GLA 玉衡内外网数据交换平台
技术白皮书

西藏国路安科技股份有限公司

1 背景

1.1 公司介绍

西藏国路安科技股份有限公司（以下简称国路安科技）成立于 2009 年，是一家专业面向应用安全领域，提供产品研发、一体化解决方案和咨询服务的高新技术企业。短短几年间，公司发展迅速，2015 年 8 月国路安在新三板市场成功挂牌上市，股票代码 833237。目前已为政府、金融、交通、税务、林业、教育等行业用户提供了信息安全保障和高效可控的信息服务。现业务涵盖信息安全、超融合云计算、数据资产、大数据智能应用、云服务总线、智慧城市等领域，正在形成“两个中心，七大区域平台，多行业纵深发展”的全国性战略布局。

国路安科技公司现有过百名员工，拥有技术型专利 7 项，软件著作权 39 项。围绕行业用户的实际需求形成以细粒度应用标记、强制访问控制、高性能深度协议解析、资产属性模型等核心技术，自主研发多款信息安全产品并提炼成为行业用户拥趸的解决方案。

近年来在资本+技术融合发展的战略进程中，国路安科技与航天科工、神州数码、中电科等合作方一起，联手进军智慧城市、物联网大数据等省市级平台建设。以某票务平台支付系统为例，2011 年正式上线试运行以来，国路安的安全技术和持续服务已保障累计数十亿的交易记录和万亿级的票务资金安全。国路安科技始终秉承利他之心的企业价值观，以精益求精的态度不断创新产品技术，为和谐共赢的社会贡献企业价值。

1.2 信息安全隔离交换技术的发展过程

安全隔离技术是指在需要信息交换的情况下，实现网络隔离的信息安全的软硬件技术。随着电子政务建设安全隔离需求的发展，我国的隔离技术这几年来发展迅速，走过了以下历程：

第一代隔离技术——完全的隔离。此方法使得网络处于信息孤岛状态，做到了完全的物理隔离，需要至少两套网络和系统，更重要的是信息交流的不便和成本的提高，这样给维护和使用带来了极大的不便。

第二代隔离技术——硬件卡隔离。在客户端增加一块硬件卡，客户端硬盘或其他存储设备首先连接到该卡，然后再转接到主板上，通过该卡能控制客户端硬盘或其他存储设备。而在选择不同的硬盘时，同时选择了该卡上不同的网络接口，连接到不同的网络。但是，这种隔离产品有的仍然需要网络布线为双网线结构，产品存在着较大的安全隐患。

第三代隔离技术—数据转播隔离。利用转播系统分时复制文件的途径来实现隔离，切换时间非常之久，甚至需要手工完成，不仅明显地减缓了访问速度，更不支持常见的网络应用，失去了网络存在的意义。

第四代隔离技术—空气开关隔离。它是通过使用单刀双掷开关，使得内外部网络分时访问临时缓存器来完成数据交换的，但在安全和性能上存在有许多问题。

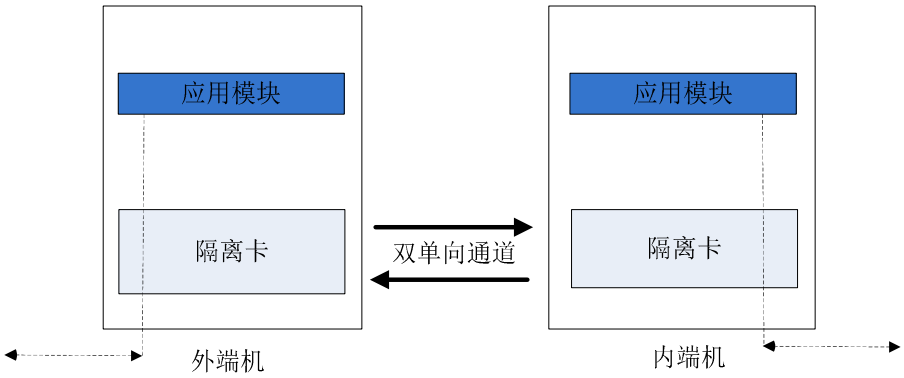
第五代隔离技术—安全通道隔离。此技术通过专用通信硬件和专有安全协议等安全机制，来实现内外部网络的隔离和数据交换，不仅解决了以前隔离技术存在的问题，并有效地把内外部网络隔离开来，而且高效地实现了内外网数据的安全交换，透明支持多种网络应用，成为当前隔离技术的发展方向。

2 产品概述

2.1 产品概述

内外网数据交换平台实现两个完全隔离的不同安全区域的数据交换，同时要保证交换过程中的信息安全。一方面，随着信息建设的发展，不同安全区域之间交换的数据量越来越大，并且呈现成倍增长的趋势，这就要求内外网隔离交换产品具备高性能的数据交换速率和极高的可靠性。另一方面，在数据交换过程中，必须对信息进行落地，进行一系列的安全性检查，确保交换的数据完整、安全、可靠。为满足以上需要，GLA 内外网数据交换平台的整体技术

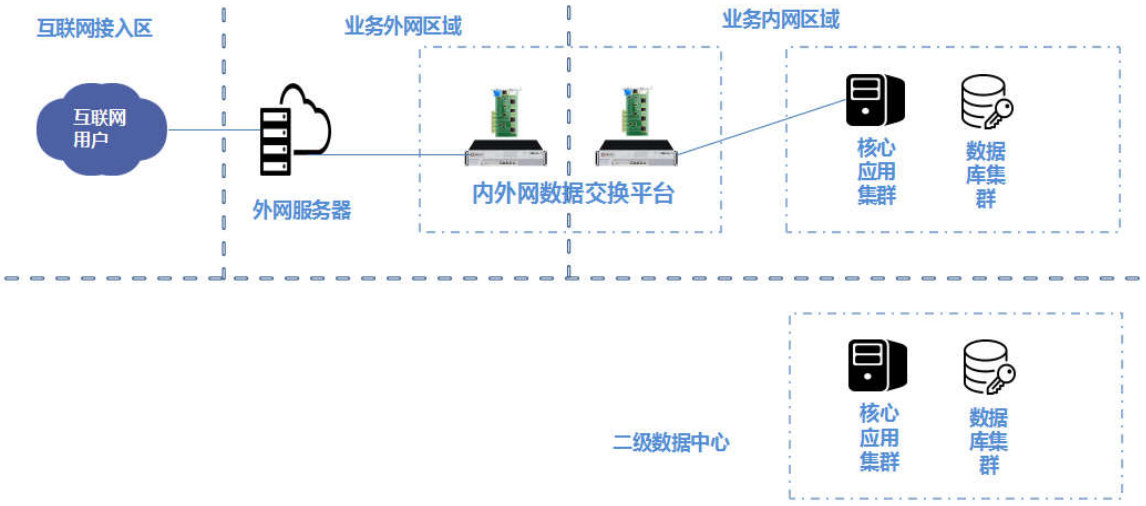
架构如下所示：



双单向隔离卡系统由外端系统隔离卡，内端系统隔离卡和应用模块三个部分构成。其中外端系统与内端系统面向不同的安全域。内外端系统的应用模块提供上层映射代理服务功能。内外端机之间采用安全双单向隔离卡连接，每一块隔离卡上均由一个单项发送的光通信模块，两块隔离卡之间的光发射模块与对端非光发射模块连接，形成隔离卡之间的双单向通信通道。

2.2 产品硬件及部署模式

GLA 内外数据交换系统的典型部署场景如下：



内外网数据交换平台部署在网络区域的边界处，对不同网络区域实现物理上的隔离，不同网络之间不能随意联通传输数据，只能通过内外网交换平台提供的特定通道进行数据交换。根据不同的网络情况，可以分成几种不同的部署场景：

2.2.1 两个数据中心之间的数据隔离交换

例如，某部委业务机构在不同的省份均有自己的数据中心，该数据中心汇总全省各地市的基础数据，并且要上报给国家级的统一机构中。此场景下，省级数据中心和国级数据中心构成两个不同的安全中心。此时，可应用内外网数据交换平台对这两个中心的数据进行隔离和安全数据交换。

2.2.2 不同机构的数据中心之间的数据隔离交换

例如，A 部委和 B 部委都建设有自己的数据中心，并且是互相独立的。随着信息融合的发展，业务需要要求 A 部委访问使用 B 部委的一些数据，此时 AB 之间形成不同的网络安全区域，他们之间的数据交换就需要构成安全可靠的隔离交换。此时，可应用内外网数据交换平台对这两个中心的数据进行隔离和安全数据交换。

3 产品功能介绍

内外网数据交换系统具体的功能如下：

网间安全隔离：内外网数据交换系统采用多机系统结构，以软硬件结合的方式，有效地隔断内外网络间逻辑上的的连接，保障信息可信的交换。

协议中断，信息落地：内外网数据交换系统的内/外端机是内/外网络各自通用协议（即 TCP/IP 协议）的终点，一方的网络协议不可向对方延伸。所有过往的应用层信息都从 TCP/IP 协议包被剥离成为应用层信息。

受控的信息交换：由内外网数据交换系统连接的内外网络之间，所有信息交换活动都在预先建立的有效安全通道上进行，这些协议通道借助严格的安全策略进行控制，因此能防范恶

意攻击和敏感信息的泄漏。

基于用户的访问控制：内外网络之间，只有合法用户的特定信息交换活动才允许通过。协议通道的建立、通信、断开，都是在严格的基于用户的访问控制之下进行的。

防范各类攻击和信息泄漏：借助用户访问控制、安全协议通道的建立、安全策略的设定，内外网数据交换系统可以发现、过滤并阻塞各种已知和未知的攻击，特别是很多基于应用的攻击手段，例如 Web 脚本攻击、病毒和蠕虫等恶意代码，有效保护内部网络系统的安全性。与此同时，借助严格的内容控制，也可以防止内部敏感信息外泄。

应用级的安全审计：借助预先设定的审计策略，内外网数据交换系统可以对所有信息交换过程中出现的问题进行审计记录，便于及时获知“谁在何时做了何事”。

综上所述，内外网数据交换系统一方面可以防止来自外部网络的恶意攻击，另一方面也能防止内部网络重要信息的泄漏，在保证安全性的前提下，最终实现了灵活的网间信息交换。

3.1 产品功能结构

3.1.1 安全 Web 应用浏览功能

内外网数据交换系统的 Web 浏览实现内网用户安全的访问外部网站，同时可以提供安全的内网服务器供外网端用户访问。除了基本的配置之外，内外网数据交换系统在该业务功能加入了多种安全策略供管理员配置。

3.1.2 安全邮件收发功能

内外网数据交换系统在处理邮件相关协议时，可将其看作一个安全的邮件信息交换平台，用户可以使用常见的邮件客户端工具（如 outlook 和 foxmail）来设置在互联网上的公共邮箱，以便实现邮件信息交换。 内外网数据交换系统在业务功能的处理中加入了多种保护邮件

的策略设置。

3.1.3 安全 FTP 文件交换功能

内外网数据交换系统提供的 FTP 协议通道主要保护内网 FTP 服务器不受攻击。除受控通道的基本安全支持外，FTP 协议还可对使用 FTP 通道传输的内容进行过滤，包括恶意代码的查杀。

3.1.4 安全配置功能

内外网数据交换系统提供统一的 B/S 模式的管理配置页面，用户可以使用数字证书的方式登录管理界面，对系统的各个参数进行配置。管理页面采用三权分立的设计，有效区分各个管理员的职能，并且实现清晰的管理员操作日志审计。在内外网数据交换系统中，可以实现一端配置，两端应用的功能，用户在使用过程中只需要登录一端，即可以进行整个交换平台的配置，增强了用户的管理的方便性。

内外网交换平台系统采用安全加固的可信操作系统，使用特定的方式访问管理界面，进而保证系统的安全性。

3.1.5 网络配置功能

内外网数据交换系统提供对设备及网络的配置，根据内外网数据交换系统接入应用系统的模式和部署方式不同，可以对设备信息和网络地址进行不同的配置。同时，根据业务使用要求，可以针对业务的管理口和业务口进行调整，满足用户的多种不同的要求。

3.1.6 安全审计功能

内外网数据交换系统的审计功能提供了系统自身日志、管理操作日志、业务日志。对应

用环境中的用户操作进行全面的安全审计，为用户提供极具可读性的操作级审计日志，兼容第三方审计系统，保证应用系统中用户访问行为、重要安全事件等具有历史追溯性。

3.1.7 定制应用

除了以上几种基本的应用外，内外网数据交换系统还可以根据用户的需求进行新的自定义应用的开发。自定义应用得益于内外网数据交换系统在设计上的强大的可扩展性，它使得内外网数据交换系统具有了很大的灵活性，能够适应多种应用领域。

此处详细介绍产品的各个功能，值得注意的是毕竟产品白皮书是对外的宣传手册，不能泄露核心信息，把握“描述多于定义，定性多于定量”原则

4 产品特点

4.1 实现严格的数据隔离

内外网数据交换系统的安全隔离，只允许内外网数据交换平台通过专有单一协议进行直接跨网通信，而对其他非授权通信一律阻断，实现多个安全子域之间的数据隔离。

4.2 细粒度的访问控制保障应用安全

内外网数据交换系统面向用户应用，采用身份认证技术、细粒度访问控制技术、强审计技术、加密技术、防攻击技术等多种安全机制，全方位保障用户业务应用系统的安全。可信应用安全系统综合考虑用户业务的实际安全性需求和信息安全等级保护安全技术指标，满足了关键业务应用系统的高等级安全要求。

4.3 有效提升业务性能和可靠性

内外网数据交换系统采用负载均衡技术、应用转发技术、流量整形技术、WEB 加速技术、自容忍机制等多种技术，有效地帮助用户提升业务性能和可靠性。当用户业务应用系统出现大流量访问时，内外网数据交换系统可对输入/输出数据进行合理的流量整形，避免数据拥塞造成应用服务性能下降或者设备宕机，从而保障重要业务运行的连续性和可靠性。当服务流量达到临界阈值时，内外网交换系统可自动设置优先保护重要应用服务的安全。内外网交换系统可通过 WEB 加速功能，提升用户 B/S 模式业务系统响应速度和处理性能，改善客户端的使用体验。

4.4 实现集中的安全管理

内外网数据交换系统通过内置 LDAP、SNMP 和 Syslog 协议功能模块，实现与第三方集中安全管理平台的兼容。同时，可信应用安全系统还支持第三方的统一身份认证，提高安全机制的普适性。

4.5 安全机制自身可信

内外网数据交换系统采用基于密码的可信安全平台设计，确保安全机制不会被破坏，不会被规避，更不会成为安全攻击的跳板，在保障自身安全性的同时有效帮助用户保护应用服务器的安全。当出现系统故障时，通过内置的自检功能，可确保迅速回到保护状态，无需系统管理员手动干预，始终确保业务运行的连续性。实现双机热备功能，进一步提高本身的可靠性。

4.6 兼容多种应用类型

内外网数据交换系统支持多种用户使用场景 ,支持多种应用类型 ,如支持 HTTP、HTTPS、SMTP/POP3、TNS、FTP 等协议

4.7 全面的安全审计

支持管理员操作行为审计，支持业务级操作行为和用户对应用资源的访问记录，兼容第三方安全审计管理平台，支持 Syslog 日志输出协议。

5 客户收益

5.1 提升客户信息系统建设的安全性。

5.2 帮助客户构建符合国家等保要求的信息系统。

5.3 规范客户对外数据交换的统一接口。

5.4 增强信息融合过程中的易用性。

6 特别说明

6.1. 本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，国路安恕不另行通知。

6.2. 本手册中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，此可能产生的差异为正常现象，相关问题请咨询国路安客户服务中心。

6.3. 本手册中没有任何关于其他同类产品的对比或比较，国路安也不对其他同类产品表达意见，如引起相关纠纷应属于自行推测或误会，国路安对此没有任何立场。

6.4. 本手册中提到的信息为正常公开的信息，若因本手册或其所提到的任何信息引起了他人直接或间接的资料流失、利益损失，国路安及其员工不承担任何责任。