聚铭安全隔离与信息交换系统产品技术白皮书

聚铭网络科技有限公司

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和北京聚铭信安科技有限公司。

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

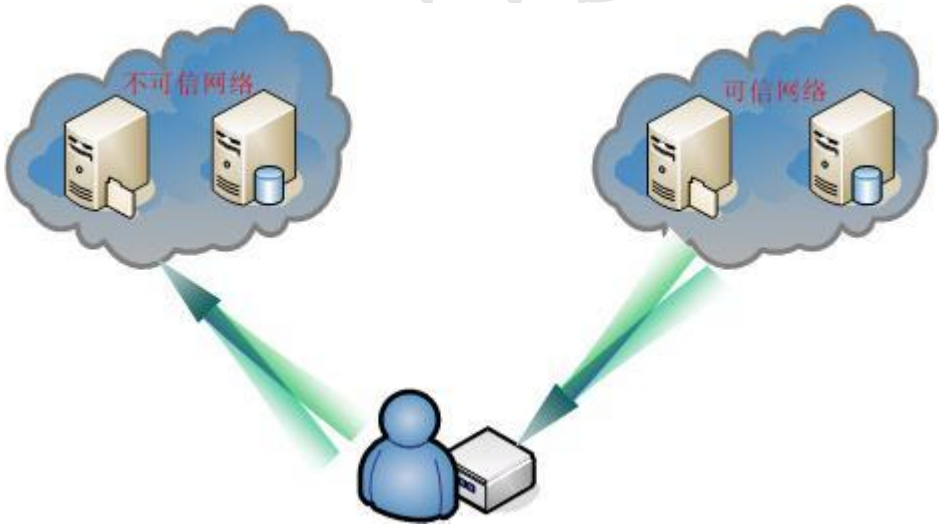
产品支持：support@juminfo.com

1. 背景介绍

随着网络技术的不断应用和完善，Internet 正在越来越多地渗透到社会的各个方面。一方面，企业上网、电子商务、远程教育、远程医疗等一系列网络应用蓬勃发展，人们的日常生活与网络的关系日益密切；另一方面，网络用户组成越来越多样化，出于各种目的的网络入侵和攻击越来越频繁。人们在享受互联网所带来的丰富、便捷的信息同时，也日益感受到频繁的网络攻击、病毒泛滥、非授权访问、信息泄密等问题所带来的困扰。

传统的安全产品可以以不同的方式满足我们保护数据和网络安全的需要，但不可能完全解决网络间信息的安全交换问题，因为各种安全技术都有其局限性。为保护重要内部系统的安全，

在不同安全等级的网络及系统之间实施安全隔离是一个行之有效的安全保密措施，可切断信息泄漏的途径。最初的解决方案很简单，即通过人工的操作来实现。如下图所示：



在不同安全等级的网络中进行信息交换的时候，由指定人员将需要转移的数据拷贝到软盘等移动存储介质上，经过查病毒、内容检查等安全处理后，再复制到目标网络中。这种解决方案可实现网络的安全隔离，但数据的交换通过人来实现，工作效率低；安全性完全依赖于人的因素，可靠性无法保证。在数据量不大，交换不频繁的情况下，通过人工交换数据的确简单可行。然而，随着电子政务的开展，内外网交换数据的数量和频率呈几何量级上升，这种解决方案已经越来越

无法满足用户的需要。如何保证信息在不同安全等级的网络间安全交换成为制约电子政务发展的瓶颈。

安全隔离与信息交换系统（简称：网闸）是新一代网络安全隔离产品。该产品采用专用硬件和模块化的工作组件设计，集成安全隔离、实时信息交换、协议分析、内容检测、访问控制、安全决策等多种安全功能为一体，适合部署于不同安全等级的网络间，在实现多个网络安全隔离的同时，实现高速的、安全的数据交换，提供可靠的信息交换服务。

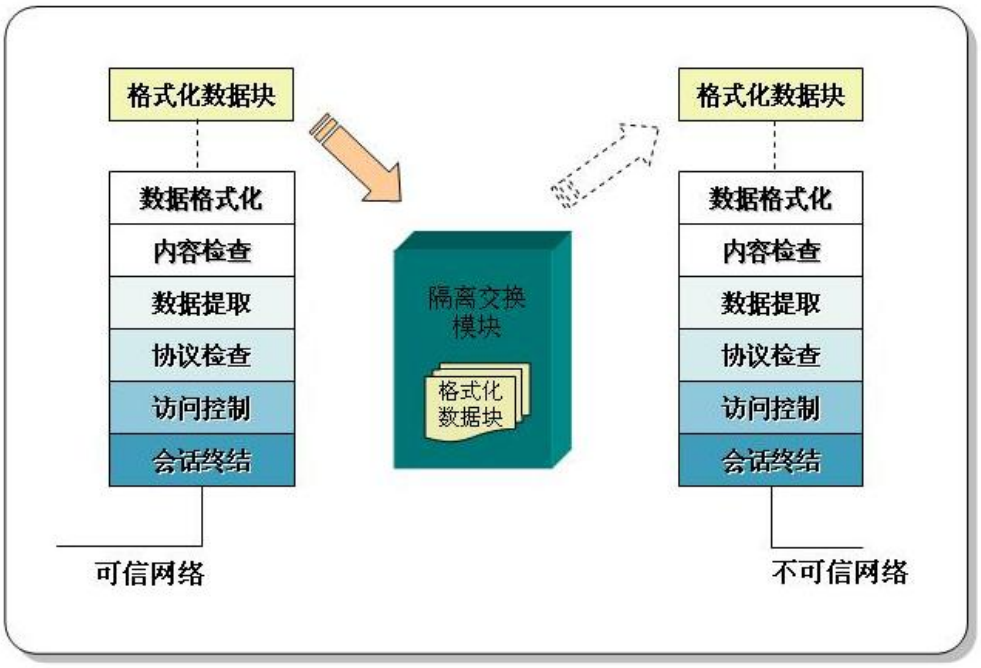
安全隔离与信息交换系统可广泛应用于各级政府机关、军队、公安、科研院校及民航、电力、石油、金融、证券、交通等网络环境，实现信息的安全交换。尤其适合于电子政务、网上工商、网上报税、网上报关、电子审批、政府信息系统管理等需要严格内外网隔离的应用环境。

2. 产品原理

安全隔离与信息交换系统的工作基于人工信息交换的操作模式，即由内外网主机模块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安全隔离与信息交换系统放心的访问非可信网的资源，而不必担心可信网的安全受到影响。

信息通过安全隔离与信息交换系统传递需经过多个安全模块的检查，以验证被交换信息的合法性。当访问请求到达内外网主机模块时，首先由安全隔离与信息交换系统实现 TCP 连接的终结，确保 TCP/IP 协议不会直接或通过代理方式穿透安全隔离与信息交换系统；然后，内外网主机模块会依据安全策略对访问请求进行预处理，判断是否符合访问控制策略，并依据 RFC 或定制策略对数据包进行应用层协议检查和内容过滤，检验其有效载荷的合法性和安全性。一旦数据包通过了安全检查，内外网主机模块会对数据包进行格式化，将每个合法数据包的传

输信息和传输数据分别转换成专有格式数据，存放在缓冲区等待被隔离交换模块处理。这种“静态”的数据形态不可执行，不依赖于任何通用协议，只能被安全隔离与信息交换系统的内部处理机制识别及处理，因此可避免遭受利用各种已知或未知网络层漏洞的威胁。如下图所示：



安全隔离与信息交换系统通过专有的隔离交换卡实现内外网主机模块的缓冲区内存映射功能，将指定区域的数据复制到对端相应的区域，完成数据的交换。隔离交换卡内嵌安全芯片，采用高速全双工流水线设计，内部吞吐速率达 5Gbps，完全可以满足高速数据交换的需要。

隔离交换模块固化控制逻辑，与内外网模块间只存在内存缓冲区的读写操作，没有任何网络协议和数据包的转发。隔离交换子系统采用互斥机制，在读写一端主机模块的数据前先中止对另一端的操作，确保隔离交换系统不会同时对内外网主机模块的数据进行处理，以保证在任意时刻可信网与非可信网间不存在链路层通路，实现网络的安全隔离。

当内外网主机模块通过隔离交换模块接收到来自另一端的格式化数据，可根据本端的安全策略进行进一步的应用层安全检查。经检验合格，则进行逆向转换，将格式化数据转换成符合 RFC 标准的 TCP/IP 数据包，将数据包发送到目的计算机，完成数据的安全交换。

3. 主要功能

3.1 访问控制

系统支持强大的访问控制策略，支持通过源地址、目的地址、端口、协议等多种元素对允许通过安全隔离与信息交换系统传输的数据进行过滤，判断是否符合组织安全策略。

3.2 地址绑定

提供 IP 与 MAC 地址绑定功能，可对指定接口所连接的网络中的主机的 IP 和 MAC 地址进行绑定，防止内部用户盗用 IP 和内网地址资源分配的混乱，方便网络 IP 资源管理，支持 IPV4 和 IPV6 双协议。

3.3 安全浏览

- 支持 HTTP、HTTPS 应用协议，实现各种互联网浏览和访问；
- 支持对 HTTP、HTTPS 协议端口访问过滤，支持源地址、目标地址及端口过滤控制；
- 支持 URL 过滤、页面内容过滤、文件名过滤、脚本过滤等。

3.4 邮件访问

- 支持基于 SMTP 协议的邮件发送和 POP3 协议的邮件接收；
- 支持对 SMTP、POP3 协议端口访问过滤，支持源地址、目标地址及端口过滤控制；
- 支持邮件收/发件人地址过滤、主题关键字黑名单过滤、附件大小和类型过滤等。

3.5FTP 访问

- 支持 FTP 文件传输应用协议，允许用户选择 FTP 传输模式；
- 支持对 FTP 协议端口访问过滤，支持源地址、目标地址及端口过滤控制；
- 支持访问用户名过滤、访问协议命令过滤、上传下载文件类型过滤等。

3.6 数据库访问

- 支持 MySql、SqlServer、Oracle、DB2、Sybase 等主流数据库系统的访问；
- 支持达梦、金仓等国产化数据库系统的访问；
- 支持对数据库协议端口访问过滤，支持源地址、目标地址及端口过滤控制；
- 支持对访问数据库的用户过滤控制。

3.7 定制访问

- 支持用户自定义协议类型和端口，实现特定 TCP、UDP 协议的数据隔离交换；
- 支持对用户自定义协议端口访问过滤，支持源地址、目标地址及端口过滤控制。

3.8 文件同步

- 实现不同安全等级网络之间的安全文件交换，支持 SFTP、NFS、SMBFS、SAMBA 等文件系统；
- 文件完整性校验机制，如若文件同步异常，将提示用户重新传输；
- 支持文件增量传输，如果发送端数据变化时，发送端都能及时将更新的数据发送至接收端。

3.9 内容检查

安全隔离与信息交换系统提供多种内容安全过滤与内容访问控制功能，既能有效的防止外部恶意代码进入内网，也能控制内网用户对外部资源不良内容的访问及敏感信息的泄漏。安全隔离与信息交换系统的内容检查机制主要针对 HTTP、FTP、邮件及文件交换等应用，包括 URL 过滤、关键字过滤、Cookie 过滤、文件类型检查、病毒查杀及入侵检测等操作。

◆ URL/域名过滤

安全隔离与信息交换系统可对用户访问的Web站点的域名及URL等进行基于正则表达式的过滤，禁止用户访问暴力、色情、反动的主页或站点中的特定目录或文件。

◆ 黑/白名单关键字过滤

安全隔离与信息交换系统可对邮件标题和内容以及传输的文件等进行黑/白名单关键字过滤，进行单词及短句的智能匹配，禁止包含特定关键字的敏感信息泄漏，或只允许包含相应关键字的文件通过安全隔离与信息交换系统传递。

◆ COOKIE 过滤

安全隔离与信息交换系统可对 COOKIE 进行过滤。通过对 COOKIE 进行过滤，可以防止敏感信息的泄漏。同时还可以防止用户进行浏览论坛、上网聊天等违反安全策略的操作。

◆ 文件类型检查

安全隔离与信息交换系统可对传输的文件进行类型检查，只允许符合安全策略的文件通过安全隔离与信息交换系统传递。避免传输二进制文件可能带来的病毒和敏感信息泄露等问题。

◆ 病毒及恶意代码检查

系统可内嵌杀病毒引擎，针对文件交换模块、FTP 访问模块、安全浏览模块、邮件访问模块防病毒功能。对允许传输的文件进行病毒的检查，确保进入可信网络的文件不包含病毒及 Java/JavaScript/ActiveX 等恶意代码，支持本地升级及远程升级。

◆ 入侵检测

可对网页攻击、缓冲区溢出攻击、后门/木马、P2P、病毒/蠕虫、拒绝服务攻击、扫描类攻击等多种攻击类型进行实时检测并记录日志。

3.10 数据库同步模块

安全隔离与信息交换系统的数据库同步模块，独立自主开发完成，完全内置于安全隔离与信息交换系统内部，所有的同步操作由安全隔离与信息交换系统自己独立完成。不在用户数据库中安装任何客户端软件，不需要在用户网络中部署专用服务器，对用户数据库不作任何改变。该模块支持 Oracle 和 Sql Server 等流行数据库版本，同时预留开发接口，定制支持各种数据库系统。在高速运行的基础上解决了字段级数据同步、双向数据同步、大字段同步等技术难题，适合于各种数据库同步工作的需要。

由于是安全隔离与信息交换系统自身发起的动作，所以安全隔离与信息交换系统两侧不开放任何基于数据库访问或者定制 TCP 的网络服务端口，避免网络安全漏洞。

- 支持 MySql、SqlServer、Oracle、DB2、Sybase 等主流数据库系统的同步；
- 支持达梦、金仓等国产化数据库系统的同步；
- 支持同构、异构等传输方式。

3.11 高可用设计

安全隔离与信息交换系统遵循高可用性设计，支持网络口、HA 多种高可用实现模式，最多支持 32 台设备进行负载均衡，全面解决设备故障与链路故障造成的业务中断，保证系统 7X24 小时不间断服务。

3.12 轻松的管理

安全隔离与信息交换系统配备专门的管理端口，通过数字证书认证与管理信息的加密传输实现安全隔离与信息交换系统设备的集中管理。系统采用全中文的 Web 方式进行远程网络管理，支持通过 IPV4 或者 IPV6 协议对安全隔离与信息交

换系统进行管理，界面友好，操作方便。系统管理员和审计员实现分权管理，使得对安全隔离与信息交换系统的管理更加安全可控，避免人为因素带来的安全风险。

3.13 传输方向控制

安全隔离与信息交换系统采用双通道通信机制，从可信网到非可信网的数据流与从非可信网到可信网的数据流采用不同的数据通道，对通道的分离控制保证各通道的传输方向可控。在特殊应用环境中可实现数据的单向传送，以避免信息的泄漏。

3.14 协议分析能力

系统支持 HTTP/HTTPS、POP3、SMTP、FTP 等多种应用层协议，可对常见协议的命令和参数进行分析和过滤。

应用数据以“原始”的形态在内外主机模块中传递，数据包经过预处理、安全决策、RFC 校验、协议分析、数据提取、格式化等多个处理模块的检查，充分保证了交换信息内容的安全。

3.15 完善的安全审计

安全隔离与信息交换系统提供管理员多种手段了解网络运行状况及可疑事件的发生。用户可根据特定的需要进行日志审计（包括系统日志、访问控制策略日志、应用层协议分析日志、应用层内容检查日志等）。系统支持本地日志缓存，可实现本地日志的浏览查询等操作。日志依据事件的重要程度分为错误/警告/通知三级，支持 Syslog 日志存储，可实现日志的分级发送。

安全隔离与信息交换系统提供管理员多种手段了解网络运行状况及可疑事件的发生。主要方式如下：

控制台方式：通过管理控制台可以实时监控日志告警信息。

Syslog：以 Syslog 方式向管理工作站发送告警信息。

3.16 强大的抗攻击能力

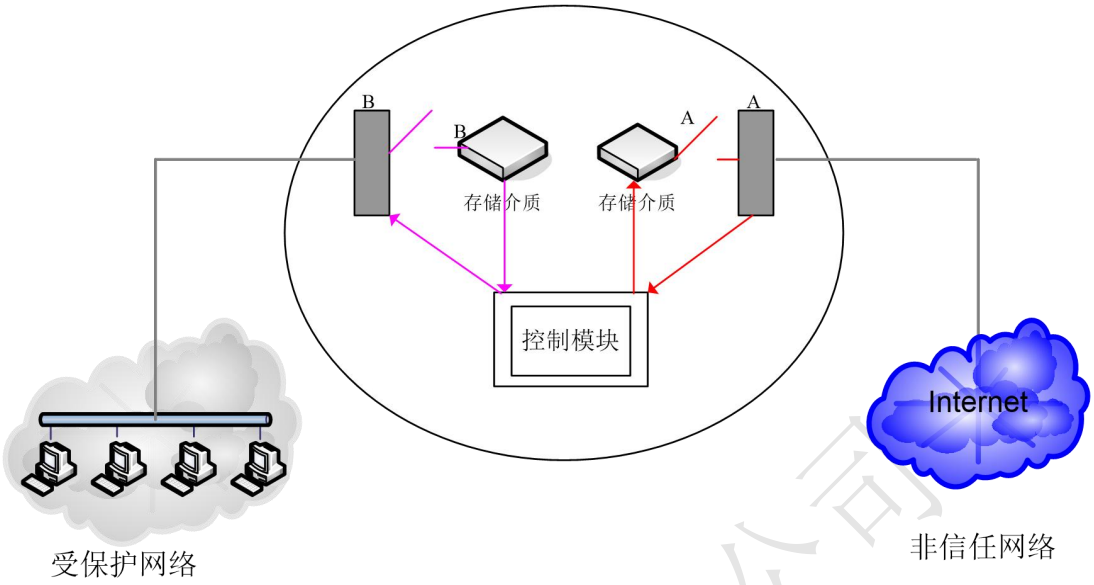
安全隔离与信息交换系统具备强大的抗攻击能力，内外网主机模块采用专用的安全操作系统，内核经过特殊定制，实现强制性访问控制，保护自身进程及文件不被非法篡改和破坏。

4. 产品亮点

在网络中部署既能够符合政府、军队、企事业单位等的强制性安全策略——既在不同安全等级的网络间实现安全隔离，又能够保证可靠、安全的信息交换，提供文件交换、收发电子邮件、数据库同步、安全浏览等多种服务，在网络应用的安全性及可用性间取得完美的平衡。

4.1 安全高效的硬件交换系统

安全隔离与信息交换系统具有安全团队自主研发的内外主机系统间的安全检测与控制处理单元，采用专有电路设计的双通道高速数据交换卡，实现了独立的硬件交换控制逻辑，无操作系统及任何“软”控制，自主完成数据的交换，系统只负责把数据写到隔离交换卡中的缓冲区，由隔离交换卡根据硬件控制逻辑自动完成数据交换，自动同步两侧控制逻辑，进行互斥的读写操作，同时还具有自动数据完成性校验，当发现数据错误时，自动重传，保证数据的完全正确。在保证安全性的同时，提供更好的处理性能，能够适应各种复杂网络环境对隔离应用的需求。



安全隔离与信息交换系统在内外主机系统间采用专有协议，阻断网络连接，不仅使得信息网络的抗攻击能力大大增强，而且有效地防范了信息外泄事件的发生。

4.2 完美的网络环境适应性

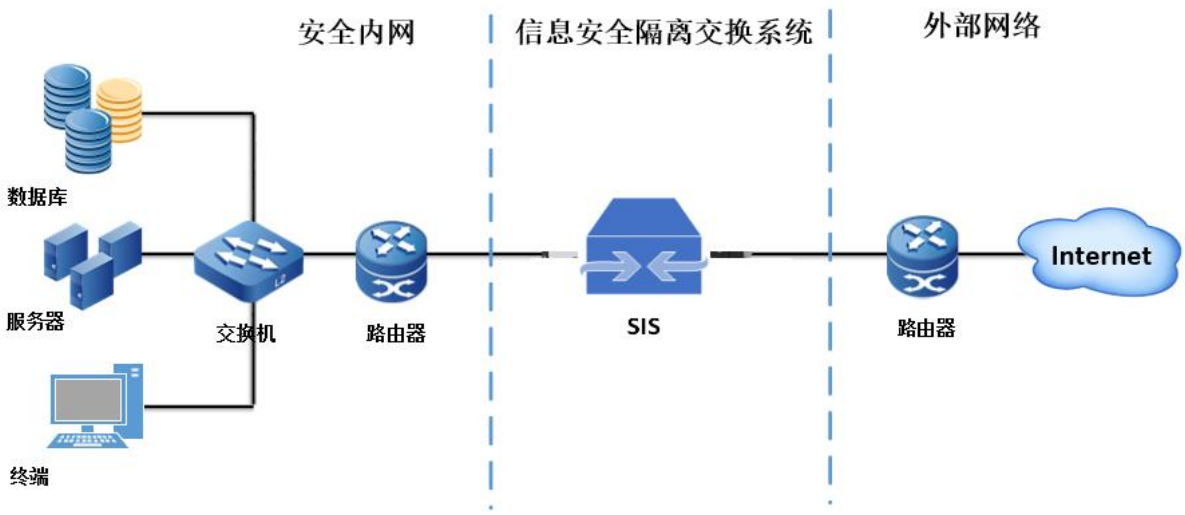
安全隔离与信息交换系统支持 IPV4 和 IPV6 两种协议栈，可灵活部署、完美适应各类型网络，而且支持 IPV4/IPV6 混合接入，即支持一端为 IPV4 环境，一端为 IPV6 环境。强大的网络环境适应性，不需要改变网络环境，更换网络设备，全业务应用支持，能够适应工业环境业务应用数据交换要求，更是有效保障了数据安全。

4.3 可靠的冗余和负载均衡架构

安全隔离与信息交换系统基于可靠性的考虑，通过双机热备等技术保证了在网络或设备故障时，业务的不间断运行。

在网络流量较大时，也可能会造成业务不可用和响应速度下降，安全隔离与信息交换系统支持多台设备的负载均衡（最多支持 32 台），最大限度的提升了网

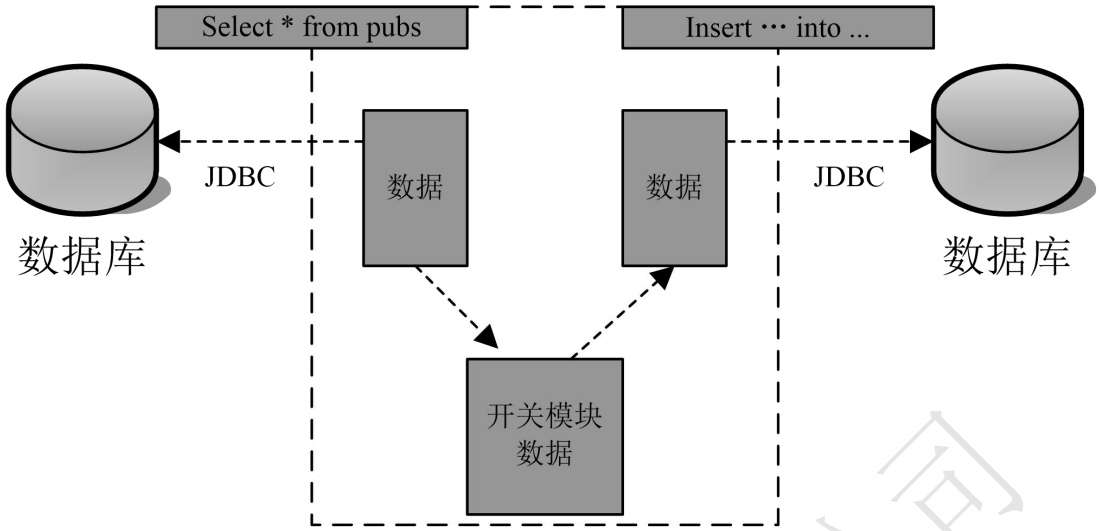
络的可用性。



4.4 先进的数据库同步技术

安全隔离与信息交换系统常会应用在数据库服务器的环境中，为了实现数据库同步，一般情况下都需要在内、外网数据库服务器上安装数据库同步软件，这不仅会占用数据库服务器的资源、增加部署和实施的难度，同时不可避免会有漏洞。

安全隔离与信息交换系统采用先进的同步技术，无需在内、外网数据库服务器上安装第三方同步软件，减少因安装第三方同步软件造成对数据库影响的可能性，还可提供对数据库用户的细粒度控制。同时由于不用开放监听端口，更具安全性，为用户提供了性价比极高的数据库同步解决方案。



4.5 核心应用的安全最大化

从安全实现的角度来讲，越接近应用层，则安全问题越复杂，解决问题也越困难。安全隔离与信息交换系统将应用层的数据转换成专有的数据格式进行处理，只允许安全的、可靠的信息在网络中传递。信息的格式、内容、交流对象等因素可依据企业安全策略指定，简化了核心应用面临的安全问题，确保了核心应用的安全最大化。

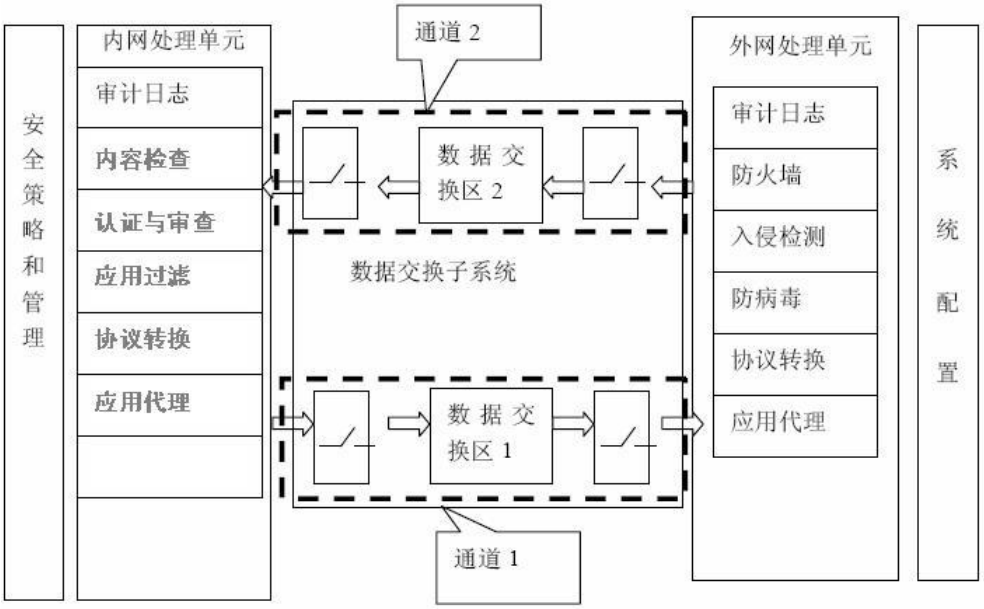
传统的安全检测产品只能发现利用已知安全漏洞发起的攻击。如果一种攻击手法还没有公布，则凭借现有的技术无法了解其攻击特征，也就无法识别攻击行为。安全隔离与信息交换系统对数据的交换不依赖于任何通用协议，没有数据包的处理及连接会话的建立，而是以静态的专有格式化数据块的形式在内/外网间传递，因此不会受到任何已知或未知漏洞的威胁。

4.6 深度内容检测

安全隔离与信息交换系统提供多种内容安全过滤与内容访问控制功能，既能有效的防止外部恶意代码进入内网，也能控制内网用户对外部资源不良内容的访问及敏感信息的泄漏。

内容检查机制可以针对 HTTP、FTP、邮件及文件交换等应用，包括 URL 过滤、

关键字过滤、Cookie 过滤、文件类型检查及病毒查杀等操作。



内容检查机制还可以针对客户自定义的协议，包括对自定义协议中的指定字段，如应用层协议、内容、关键字等，都可以直接检测出来，根据白名单或黑名单设置，允许通过或者禁止通过。

4.7 支持全国产化

采用全国产化硬件+国产化操作系统平台，符合国家信创要求，提高产品的安全性和可靠性，产品更加安全可控。

5. 典型应用

安全隔离与信息交换系统适合部署在需要在不同安全等级的网络间实现信息共享的环境，可应用在不同的涉密网络之间；同一涉密网络的不同安全域之间；与互联网物理隔离的网络和秘密级涉密网络之间；未与涉密网络连接的网络和互联网络之间，通过安全隔离与信息交换系统的安全控制，在保证信息安全的前提下更好地促进各个业务系统的互联互通、资源共享。

5.1 数据库安全同步解决方案

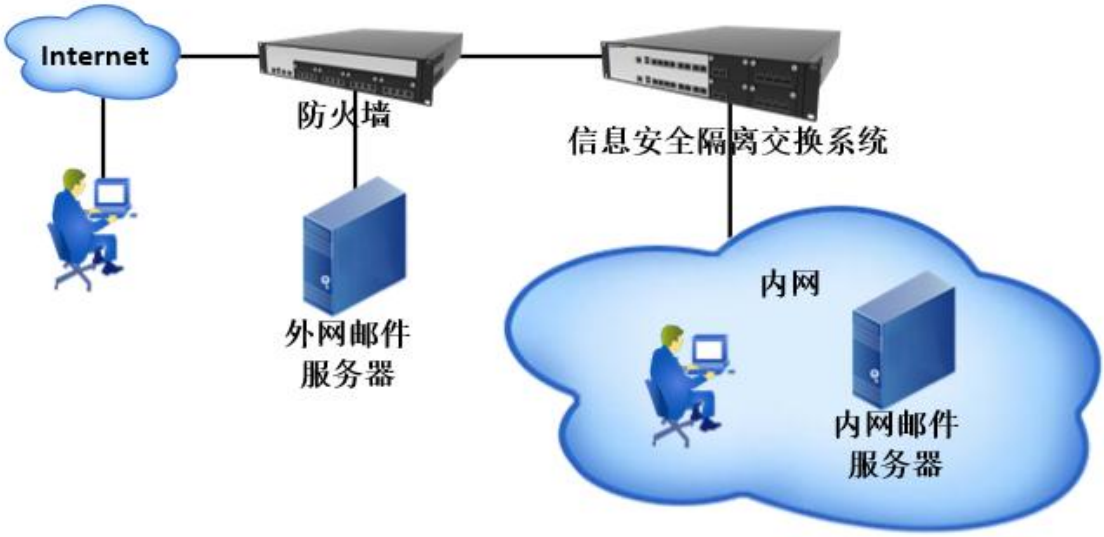
某政府部门开展电子政务，允许公众通过互联网提交服务申请并查询结果。如果允许访问者通过 Web 服务器直接向核心数据库服务器发起数据访问请求，则黑客可能穿透防火墙的保护直接侵入后台数据库系统，严重威胁到业务的正常开展。

如上图所示，采用安全隔离与信息交换系统，在核心数据库服务器和外部不可信网络间实现安全隔离，则来自互联网的用户只能通过 Web 服务器访问到前置数据库服务器。根据安全策略定时将前置数据库和核心数据库的内容进行同步，既可满足对外服务的要求又提供了安全保障。这种方式强化了应用层的安全控制，可有效防止 TCP/IP 数据包穿越网络到达核心数据库服务器，大大增强了系统的安全性，为电子政务的有效开展提供了可靠的保证。

安全隔离与信息交换系统提供多种数据库同步方式，可定制同步周期及方向，支持 Oracle、Sybase、SQL Server、MySQL、DB2 等多种主流数据库。系统支持基于触发器和快照两种方式的增量数据复制，可实现异类数据库间的数据同步。系统提供 C/C++编程接口，可以方便的与其它系统的集成。

5.2 安全邮件收发解决方案

某机构强制要求内网禁止与互联网相连，但根据业务需要必须通过电子邮件与外界进行信息交流。如采用人工方式，即由专人负责在公众信息网接收电子邮件，再通过移动存储介质复制到内部网进行处理，则信息不能得到及时处理，严重影响工作效率；若采用内外网邮件服务器转发的方式，安全又得不到保证。



为解决这一问题，在内外网间部署安全隔离与信息交换系统。安全隔离与信息交换系统可以保证可信内网与 Internet 安全隔离，内外网邮件服务器间不存在链路层连接，没有数据包的交换，因此无法通过邮件系统对内部办公网发起攻击。系统可以为每个用户制定各自的邮件交换策略，对邮件内容、附件类型及垃圾邮件、带病毒邮件等进行过滤，从而使内网用户可以在内网安全地收发邮件，保证安全的邮件处理。

5.3 安全文件交换解决方案

安全隔离与信息交换系统，由安全管理员制定相应的信息交换策略，在网络安全隔离的前提下定时进行文件交换。系统还支持交换方向、文件类型的指定，可对被交换文件进行内容检查、查病毒等处理，只允许或不允许包含相应内容的

文件通过安全隔离与信息交换系统传递。

安全隔离与信息交换系统可对数字签名进行校验，以起到身份认证、防抵赖的作用。