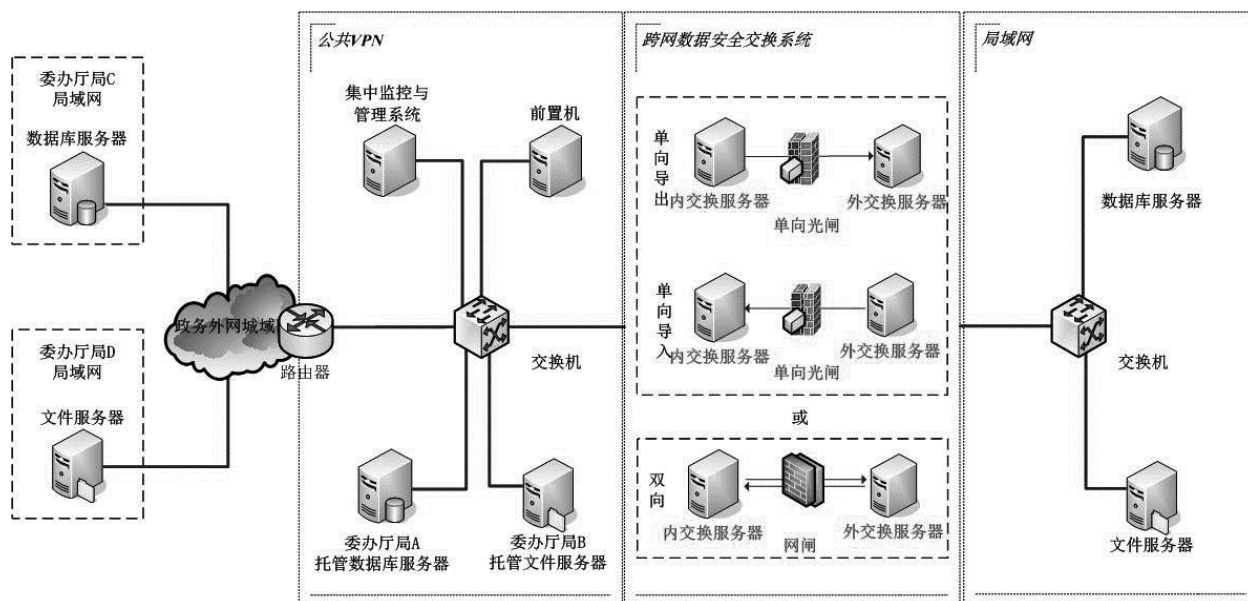


图4 单前置模式示意图

需要进行跨网数据安全交换的部门共用一台前置机，各部门将所需交换的数据主动推送到前置机上，由跨网数据安全交换系统到前置机抽取数据并直接交换到相关信息系统中。

6.3.1.3 无前置模式

适用场景：跨网数据安全交换系统和两端数据（数据库及文件服务器）责任主体为同一个单位，跨网数据安全交换系统两端直接面向信息系统，抽取和装载信息系统的数据，例如某政务部门内部两个物理隔离的局域网之间数据交换可采用此模式。

跨网数据安全交换系统负责对数据库服务器和文件服务器进行设备认证。

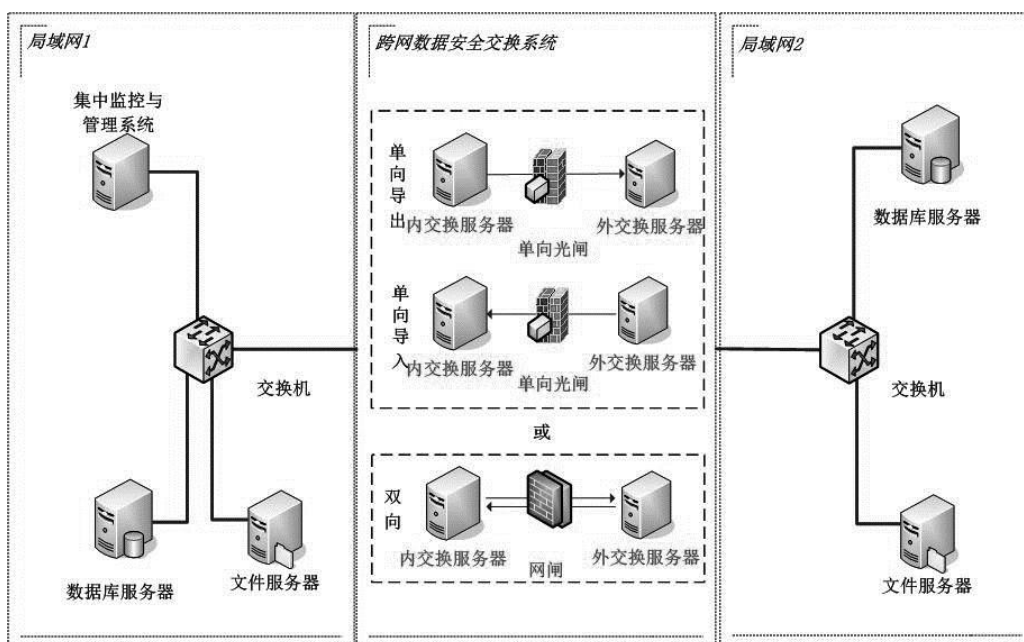


图5 无前置模式示意图

跨网数据安全交换系统直接连接信息系统抽取数据，并将数据交换到另一端信息系统中。

6.3.2 流媒体数据交换和请求命令与响应数据交换

适用场景：流媒体数据交换和请求命令与响应数据交换时，跨网数据安全交换系统两端直接面向信息系统。

跨网数据安全交换系统负责对流媒体服务器以及其他应用服务器进行设备认证。

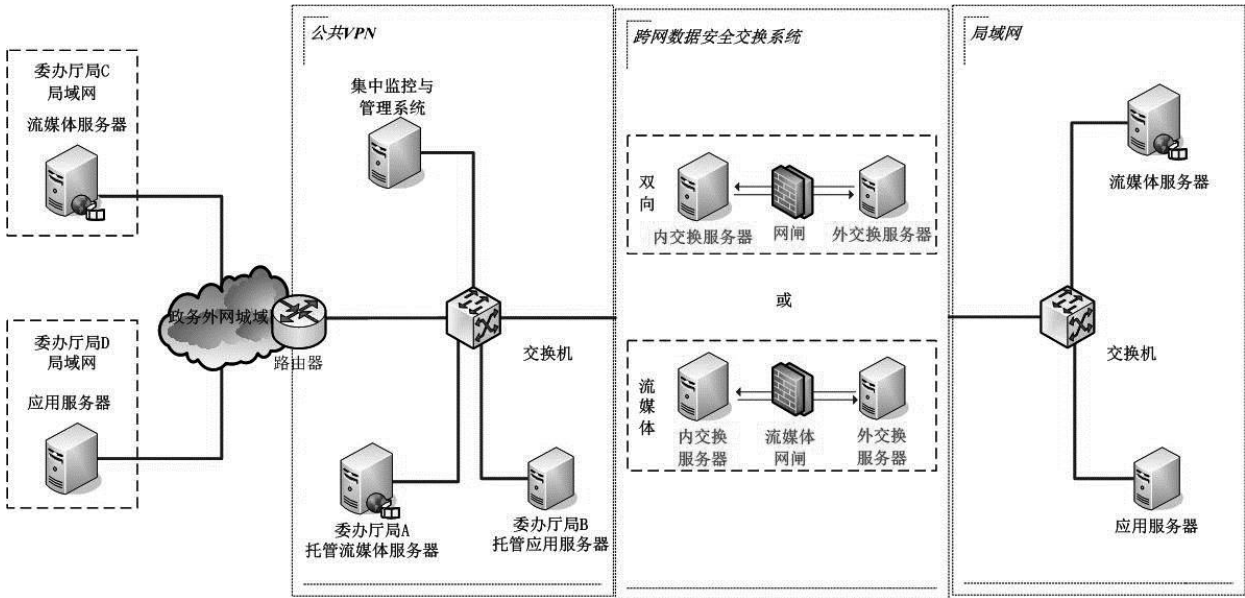


图6 流媒体数据交换和请求命令与响应数据交换模式示意图

跨网数据安全交换系统直接连接信息系统，并将数据交换到另一端信息系统中。

6.4 性能要求

根据并发量、日均数据交换量的不同需求，性能要求分为A类、B类两档，详见表1。以下性能指标都是在单一数据交换对象进行交换时对跨网数据安全交换系统的性能要求。

表1 性能要求分类基准表

数据交换对象 \ 级别	A 类	B 类
数据库数据	日交换量 2 亿条、200GB，并发表数 4000	日交换量 1 亿条、100GB，并发表数 2000
文件数据	日交换量 5 千万个、500GB，并发文件个数 60	日交换量 3 千万个、300GB，并发文件个数 30
流媒体数据	日交换量 5TB，并发连接数 300	日交换量 3TB，并发连接数 200
请求命令与响应数据	日交换量 6TB，并发连接数 3500	日交换量 3TB，并发连接数 2000

6.4.1 数据库数据交换

- a) A 类
 - 1) 数据库数据交换传输吞吐量不小于 400Mbps；
 - 2) 数据库到数据库传输记录数不小于 1500 条/秒。
- b) B 类
 - 1) 数据库数据交换传输吞吐量不小于 200Mbps；

- 2) 数据库到数据库传输记录数不小于 1000 条/秒。

6.4.2 文件数据交换

- a) A 类
 - 1) 文件数据交换个数（大于 10KB/文件）不小于 500 个/秒；
 - 2) 文件数据交换吞吐量不小于 500Mbps。
- b) B 类
 - 1) 文件数据交换个数（大于 10KB/文件）不小于 300 个/秒；
 - 2) 文件数据交换吞吐量不小于 300Mbps。

6.4.3 流媒体数据交换

- a) A 类
 - 1) 最大传输延时不大于 100ms；
 - 2) 视频传输能力不低于 300 路并发（每路 D1 画质，2Mbps）；
 - 3) 适用码流从 20Kbps 到 8Mbps；
 - 4) 数据包丢失率不大于 0.5‰。
- b) B 类
 - 1) 最大传输延时不大于 200ms；
 - 2) 视频传输能力不低于 200 路并发（每路 D1 画质，2Mbps）；
 - 3) 适用码流从 20Kbps 到 8Mbps；
 - 4) 数据包丢失率不大于 0.8‰。

6.4.4 请求命令与响应数据交换

- a) A 类
 - 1) 最大传输延时不大于 100ms；
 - 2) 最大并发请求数不小于 3500 个；
 - 3) 吞吐量不小于 700Mbps。
- b) B 类
 - 1) 最大传输延时不大于 200ms；
 - 2) 最大并发请求数不小于 2000 个；
 - 3) 吞吐量不小于 400Mbps。

6.5 管理要求

部署集中监控与管理系统应满足如下管理功能要求：

- a) 支持实时监控系统业务状态、通道运行状态；
- b) 支持通过图、表等方式展现系统业务相关统计信息，并应按不同时间粒度和区间汇总；
- c) 支持查询、检索、列表展现安全事件和交换内容等审计信息；
- d) 支持查询、检索、列表展现系统管理员、系统安全员、系统审计员管理行为等审计信息；
- e) 支持查询、检索、列表展现安全事件报警信息；
- f) 支持报警、审计日志的备份功能，并提供备份数据的导入、导出、查询功能；
- g) 支持接收符合标准 SYSLOG 或 SNMP 接口规范的日志。

附 录 A
(资料性附录)
数据交换需求表

表 A.1 数据交换需求表

业务系统名称	
业务种类	<input type="checkbox"/> 数据库数据 <input type="checkbox"/> 文件数据 <input type="checkbox"/> 流媒体数据 <input type="checkbox"/> 请求命令与响应数据
数据流向种类	<input type="checkbox"/> 双向 <input type="checkbox"/> 单向
业务单位名称	
联系人及电话	
业务接入拓扑图	
<p style="color: gray; text-align: center;">在拓扑中标识服务器等设备联网方式。如：互联网、VPDN、MPLS VPN、专线等。</p>	
填写内容说明 和要求	<ol style="list-style-type: none"> 1. 描述业务办理流程、业务处理逻辑； 2. 业务系统是否已经正常运行，检查安全隔离的网络两端有无承载该业务运行的服务器或数据库，如没有则需要增加服务器或数据库； 3. 服务器与跨网数据安全交换系统的连接方式； 4. 信息系统采用的请求命令与响应协议类型（如 HTTP、SOAP 等）； 5. 数据实时性要求（如：数据需在 10 分钟以内交换到目标端）； 6. 估算数据日交换总量（单位：MB）； 7. 数据库数据交换所涉及的数据库类型及版本或者文件数据交换所涉及的操作系统及版本； 8. 源端数据库记录交换后是否保留； 9. 源端数据库是否允许创建交换所需的触发器、存储过程、临时表，业务表是否存在主键、唯一索引、自增长型字段； 10. 选择数据交换对象，在附表中选择对应的业务配置信息需求表并填写完整。

附 录 B
(资料性附录)
业务配置信息需求表

表 B.1 数据库数据交换业务配置信息需求表

业务名称:					
需求描述					
交换方式	选择传输需求: <input type="checkbox"/> 外向内单向传输 <input type="checkbox"/> 内向外单向传输 <input type="checkbox"/> 双向交换				
数据操作方式	数据被同步后, 源端是否保留原始数据? <input type="checkbox"/> 保留 <input type="checkbox"/> 不保留				
业务需求单位			联系人及联系电话		
数据库连接配置					
() 所在网络名称、 区域名称	IP		() 所在网络名称、 区域名称	IP	
	字符集			字符集	
	库类型及版本			库类型及版本	
	数据库所有者 /SID			数据库所有者 /SID	
	库名			库名	
业务表同步 对应关系	内向外单向同步				
	源表:		目标表:		
	外向内单向同步				
	源表:		目标表:		
双向同步					
	源表:		目标表:		
业务表的主从 关系					
填写人 (签字、盖章)					

表 B.2 文件数据交换业务配置信息需求表

业务名称:					
需求描述					
同步方式	选择同步需求: <input type="checkbox"/> 外向内单向同步 <input type="checkbox"/> 内向外单向同步				
数据操作方式	数据被同步后, 源端是否保留原始数据? <input type="checkbox"/> 保留 <input type="checkbox"/> 不保留				
业务需求单位			联系人及联系电话		
文件服务器配置					
外端	IP		内端	IP	
	操作系统类型及版本			操作系统类型及版本	
	数据文件目录			数据文件目录	
文件格式审计 (允许类型/ 不允许类型)	如: 只允许 XML 通过		源端文件操作 方式	<input type="checkbox"/> 删除 <input type="checkbox"/> 保留	
是否扫描病毒	<input type="checkbox"/> 是 <input type="checkbox"/> 否		发现病毒操作 方式	<input type="checkbox"/> 隔离 <input type="checkbox"/> 隔离并报警	
同步模式(选择 其中一种)	<input type="checkbox"/> mount 方式: 业务服务器不允许安装客户端的情况下, 应通过共享业务服务器的数据目录实现数据的同步。 <input type="checkbox"/> agent 方式: 业务服务器允许安装客户端, 通过客户端与数据交换系统之间建立可信加密通道, 实现数据的同步。				
填写人 (签字、盖章)					

附 录 C
(资料性附录)
前置机信息表

表 C.1 前置机需求表 (由需求单位负责填写)

业务名称:	需求表编号(如2014/2/20/001):
交换方式	选择传输需求: <input type="checkbox"/> 外向内单向传输 <input type="checkbox"/> 内向向外单向传输 <input type="checkbox"/> 双向交换
数据管理软件	文件服务类型: <input type="checkbox"/> FTP <input type="checkbox"/> SMB <input type="checkbox"/> AGENT <input type="checkbox"/> 其他_____
连接服务器IP 列表	IP1: IP2: IP3:
前置模式	<input type="checkbox"/> 双前置 <input type="checkbox"/> 单前置
存储时间	文件在前置机上修改时间为判断依据, 超过此时间文件将被删除 <input type="checkbox"/> 1天 <input type="checkbox"/> 7天 (默认) <input type="checkbox"/> 30天 <input type="checkbox"/> 其他_____
其他需求描述	
填写人 (签字、盖章)	

表 C.2 前置机反馈表（由建设单位负责反馈）

业务名称：_____		对应需求表编号(如 2014/2/20/001)：_____	
反馈表编号(如 2014/2/20/001)：_____			
数据管理软件	文件服务类型： <input type="checkbox"/> FTP <input type="checkbox"/> SMB <input type="checkbox"/> AGENT <input type="checkbox"/> 其他_____ IP： 目录： 用户名：		
连接服务器 IP 列表	IP1： IP2： IP3：		
前置模式	<input type="checkbox"/> 双前置 <input type="checkbox"/> 单前置		
存储时间	文件在前置机上修改时间为判断依据，超过此时间文件将被删除 <input type="checkbox"/> 1 天 <input type="checkbox"/> 7 天（默认） <input type="checkbox"/> 30 天 <input type="checkbox"/> 其他_____		
存储要求	文件夹命名规则：单位首字母简写 文件命名规则：应用系统简称+日期+流水号，如 unimas-20140220-0000001 应用系统简称必须为纯英文字母，最长 20 位 日期为文件在前置机创建时间，格式为 YYYYMMDD，如 20140220 流水号每天重新从 1 开始计数，长度为 8 位，不足 8 位前面补零 系统简称、日期和流水号之间使用“-”字符连接		
其他需求确认			
填写人 (签字、盖章)			

表 C.3 前置机配置建议参考表

操作系统	CPU	内存	硬盘
Windows 2003 及以上 server 操作系统/Linux redhat	双路、四核、2.1GHz	32GB	1TB