绿盟绿盟安全隔离与信息交换系统

技术白皮书

■ **文档编号**	请输入文档编号	■ **密级**	请输入文档密级
■ **版本编号**		■ **日期**	2018-06-14

■ **版本变更记录**

时间	版本	说明	修改人
2018-06-14	V1.0		刘智飞

■ **适用性声明**

本模板用于撰写绿盟科技内外各种正式文件，包括技术手册、标书、白皮书、会议通知、公司制度等文档使用。

目录

表格索引

插图索引

一、 概述

1.1 产品背景

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。随着互联网基础设施的不断完善，中国互联网进入了新的发展阶段，如何充分利用互联网改进工作方式、提高工作效率成为最主要的议题，因此党和政府积极推动“电子政务”工程的建设，希望实现各部门资源共享、协同办公，进而提高政府办公效率，同时实现政务公开并强化政务监管。电子政务建设需要将原本相互独立、相互隔离的各部门网络相互连接，实现适度资源共享和业务互动，同时，各部门、各单位也需要将政府内网的部分信息及业务向互联网公开，提供信息服务。在这种情况下，人们最关心的是如何确保数据安全和防止机要信息外泄，因为这些问题直接与国家安全、政府形象相关。

毫不夸张地说，信息安全是电子政务建设的重中之重，但是在信息安全保障问题上，我们又面临这样问题：首先，仅依靠简单的、单一的安全措施，如防火墙、防病毒，根本无法满足电子政务建设的安全需求；其次，如果采取早期的隔离方式，如使用隔离卡，或是利用移动介质进行手动数据传递，这种低效率、低可靠性的解决方案也无法满足电子政务建设的业务需求，因此，用户需要具有更安全、更高效的隔离技术及产品用以进行内外网信息交换。

安全隔离技术首先出现于国外，最早出现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，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，我公司依仗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、更高性能的绿盟安全隔离与信息交换系统。

1.2 产品概述

绿盟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既可实现内外网络进行安全数据通信，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。

1.3 产品定位

绿盟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；

绿盟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。

国家保密局对绿盟安全隔离与信息交换系统类产品的应用也做了规定，规定绿盟安全隔离与信息交换系统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”。

二、 技术简介及参数

2.1 系统组成

绿盟安全隔离与信息交换系统设备分别由内、外网处理单元与数据交换单元（专用隔离芯片）三部分组成。内、外网处理单元是一台专有的网络安全计算机设备，分别连接于内外网络。内、外网处理单元之间通过专用的隔离芯片进行数据的摆渡传输，其过程类似 U 盘拷贝。当专用隔离芯片与内网联通时与外网电路是断开的，当隔离部件与外网联通时，与内网是断开的。并在确保网络隔离的前提下实现适度的数据交换；

2.2 硬件组成及参数

- 物理参数

  机箱配置：标准 19 英寸机架式

  材　　料：重负荷钢

- 电气参数

  电压：220V

  功率：350W

- 运行环境

表 1：运行环境技术参数

运行温度	-5 ～ 40℃
运行湿度	最大相对湿度 5%～90%，不结露
工作温度	0 ～ 60℃
储存温度	-20 ～ 70℃

- 电磁屏蔽
  - ✧ IEC－1000－4－2（ESD）
  - ✧ IEC－1000－4－3（辐射敏感性）
  - ✧ IEC－1000－4－4（点快速瞬变）
  - ✧ IEC－1000－4－5（电涌）
  - ✧ IEC－1000－3－2（谐波）

2.3 系统构架及工作原理

我们知道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。绿盟安全隔离与信息交换系统既然隔离、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，绿盟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绿盟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，绿盟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，绿盟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绿盟安全隔离与信息交换系统上。绿盟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）。

绿盟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 协议都不可能穿透绿盟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绿盟安全隔离与信息交换系统为例，说明通过绿盟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，

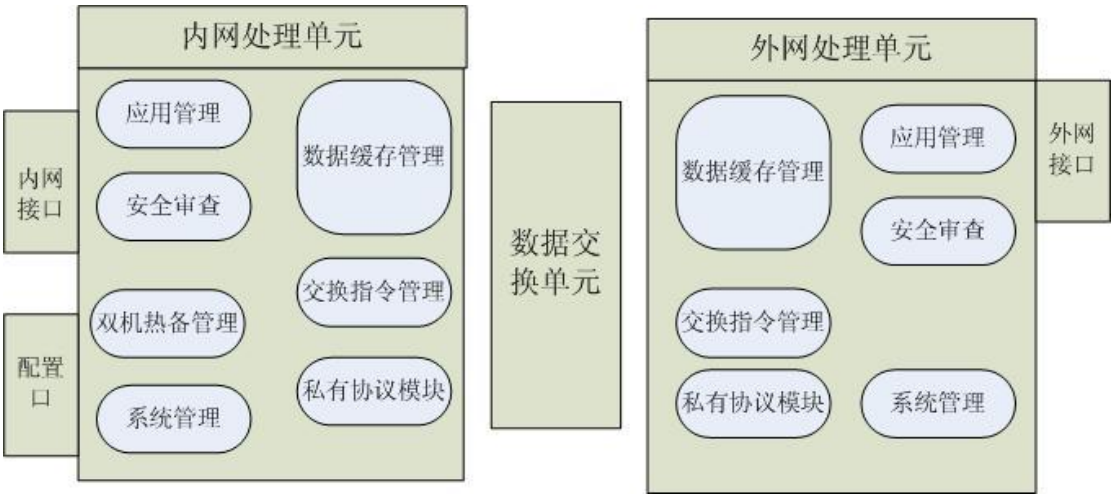

图 1 系统架构

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，

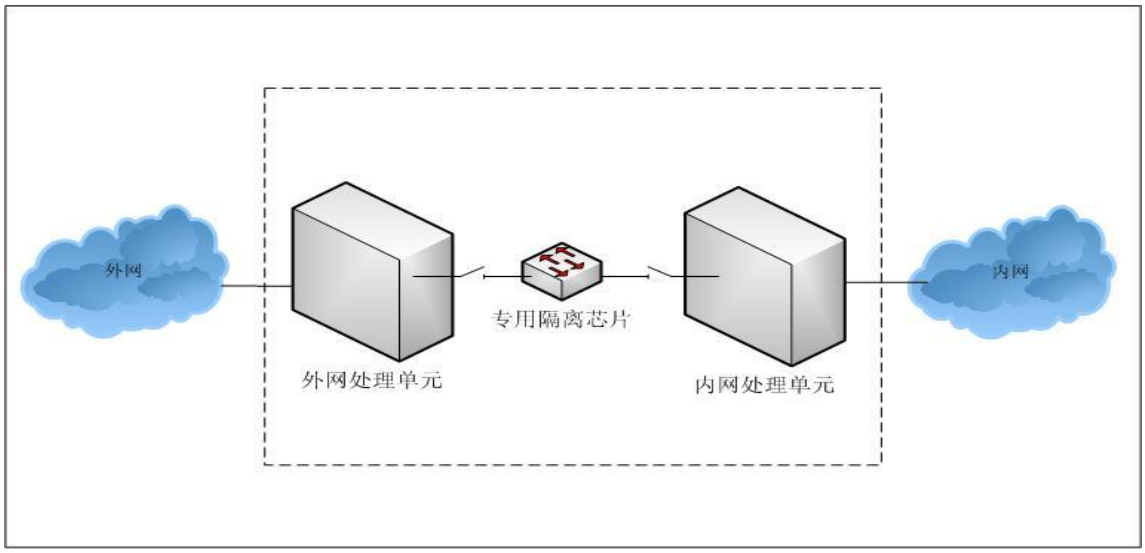

图 2 工作原理

一旦数据完全写入绿盟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。

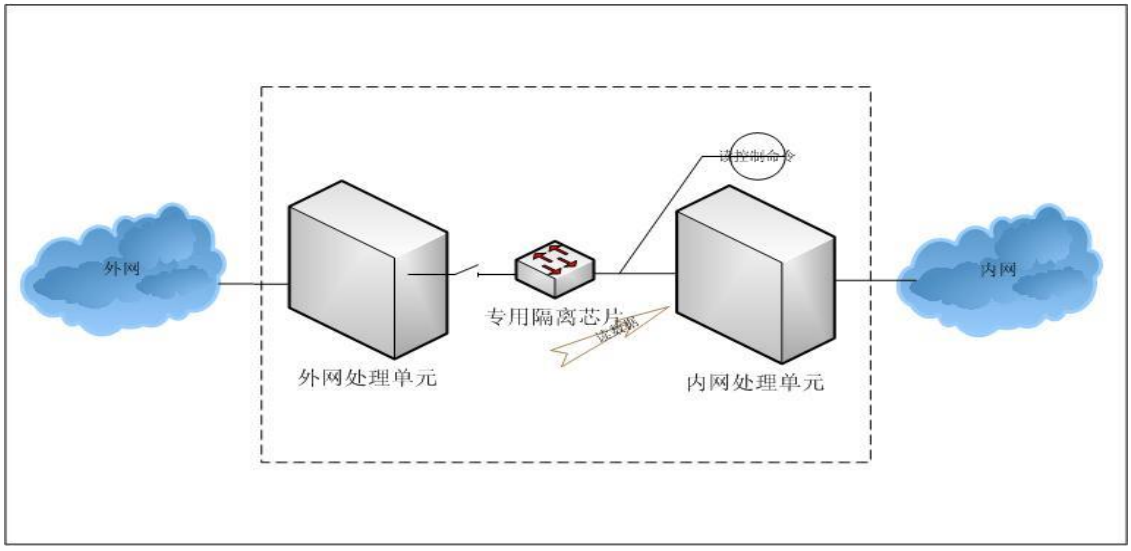

图 3 工作原理 2

绿盟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数据穿透安全传输通道，确保所有通过的数据包只被控制单元识别的合法纯数据。

绿盟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。

三、 产品功能

绿盟安全隔离与信息交换系统的主要功能特点就是在保证两个网络隔离的情况下，做一定的安全数据交换，绿盟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，其数据流转过程类似 U 盘拷贝，也像船只通过船闸的过程，所以绿盟安全隔离与信息交换系统被业内形象的简称为“绿盟安全隔离与信息交换系统”。绿盟安全隔离与信息交换系统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既可实现内外网络进行安全数据通信，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。

3.1 业务功能

3.1.1 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，仅许可正常的、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。

3.1.2 信息交换

绿盟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绿盟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。

- **Web 信息交换**：通过系统内部的 Web 处理模块，绿盟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，绿盟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，绿盟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：**绿盟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。我公司绿盟安全隔离与信息交换系统产品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绿盟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：**绿盟安全隔离与信息交换系统设备支持标准的 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。采用绿盟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 MODBUS 主流协议，并可控制相应的功能代码。比如只允许通过 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，可借助我公司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，华御绿盟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的多。

3.1.3 网络访问控制

绿盟安全隔离与信息交换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。

3.1.4 数据内容审查

内容检查是指当绿盟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 FTP 的允许下载不允许上传，数据库的允许 SELECT 不允许 DELETE 等控制并将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。

3.1.5 缓存空间及传输数据的管理

绿盟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，保持文件访问效率。

3.1.6 双重安全防护机制

绿盟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，并且只有被允许的客户的网络请求才被响应。这样绿盟安全隔离与信息交换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，绿盟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，并在控制台示警，帮助管理员在最短时间内做出响应。绿盟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）无缝集成。

3.1.7 双协议栈接入

绿盟安全隔离与信息交换系统支持双协议栈接入，绿盟安全隔离与信息交换系统可同时设置 IPV4 及 IPV6 的地址，且互不影响

不仅仅支持在单一的 IPV4 的网络环境或 IPV6 的网络环境下工作，还支持在 IPV4 及 IPV6 的两个网络环境之间工作，可满足用户各种网络环境。

3.2 管理功能

3.2.1 安全的管理通信

绿盟安全隔离与信息交换系统只允许从绿盟安全隔离与信息交换系统设备的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。管理者与隔离绿盟安全隔离与信息交换系统设备采用加密的 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。

3.2.2 权限分配方式

绿盟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。

3.2.3 策略定制功能

绿盟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。

3.2.4 日志审计功能

绿盟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。

3.3 高可用性功能

3.3.1 负载均衡

绿盟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。绿盟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。

3.3.2 双机热备

绿盟安全隔离与信息交换系统提供双机热备乃至多机热备功能。两台安全绿盟安全隔离与信息交换系统设备可组成热备机组，机组内绿盟安全隔离与信息交换系统设备有主绿盟安全隔离与信息交换系统设备与备用绿盟安全隔离与信息交换系统设备之分。从绿盟安全隔离与信息交换系统设备向主绿盟安全隔离与信息交换系统设备发起状态检测请求，并获取最新的访问策略。当主绿盟安全隔离与信息交换系统设备发生故障，从绿盟安全隔离与信息交换

系统设备启动并自动变为主绿盟安全隔离与信息交换系统设备。同时以声音与告警信息示警。

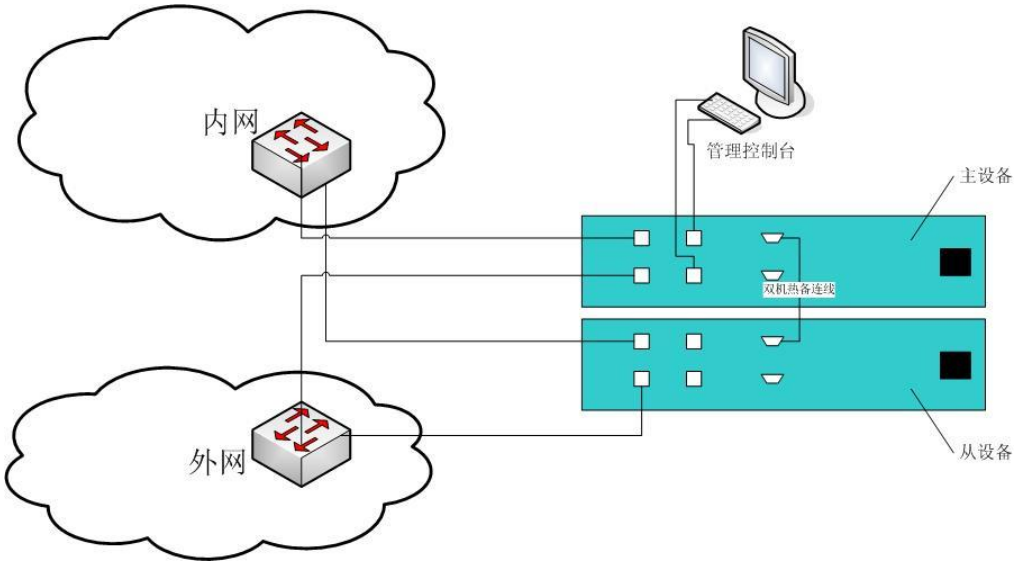

图 4 双机热备部署

四、 产品特点

4.1 高安全性

绿盟安全隔离与信息交换系统采用专有的安全操作系统，只具备绿盟安全隔离与信息交换系统必须的专用功能。安全 OS 存贮于 DOM 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。

绿盟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。绿盟安全隔离与信息交换系统采用双重全防护机制，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。

4.2 高吞吐率

绿盟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，在一台网闸设备内集成多各处理模块，成倍提升处理能力，使网闸具有很高的性能。

4.3 高可靠性

绿盟安全隔离与信息交换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，使网闸设备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。

4.4 高便利性

绿盟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，大大加强的隔离网关的便利性与可操作性。

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

五、 产品型号及性能参数

针对不同的用户的需求有不同的系列和型号相适应，不同的型号有不同的性能参数，具体参数详见型号与参数表。