



SANGFOR
深信服科技

深信服安全隔离与信息单向导入系统 光闸 FGAP-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

深信服科技股份有限公司版权所有，并保留对本文档及本声明的最终解释权和修改权。

本文档中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明外，其著作权或其它相关权利均属于深信服科技股份有限公司。未经深信服科技股份有限公司书面同意，任何人不得以任何方式或形式对本文档内的任何部分进行复制、摘录、备份、修改、传播、翻译成其他语言、将其全部或部分用于商业用途。

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	1
2	需求背景	1
2.1	法规标准要求	1
2.1.1	等级保护	1
2.1.2	行业法规	3
2.2	安全需求	3
2.2.1	网络复杂，如何整合	3
2.2.2	安全隐患，如何规避	3
2.2.3	涉密信息，如何传输	3
3	产品概况	4
3.1	产品定位	4
3.2	产品介绍	4
4	产品架构与性能	4
4.1	产品架构	4
4.2	工作原理	5
5	产品功能与特性	6
5.1	产品功能	6
5.1.1	业务功能	6
5.1.2	管理功能	9
5.1.3	高可用性功能	10
5.2	产品特性	11
5.2.1	高安全性	11
5.2.2	高吞吐率	11
5.2.3	高可靠性	11
5.2.4	高便利性	12
6	产品优势与价值	12
6.1	产品优势	12

6.1.1 简便易用的界面风格	12
6.1.2 强大的业务功能	12
6.1.3 高稳定性	12
6.1.4 良好的环境适应	13
6.2 产品价值	13
7 产品应用场景	13
7.1 文件单向安全上传场景	13
7.1.1 场景需求	13
7.1.2 解决方案	13
7.1.3 实现效果	14
7.2 法院信息系统勒索病毒防护场景	15
7.2.1 场景需求	15
7.2.2 解决方案	15
7.2.3 实现效果	16

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仍可由软件控制。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

最高人民法院《关于开展全国法院办公专网信息安全专项整治工作的通知》（法[2018]295号）要求，法院办公专网与移动专网、外部专网、互联网进行数据交换须使用单向光导技术产品进行隔离，加强专网整体安全建设。

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。

2.2.3 涉密信息，如何传输

涉密网络绝对不允许与非涉密网络进行互联，但由于业务应用的需求，部分涉密信息系统需要实时地收集外部文件，传统人工刻盘的光盘摆渡机方式已经无法满足数据收集实时性要求，需要在技术上有突破。

3 产品概况

3.1 产品定位

深信服安全隔离与信息单向导入系统主要用于各地电子政务、军队、军工的信息化建设，下列场合都可使用深信服安全隔离与信息单向导入系统保障业务系统安全：

- 由政务外网向政务内网报送数据；
- 行业内下级向上级报送数据；
- 低密网向高密网传输数据；
- 低安全域向高安全域传输数据；
- 工业生产网向 MES 网/办公网传输数据。

深信服安全隔离与信息单向导入系统的应用场合包括但不限于以上几种。

3.2 产品介绍

深信服科技股份有限公司在经过大量论证之后认为光纤传输在实现单向控制和高效性、稳定性以及经济性方面可以满足单向隔离的要求。众所周知，光的传播是有方向性的，光纤传输是利用了发光端为源、感光端为目的来传输信息的。双向数据交互是采用两条光纤，一条光纤发送数据，一条光纤接收数据。当然也可以采用一条光纤双向传输，但是这是由光纤两端的收发器或光模块决定的。传统的 SFP 光模块中，发光器和收光器是分离的，因此深信服决定采用 SFP 光模块实现单向的传输。即光模块发光端接光纤的发送端，另一主机的光模块的收光端接光纤的接收端，这样的传输原理从物理上可解决数据流向的单向性问题。

深信服安全隔离与信息单向导入系统就是在采用单向传输部件的基础上，结合传统安全隔离技术的“摆渡+代理”技术，在保障信息单向传输的同时，最大限度地实现信息的实时传输和可控。

4 产品架构与性能

4.1 产品架构

深信服安全隔离与信息单向导入系统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。深信服安全隔离与信息单向导入系统

由内、外网处理单元和单向传输单元组成。单向传输单元在内、外网主机间按照指定的周期进行安全数据的摆渡。

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。深信服安全隔离与信息单向导入系统既然隔离、阻断了网络的所有连接，实际上就是隔离、阻断了会话的连通。深信服安全隔离与信息单向导入系统借鉴传统光闸技术，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单向导入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单向导入系统将外部主机的 TCP/IP 协议全部剥离，将原始数据通过存储介质，以单向发送的方式导入到内部主机系统，内部主机系统再将相应的信息发送至真正的使用者或在本地实现备份。

深信服安全隔离与信息单向导入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。下面以信息流由外网到内网为例，说明通过深信服安全隔离与信息单向导入系统的信息传输过程。

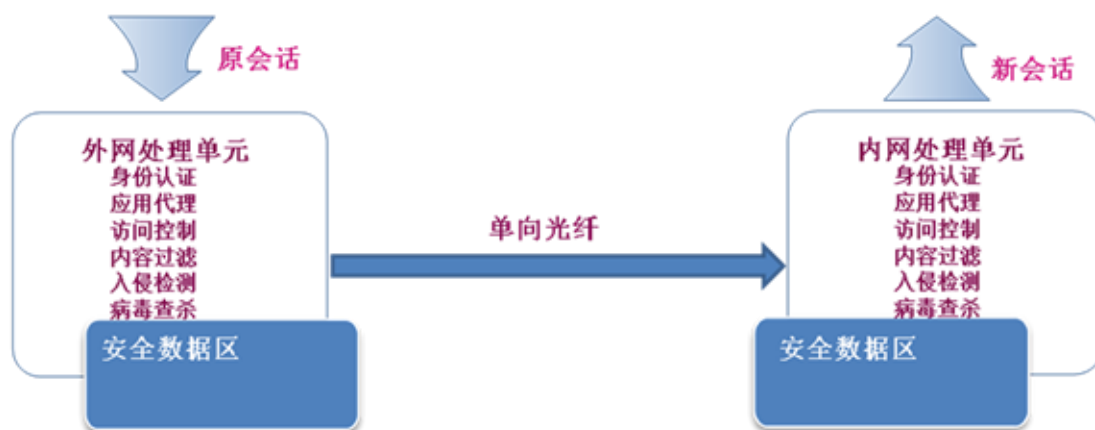


图 4.1 工作原理

深信服安全隔离与信息单向导入系统由内网处理单元、外网处理单元与单向传输单元（单向光纤通道）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。单向传输单元采用专用安全传输控制硬件加 SFP 光模块，通过层层搬运的方式实现信息的单向安全传输。

深信服安全隔离与信息单向导入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传输。单向传输单元按照设定的周期由外网处理单元的安全数据交换区将数据内容提取并单向传输至内网处理单元的安全数据下载区，等待用户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

- 物理单向：系统由内网单元、外网单元及单向传输单元三个物理部分组成。单向传输单元的物理单向由单向光纤实现；
- 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：系统采用应用解码，客户应用可经过模块编码验证，只有符合白名单的编码规则的数据才可被传输至内网单元；
- 内容隔离：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，仅许可正常的、用户许可的网络应用，防范未知的安全风险。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。

5.1.1.2 信息交换

深信服安全隔离与信息单向导入系统的工作原理基于人工信息交换的操作模式，即由外网处理单元接收来自客户端的发送数据请求，内网处理单元负责接收来自外网处理单元的信息，并将信息提交至目标服务器。由于单向传输单元的物理单向性，两个处理单元之间没有交互式会话，无法实现发送数据的校验。在此前提下，通过专有硬件实现网络间信息的实时单向传输可能会造成部分数据的丢

失。深信服安全隔离与信息单向导入系统采用独特的冗余数据算法，最大限度地保证了数据的完整性。

- **TCP 应用层：**通过系统内部的 TCP 代理处理模块，深信服安全隔离与信息单向导入系统能够实现代理外网客户端发送的 TCP 会话，并对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进行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；
- **UDP 应用层：**通过系统内部的 UDP 代理处理模块，深信服安全隔离与信息单向导入系统能够实现代理外网客户端发送的 UDP 会话，并对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进行日志报警。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；
- **主动文件信息交换：**通过系统内置的 FTP 文件客户端模块，深信服安全隔离与信息单向导入系统能够实现主动到外网 FTP 服务器抓取文件并向内网的 FTP 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；
- **被动文件信息交换：**通过系统内置的专用文件传输模块，深信服安全隔离与信息单向导入系统能够实现外网向内网的私有文件的安全、单向的传输。客户机通过管理控制台分配的账号，使用专用的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 邮件代理引擎，实现外网邮件服务器将邮件转发至深信服安全隔离与信息单向导入系统的外网处理单元，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，深信服安全隔离与信息单向导入系统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、武汉达梦等国产数据库的同步。支持异构数据库之间的同步，支持按条件过滤的同步；

- 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：深信服安全隔离与信息单向导入系统支持与深信服安全隔离与信息交换系统进行联动，实现在深信服安全隔离与信息交换系统传输双向信令，在深信服安全隔离与信息单向导入系统中传输单向视频流；
- 双单向联动：支持两台深信服安全隔离与信息单向导入系统组成一个双向应用的代理环路，在两条单向链路上实现业务双向服务。

5.1.1.3 网络访问控制

深信服安全隔离与信息单向导入系统具有强大的访问控制力，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）访问系统。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：深信服安全隔离与信息单向导入系统的内、外网单元可分别实现链路层、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：深信服安全隔离与信息单向导入系统的内、外网单元可分别实现定制、绑定哪些用户可以访问系统。

5.1.1.4 数据内容审查

内容检查是指深信服安全隔离与信息单向导入系统外网处理单元对接收到的文件和信息进行安全性检查，确保只有符合保密、安全策略的数据、文件才允许被单向传输至内网端。

- 白名单规则：数据流代理应用规范可由管理员设定，只有符合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：深信服安全隔离与信息单向导入系统的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摒弃并记录日志告警；

- 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；
- 病毒检查：深信服安全隔离与信息单向导入系统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。

5.1.1.5 文件校验二次传输

由于深信服安全隔离与信息单向导入系统的单向传输特性，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。因此系统提供了传输记录的校验功能，管理员可根据一段时间导出接收记录，并在外网处理单元导入记录进行校验，当发现丢失的文件或错误的文件后，系统提供重传功能，最大限度地保证数据的完整性。

5.1.1.6 缓存空间及传输数据的管理

深信服安全隔离与信息单向导入系统的内、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，保持文件访问效率。

5.1.1.7 双重安全防护机制

深信服安全隔离与信息单向导入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，并且只有被允许的客户的网络数据或文件才被传输，因此深信服安全隔离与信息单向导入系统就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单向导入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，并在控制台示警，帮助管理员在最短时间内做出响应。

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单向导入系统只允许从专用的管理控制端口进行管理，管理员可设置允许管理设备的地址。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。

5.1.2.2 权限分配方式

深信服安全隔离与信息单向导入系统采取系统策略配置管理员与日志管理员角色分立的权限分配模式，用户只能维护操作本类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单向导入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。并且系统提供了强大的帮助系统，它详细地介绍了深信服安全隔离与信息单向导入系统的安装、使用的各个步骤并举例说明。

5.1.2.4 日志审计功能

深信服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，深信服安全隔离与信息单向导入系统设备内置日志存储空间。支持标准 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。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。

5.1.3 高可用性功能

深信服安全隔离与信息单向导入系统提供双机热备乃至多机热备功能。两台安全设备可组成热备机组，机组内设备有主设备与备用设备之分，两台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：

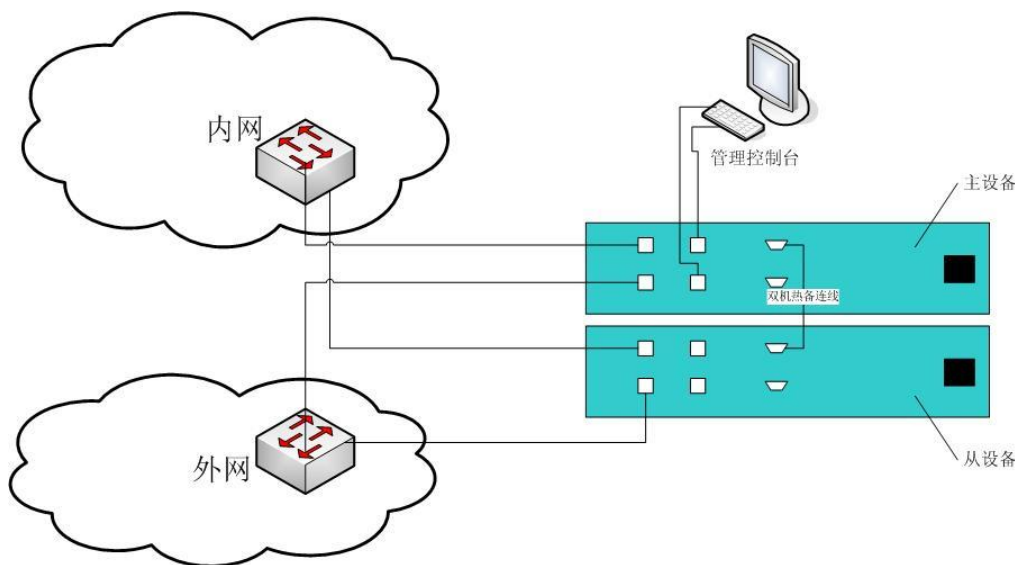


图 5.1 双机热备拓扑图

5.2 产品特性

5.2.1 高安全性

深信服安全隔离与信息单向导入系统采用专有的安全操作系统。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、应用层洪泛等攻击。

深信服安全隔离与信息单向导入系统采用专用的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。深信服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新型安全隐患,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单向导入系统的内、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单向导入系统内集成多个处理模块,成倍提升处理能力,使安全隔离与信息单向导入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单向导入系统的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单向导入系统

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单向导入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。管理用户及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单向导入系统的便利性与可操作性。

6 产品优势与价值

6.1 产品优势

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 TCP/UDP 单向业务代理功能之外，深信服安全隔离与信息单向导入系统产品还兼具如下与业务场景深度相关的功能：

- 数据库单向同步与文件单向同步
- 光网联动
- 邮件中继代理
- 双单向 TCP 代理
- 支持多种形态的组播代理
- 文件传输既支持主动抓取推送，又支持被动接收代理

6.1.3 高稳定性

系统在适配不同的文件大小以及数据吞吐量时，自动采取不同的系统调节参数，以在系统性能与稳定性间平衡运行，保证在系统稳定的基础上发挥出最高的性能。

6.1.4 良好的环境适应

系统的文件传输以及数据库同步等模块均可采用内置或外置的方式进行部署，同时外置的数据库同步和文件同步均支持 WINDOWS/LINUX 等主流操作系统。

6.2 产品价值

采用深信服安全隔离与信息单向导入系统做不同安全域间的数据单向传输，通过对文件、数据、业务流量的检查与摆渡，实现域间数据安全、单向的传输。

- 1) 实现外网端向内网端单向传输文件；
- 2) 实现外网端向内外端单向同步数据库；
- 3) 内网不能向外网传输任何数据；
- 4) 符合国家相关网络安全政策要求。

7 产品应用场景

7.1 文件单向安全上传场景

7.1.1 场景需求

深信服安全隔离与信息单向导入系统主要用于各地电子政务、军队、军工的信息化建设，下列环境都可使用深信服安全隔离与信息单向导入系统保证业务系统安全：

- 由政务外网向政务内网报送数据
- 行业内下级向上级报送数据
- 低密级网向高密级网传输数据
- 低安全域向高安全域传输数据
- 工业生产网向 MES 网/办公网传输数据

7.1.2 解决方案

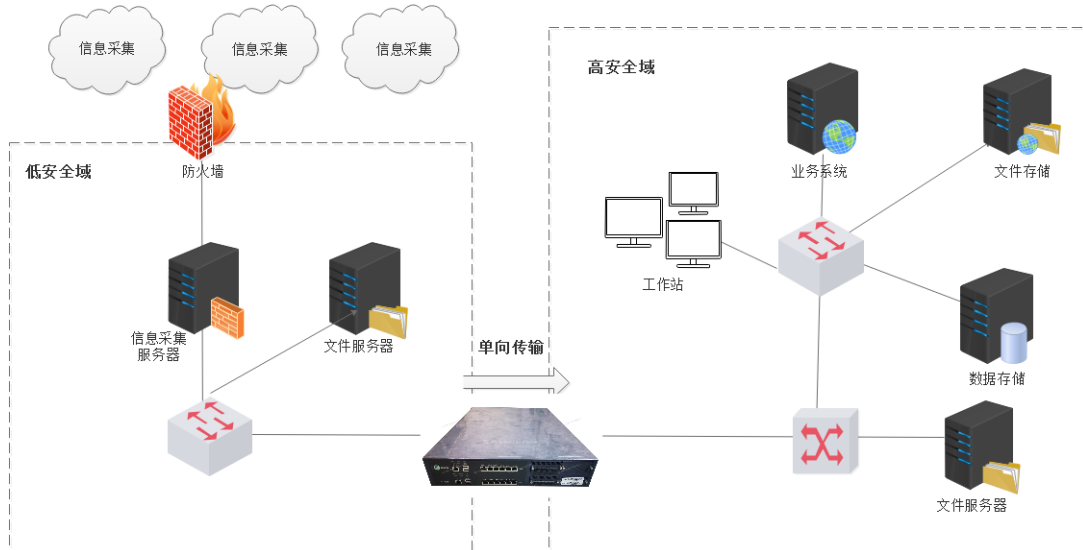


图 7.1 拓扑图

7.1.3 实现效果

- 冗余算法保证完整性

鉴于深信服安全隔离与信息单向导入系统的单向传输特点，接收单元无任何反馈信息，深信服安全隔离与信息单向导入系统采用了专有冗余算法，实现即使在出现少量丢包时，仍能保证文件的完整性。

- 传输文件安全可控

基于用户账户验证机制，只有合法用户文件才能被上传。同时，目录空间有私有区和公共区之分，满足了文件传输的自由度要求。

- 多样化的日志管理

深信服安全隔离与信息单向导入系统详细记录了系统日志、管理日志、通信日志、安全性阻断日志、内容检查日志等日志信息。

- 设备健康状况自检

具备健康状况自查功能，出现故障时会通过显示输出、声音、日志等方式进行告警。

- 良好的环境适应性

无论主动传输还是被动传输，均兼容 Windows/Linux/Unix 等多种平台。

7.2 法院信息系统勒索病毒防护场景

7.2.1 场景需求

随着在线庭审直播、在线案件受理平台等法院对外在线业务的开展，业务专网需要与互联网或其他相关业务单位之间交换数据。在网络边界部署安全产品不当，就会造成法院业务专网边界完整性的破坏。当业务专网与这些非信任网络之间交换数据时就可能引入各种安全风险，其中包括令人谈其色变的勒索病毒。勒索病毒对业务系统的破坏巨大，一旦中了勒索病毒，对业务系统以及数据都会造成巨大的破坏。

7.2.2 解决方案

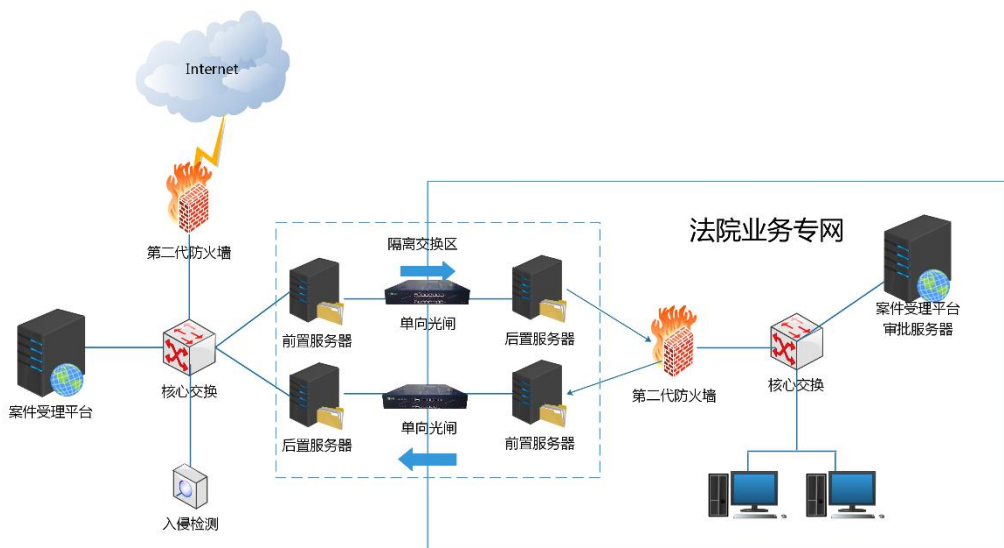


图 7.2 拓扑图

根据勒索病毒的特点，除通过网络设备简单关闭端口外（445、135、137、139、3389 等），在内外网数据交换时，也需要采取网络协议终止、内容检查与日志审计，确保网络请求无法穿透系统进入法院业务专网，从而阻止勒索病毒等蠕虫病毒传播到法院业务专网。

推荐法院业务专网与其他网络边界使用深信服安全隔离与信息单向导入系统产品进行隔离交换。

深信服安全隔离与信息单向导入系统利用光信号的单向性特点，实现数据的绝对单向传输，防止了所有穿透性业务请求，只单向摆渡明确允许的信息，切断了所有依赖网络传播的已知和未知风险。对于需要双向交换的数据，深信服安全

隔离与信息单向导入系统提供了由两个独立单向光闸组成双向数据交换通道的方案，比防火墙、传统双向网闸的方案更安全。

7.2.3 实现效果

- 屏蔽现有的勒索病毒及勒索病毒变种法传播到法院内网；
- 满足最高法（FYB/T53001-2017）单向传输要求。