SANGFOR
深信服科技

深信服安全隔离与信息交换系统
网闸 GAP-1000 V3.0 白皮书

深信服科技股份有限公司

2019 年 05 月 20 日

版权声明

免责条款

本文档仅用于为最终用户提供信息，其内容如有更改，恕不另行通知。

深信服科技股份有限公司在编写本文档的时候已尽最大努力保证其内容准确可靠，但深信服科技股份有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

信息反馈

如果您有任何宝贵意见，请反馈至：

地 址：深圳市南山区学苑大道 1001 号南山智园 A1 栋

邮 编：518055

电 话：0755-86627888

传 真：0755-86627999

您也可以访问深信服科技网站：www.sangfor.com.cn 获得最新技术和产品和方案信息。

目 录

1 概述

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地提高了办公效率。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，尤其是针对涉密信息的防护，党和政府已将信息安全建设提到一个相当的高度上来。自 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。但是标准安全隔离技术虽然从物理上隔离了两个网络，但是其物理安全通道的方向性可由软件控制。对于涉密网络，需要的是防止任何泄密的可能，因此如何从物理层完成数据流向的控制成为一个亟待解决的问题。

2 需求背景

2.1 法规标准要求

2.1.1 等级保护

当前我们国家正面临经济社会结构调整和转型，信息技术已经成为新的引擎，可以预见，网络和信息系统作为新兴动力的承载者，必将构建起整个经济社会的神经中枢，其重要性带来的必然是安全保障的紧迫性。

为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展。2016 年十二届全国人大常委会第二十四次会议表决通过的《中华人民共和国网络安全法》于 2017 年 6 月 1 日起实施。网络安全法明确了网络空间主权的原则，明确了网络产品和服务提供者的安全义务，明确了网络运营者的安全义务，进一步完善了个人信息保护规则，建立了关键信息基础设施安全保护制度。

同时《中华人民共和国网络安全法》在第 21 条明确规定了“国家实行网络安全等级保护制度，要求网络运营者应当按照网络安全等级保护制度要求，履行安全保护义务”；第 31 条规定“对于国家关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”。等级保护制度在今天已上升为法律，并在法律层面确立了其在网络安全领域的基础、核心地位，正如业内所言：不做等保就是违法。

开展信息安全等级保护工作是能够有效地降低政府、企业、事业单位等信息安全风险、完善信息安全防护策略的重要手段，也是落实国家关于开展信息安全等级保护工作相关规定的关键任务。

等级保护关于网络安全的相关要求如下表：（其中加深部分为三级特有要求，未加深部分为二、三级共有要求）

表 2.1 网络安全等级保护基本要求（2.0 版本）

控制点	基本要求
8.1.2.1 网络架构	c) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
	d) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；
8.1.3.1 边界防护	a) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；
	b) 应能够对非授权设备私自联到内部网络的行为进行检查或限制；
	c) 应能够对内部用户非授权联到外部网络的行为进行检查或限制；
	d) 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。
8.1.3.2 访问控制	a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
	b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
	c) 应对源地址、目的地址、源端口、目的端口和协议等进

控制点	基本要求
	行检查，以允许/拒绝数据包进出；
	d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；
	e) 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。

2.1.2 行业法规

中华人民共和国公安部印发了《公安信息通信边界接入平台安全规范（试行）》的通知，要求安全隔离设备应该具备以下安全功能：

1) 应采用三部件架构安全隔离设备。

2) 采用专用硬件和专用通信协议。

3) 协议终端、信息落地。所有过往的流量都被剥离协议，还原为应用信息。

工业和信息化部《工业控制系统信息安全防护指南》：

边界防护

第三条 通过工业防火墙、网闸等防护设备对工业控制网络安全区域之间进行逻辑隔离防护。

中石油《Q/SY1722-2014》10.3.2 中指出隔离网闸是生产网与办公网数据传输的唯一通道；

中国中煤能源集团有限公司《煤化工企业信息系统设计规范》：

6.6 生产过程控制系统宜通过 OPC 协议与实时数据库系统进行数据通信，并应采用网闸、防火墙等网络安全设备进行隔离，实现数据的单向传递。

2.2 安全需求

2.2.1 网络复杂，如何整合

面对复杂的网络承载情况，如何在保证信息安全的前提下，实现网络的互联互通，打通网络通道，数据经过安全加密传输，并最大限度保证不改动原有网络，不影响使用单位原有系统及应用。

2.2.2 安全隐患，如何规避

通过区域的数据需要采取安全防护措施，如何根据需接入的区域类型，部署对应的安全接入设备及措施，规避前端设备、传输链路、网络边界、系统应用等各环节安全风险，保证信息安全，确保数据不会发生外泄。

3 产品概况

3.1 产品定位

深信服安全隔离与信息交换系统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。

深信服安全隔离与信息交换系统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。

3.2 产品介绍

安全隔离技术首先出现于国外，最早产生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，在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。

随着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，深信服依靠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、更高性能的安全隔离与信息交换系统。

4 产品架构与性能

4.1 产品架构

深信服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。安全数据交换单元在内外网主机间按照指定的周期进行安全数据的摆渡。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即可实现内外网安全数据通信。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。

4.2 工作原理

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。安全隔离与信息交换系统隔离、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，深信服安全隔离与信息交换系统就是使用数据“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深信服安全隔离与信息交换系统与网络的内部主机系统“连接”起来，深信服安全隔离与信息交换系统将外部主机的 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，反之依然。与此类似，深信服安全隔离与信息交换系统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，即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，反之依然。即保证内、外网络不能同时连接在深信服安全隔离与信息交换系统上。深信服安全隔离与信息交换系统的原始数据“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）。

深信服安全隔离与信息交换系统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 协议都不可能穿透深信服安全隔离与信息交换系统。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，说明通过深信服安全隔离与信息交换系统的信息交换过程。

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。

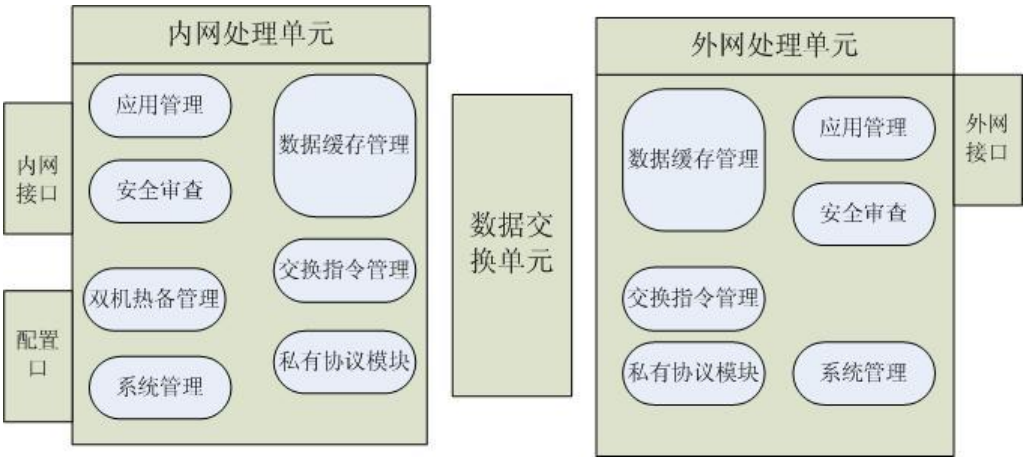

图 4.1 系统架构

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。

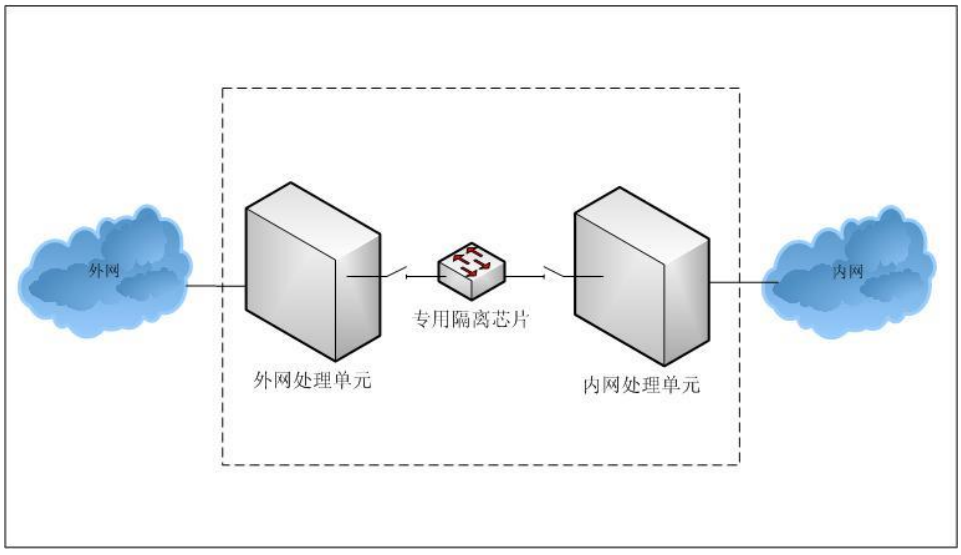

图 4.2 工作原理

一旦数据完全写入深信服安全隔离与信息交换系统的存储介质，“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 4.3 所示。

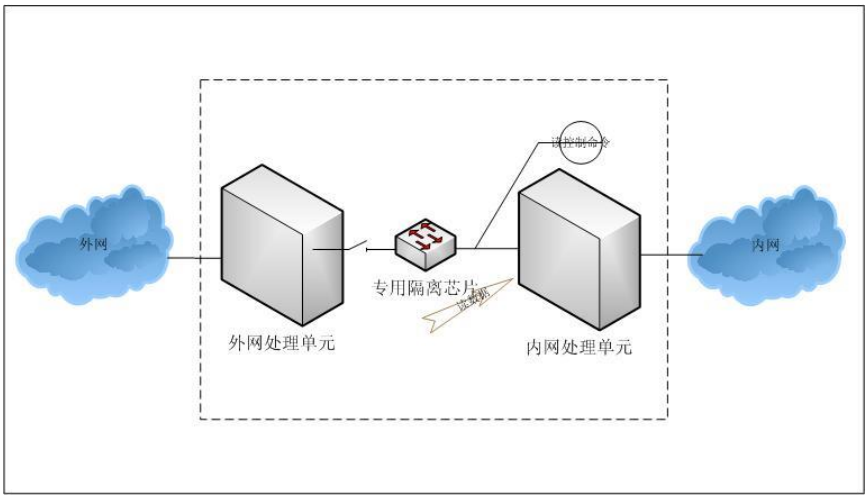

图 4.3 工作原理

深信服安全隔离与信息交换系统由内网处理单元、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的数据穿透安全传输通道的可能，确保所有通过的数据包都是只被控制单元识别的合法纯数据。

深信服安全隔离与信息交换系统的工作原理是在内、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，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。

5 产品功能与特性

5.1 产品功能

5.1.1 业务功能

5.1.1.1 安全隔离

- 物理隔离：系统由内网单元、外网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。其数据流转过程类似 U 盘在内外网处理单元之间拷贝数据；

- 协议隔离：内、外网单元主机均采用安全操作系统，分别独立完成网络协议的终止。内、外网单元之间只能通过采用非网式专有安全通道进行间歇性数据传递，内外网无法直接建立任何的协议会话，从而阻断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，不符合安全规定的数据内容将被直接删除，合法的数据才允许被安全数据交换单元交换至另一端，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，仅允许正常的、用户许可的网络应用，防范未知的安全风险。并且系统集成的防病毒功能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。

5.1.1.2 信息交换

深信服安全隔离与信息交换系统的工作原理基于人工信息交换的操作模式，即由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深信服安全隔离与信息交换系统放心地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：通过系统内部的 Web 处理模块，深信服安全隔离与信息交换系统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、原数据丢弃、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；
- 文件信息交换：通过系统内置的 FTP 应用协议处理模块，深信服安全隔离与信息交换系统能够实现内外网间的安全 FTP 数据交互，可以设定允许的

用户名、密码、动作等策略，也可以对其传输的文件类型进行过滤，摒弃不安全及泄密的因素；

- 邮件信息交换：通过内外网处理单元的 POP3、SMTP 处理模块，深信服安全隔离与信息交换系统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；

- 数据库信息交换：深信服安全隔离与信息交换系统数据库信息交换包括两部分，一为数据库信息访问交换，一为数据库信息同步。深信服安全隔离与信息交换系统同时支持这两种应用，可控制到表、字段、SQL 动作等最详细信息。目前支持的数据库种类包括 ORACLE、SQLSERVER、DB2、MYSQL、SYBASE 等几款主流数据库以及国产达梦数据库、国产人大金仓数据库等多种关系型数据库通信。通过内置的数据库处理模块，系统内能够处理穿越深信服安全隔离与信息交换系统的各种数据库操作，比如 Oracle 数据库，我们可以设置只允许 Select，不允许 Delete、Update 以及 DROP、CREATE 等操作；

- 视频信息交换：深信服安全隔离与信息交换系统支持标准的 MMS、RSTP、SIP、H323 等多种视频信息交换协议，在指定的通道中绑定视频媒体模块后，可以保证通道中传输的数据必须符合以上的媒体格式，否则丢弃；支持视频点播、回放；支持同厂家或不同厂家平台之间的国标级联；

- DCS 工控信息交换：冶金系统、电力系统、煤炭、石油、石化、化工、环保等单位的生产内网需要将生产数据及时提交到办公网络的实时数据库中，保证生产内网的绝对安全。采用深信服安全隔离与信息交换系统单向传输生产数据，采用 DCS 工控信息交换模块，使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。支持工控领域常见的 OPC/MODBUS/WINCC 等多种主流协议，并可控制相应的功能代码，例如只允许通过 MODBUS 协议读取状态信息，不能发送控制指令等；

- 组播代理：对于客户网络的组播应用做不同网络之间的代理，支持三层设备的代理穿透，支持 PIM 协议的代理，使客户组播应用无缝跨网代理；

- 特殊定制信息交换：对于用户自行研发的标准 TCP/IP 通信协议，可借助深信服提供的协议分析产品和自定义协议界面，完成用户协议的安全定制，深信服安全隔离与信息交换系统会以用户定制的命令、参数等协议解析方

式来解析用户的通信内容，从而实现在通信端口内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得多。

5.1.1.3 网络访问控制

深信服安全隔离与信息交换系统具有强大的访问控制能力，管理员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）访问自己。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：隔离系统的内、外网单元完整实现链路层、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策略；
- 访问用户控制：隔离系统的内、外网单元可实现定制、绑定哪些用户可以访问，以何种策略访问。

5.1.1.4 数据内容审查

内容检查是指当深信服安全隔离与信息交换系统准备交换文件之前对文件所进行的安全检查，确保只有符合保密、安全策略的数据、文件才允许被交换至另一端。

- 行为动作：隔离系统的内、外网单元可依据管理员设定的各个应用模块的行为动作策略进行控制，拒绝非允许的动作操作：如针对 FTP 协议，允许下载不允许上传；针对数据库访问，允许 SELECT 不允许 DELETE 等操作，并记录非授权动作到日志告警；
- 关键字检查：隔离系统的内、外网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：隔离系统的内、外网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。

5.1.1.5 缓存空间及传输数据的管理

深信服安全隔离与信息交换系统的内、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，提升文件访问效率。

5.1.1.6 双重安全防护机制

深信服安全隔离与信息交换系统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，并且只有被允许客户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，否则将被视为无效数据，直接删除并丢弃。同时，深信服安全隔离与信息交换系统内嵌防病毒和入侵检测引擎，能够实时检测、阻绝已知的各种病毒与入侵，并在控制台告警，帮助管理员在最短时间内做出响应。深信服安全隔离与信息交换系统提供开放、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）无缝连接和集成。

5.1.2 管理功能

5.1.2.1 安全的管理通信

深信服安全隔离与信息交换系统只允许从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。管理者与深信服安全隔离与信息交换系统采用加密的 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。

5.1.2.2 权限分配方式

深信服安全隔离与信息交换系统采取系统策略配置管理员、安全管理员与日志管理员三种角色分立的权限分配模式。用户只能维护和操作所属基础管理角色的功能与操作，权限各不交叉。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。

5.1.2.3 策略定制功能

深信服安全隔离与信息交换系统采用面向用户的策略定制方式，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应用环境的交换策略。此外，系统内置的初始策略更是方便了新用户的使用。

5.1.2.4 日志审计功能

深信服安全隔离与信息交换系统提供强大的日志和审计功能，日志默认存储在设备中。并且支持通过标准 SYSLOG 的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，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。

5.1.3 高可用性功能

5.1.3.1 负载均衡

深信服安全隔离与信息交换系统支持负载均衡功能。多套隔离系统可通过组成集群，以提供更高的性能。深信服安全隔离与信息交换系统提供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。

5.1.3.2 双机热备

深信服安全隔离与信息交换系统提供双机热备和多机热备功能。两台安全深信服安全隔离与信息交换系统可组成热备机组，机组内设备有主设备与备用设备之分。从设备向主设备发起状态检测请求，并获取最新的访问策略。当主设备发生故障，从设备启动并自动变为主设备，同时以声音与告警信息示警，如下图所示：

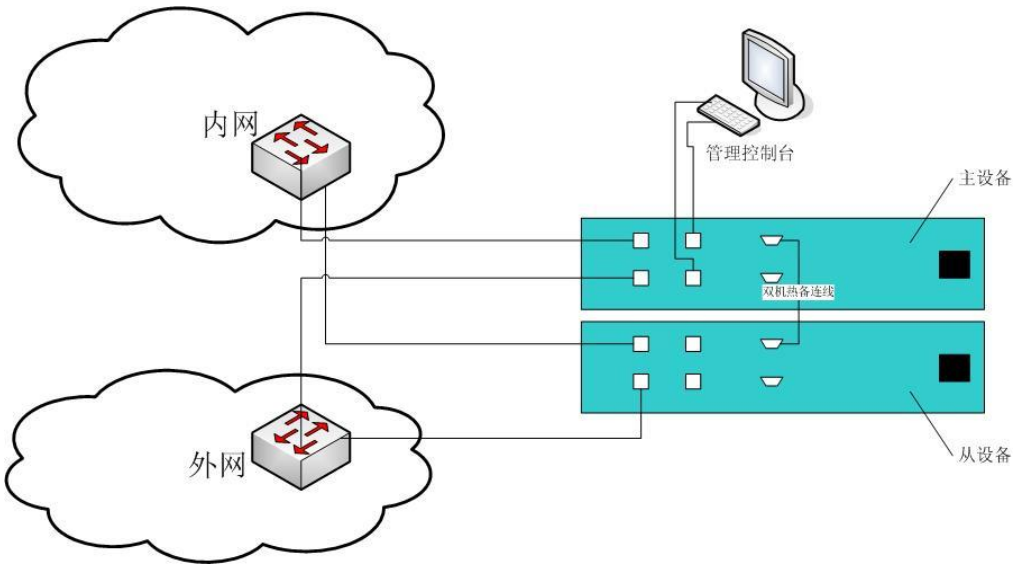

图 5.1 双机热备拓扑图

5.2 产品特性

5.2.1 高安全性

深信服安全隔离与信息交换系统采用专有的安全操作系统，只保留深信服安全隔离与信息交换系统必须的专用功能。安全 OS 存贮于 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过滤引擎，可防止 DoS 和 DDoS、缓冲区溢出、恶意编码、应用层洪水等攻击。

深信服安全隔离与信息交换系统采用专用的安全通道进行内外网信息交换，业务数据通过物理隔离、协议隔离、内容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。深信服安全隔离与信息交换系统采用双重安全防护机制，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、入侵检测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。

5.2.2 高吞吐率

深信服安全隔离与信息交换系统的内、外网处理单元采用复杂对称多处理（RSMP）技术，在一台深信服安全隔离与信息交换系统内集成多个处理模块，成倍提升处理能力，使深信服安全隔离与信息交换系统具有很高的性能。

5.2.3 高可靠性

深信服安全隔离与信息交换系统设备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，使深信服安全隔离与信息交换系统可在超重负荷的环境下长期稳定运行。双机热备的部署方式可使系统抵抗灾难性损坏时的可靠性成倍提高。

5.2.4 高便利性

深信服安全隔离与信息交换系统为方便管理员使用，在出厂设置已提供了一套适合多数网络环境的常用安全策略，管理员用户只需要将设备对应的 IP 地址修改为实际网络中分配的 IP 地址即可。日志用户与策略配置用户的权限分立以及层次化的权限划分允许用户可将各类管理工作交由不同的用户来完成，真正与管理需求相吻合。管理用户、访问用户以及众多的日志审计记录均实现可导入导出操作，大大加强了深信服安全隔离与信息交换系统的便利性与可操作性。

深信服安全隔离与信息交换系统支持多种工作模式，极大地适应了用户的各种网络环境变化要求。

6 产品优势与价值

6.1 产品优势

深信服提供了业界领先的安全隔离解决方案，其主要优势在于：

6.1.1 简便易用的界面风格

系统通过 HTTPS 方式提供系统工作监控工作台、配置向导、配置提示等方式，为用户提供了简单易用的界面，即使是初次使用系统，也完全能在较短的时间内掌握。

6.1.2 强大的业务功能

除标准的业务代理功能之外，深信服产品还兼具如下与业务场景深度相关的功能：

- 数据库同步与文件同步
- 视频平台级联与点播
- 视频负载均衡
- OPC/MODBUS/DNP3/IEC104 等工业控制协议的识别与深度控制
- 支持多种形态的组播代理

6.1.3 通信协议深度控制

系统支持的所有代理业务中，除不可识别的应用协议之外，均可控制到应用协议的信令、参数的深度，可制作应用协议、命令的白名单。

6.1.4 多任务高并发性能

系统代理采用类 nginx 引擎，可支持多任务、高并发、大流量业务通信，同时系统支持负载均衡方式部署，解决更高业务性能需求的场景。

6.1.5 优秀的环境适应

产品支持普通代理、透明代理、路由代理三种工作模式，可适应用户的各种网络环境变化要求。

6.2 产品价值

采用深信服安全隔离与信息交换系统做不同安全域间的数据交换，通过对业务的代理、数据的检查与摆渡，实现域间数据安全、可控地交换。

1) 实现不同的隔离网络间的数据交换；

2) 不同的业务系统无需二次开发即可实现系统间数据库、文件的同步；

3) 不同安全域间的视频平台可实现平台级联；

4) 隔离网络间业务访问，代理后对业务透明；

5) 业务访问流程全程记录；

6) 符合国家相关网络安全政策要求。

7 产品应用场景

7.1 安全隔离与视频交换解决方案

7.1.1 场景需求

近年来，公安以及各大企业事业单位均建设了不同规模的视频监控系统。为了最大化地利用这些视频监控资源为公安或企业集团使用，来实现“资源共享、互联互控”和“视频监管一网控”，各个城市已经开始将各个分散的视频监控系统级联接入到一个或多个监控平台中。

出于安全考虑，不同单位的视频监控系统间互联大多采用传统的网络安全防护手段，如部署防火墙和 IPS 设备。但由于防火墙和 IPS 等设备不能有效地解决跨网络平台的级联问题，同时仅能防护到网络传输层，对于视频传输协议无法做到识别和控制，存在应用会话被挟持的风险。2016 年 10 月 21 日，因摄像头被入侵劫持，导致美国东海岸发生了大面积互联网断网事件。

作为网络安全隔离防护解决方案领航者，经过十多年的潜心研究和大量的客户案例部署实践，深信服研制了一套安全隔离与信息交换系统。深信服安全隔离与信息交换系统既能实现不同视频系统的网络隔离和协议控制，又能做到视频平台的级联、点播等业务的流畅不卡顿。

7.1.2 解决方案

在公安网与社会视频网互联中，在社会视频监控网络与公安视频专网之间、公安视频专网与公安信息专网之间，推荐部署深信服安全隔离与信息交换系统，实现视频平台的安全级联。

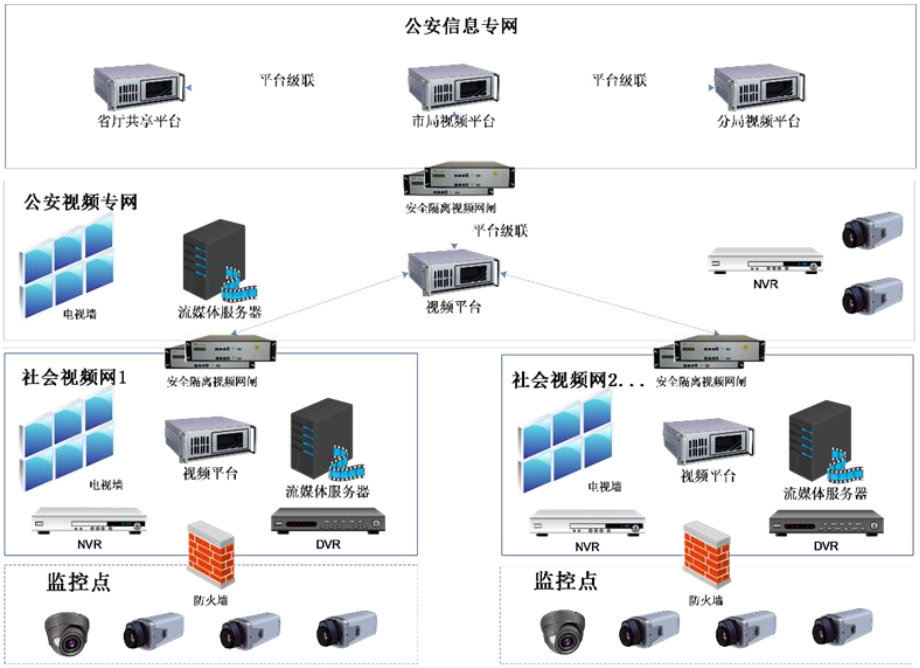

图 7.1 拓扑图

社会视频监控网络、公安视频专网、公安信息专网安全级联后，在公安信息专网就可以安全地实时浏览、回放下级社会视频监控和公安视频专网的监控画面，无需存储在本地。这样既解决了公安机关视频监控资源不足的问题，提升了社会视频监控拥有单位和全社会的治安水平，又阻断了黑客通过社会视频网入侵公安网络，也避免了公安网违规外联和一机两用违规行为的发生，是一举多得的举措。

7.2 安全隔离与数据库同步解决方案

7.2.1 场景需求

随着党和政府积极推进“互联网+政务”工程建设，为了实现“让数据多跑路，让群众少跑腿”的目标，需要实现各部门数据共享、协同办公，进而提高政府办公效率。

数据共享最简单的方式就是，数据需求方能够直接读取到提供方的数据库数据表，但是将数据库接口直接暴露在外面是极度不安全的行为。

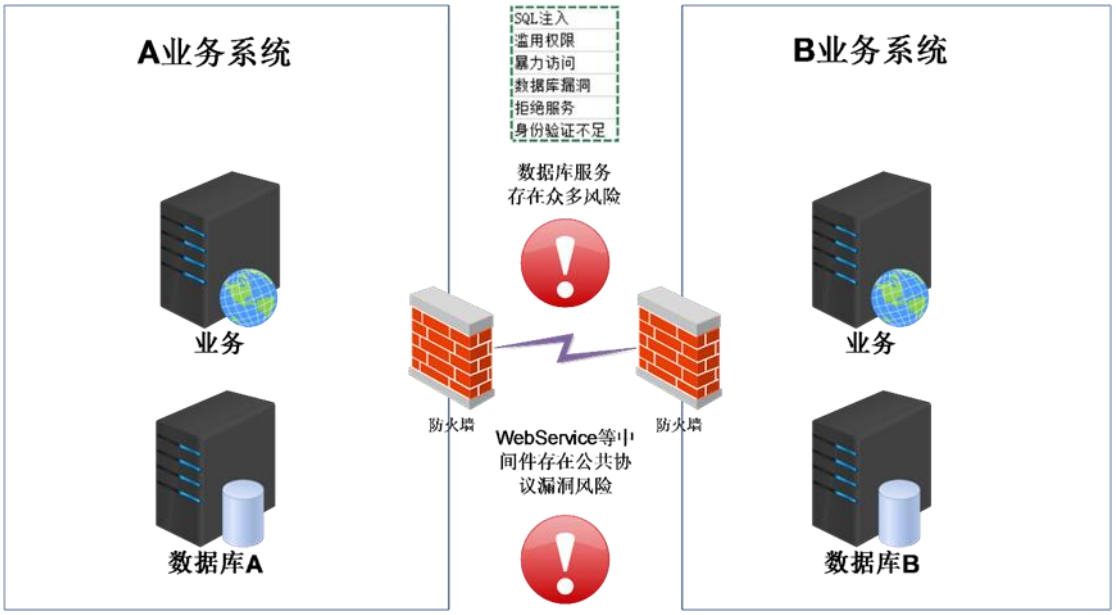

图 7.2 拓扑图

- 传统安全防护手段不足

采用基于传统访问控制技术的防火墙、入侵防御、数据库防火墙等安全设备均无法解决数据被篡改、删除等安全隐患，无法打消安全顾虑。

- 业务中间件开发难度大

由于不同业务系统可能采用不同的数据库，数据库表结构也可能不同，业务系统对接开发时，多方同步信息需要高投入。

深信服作为网络安全隔离解决方案领航者，基于物理隔离技术，总结了一套安全隔离与数据库同步解决方案。通过深信服安全隔离与信息交换系统的数据库同步功能模块，来“摆渡”完成不同业务数据库之间的指定数据的同步，从而实现对外接业务网的隔离防护，并满足等级保护管理要求。

7.2.2 解决方案

深信服安全隔离与信息交换系统采用“2+1”的系统架构，即由内、外网两个主机系统与数据交换单元（专用隔离芯片）三部分硬件架构，采用类似于船闸摆渡的工作原理，实现不同网络间的数据交换。

基于数据库触发器机制，当一侧数据库检测到有业务系统执行了插入、修改、删除数据时，数据库同步模块触发器会主动记录下执行的指令数据，并在另一侧数据库中同步执行相同的指令数据，实现两个网络间数据库数据被动“摆渡”同步。

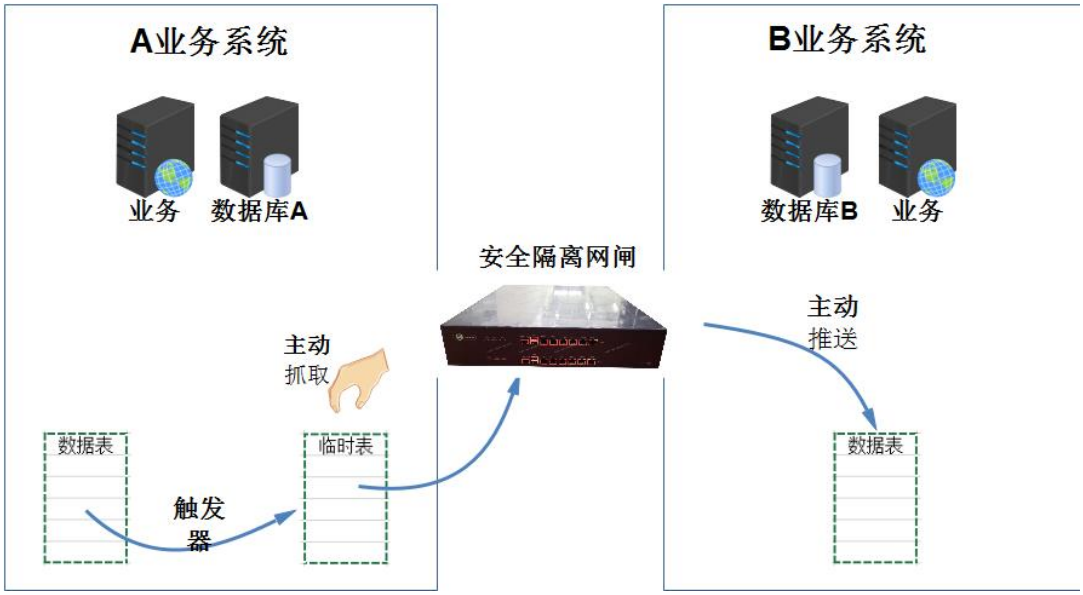

图 7.3 拓扑图

7.2.3 实现效果

- 业务软件无需再开发

启用深信服安全隔离与信息交换系统的数据库同步功能后，各业务相关方在业务对接开发过程中，开发者只需各自表达需要或能提供什么数据即可，数据同步交互交由深信服完成。

- 数据库类型覆盖全面

国外数据库：支持 Oracle、Sqlserver、Mysql、DB2、Sybase、Postgresql 等各个版本。

国产数据库：支持武汉达梦(DM)、人大金仓(Kingbase)等各个版本。

- 主动同步异构数据库

可主动实现同类型、同结构数据库之间同步，也可主动实现不同类型、不同结构数据库之间同步。

- 细粒度数据同步控制

数据同步可具体设置到字段级别。

支持 CLOB/BLOB 大字段类型字段的同步及字符集转化。

- 安全高效的数据同步

安全深信服安全隔离与信息交换系统主动发起或同步客户端软件两种形式可灵活选择。

可设置数据的单向同步与双向同步。

同步客户端软件同步形式的实现基于私有协议的加密传输。