

网神 SecSIS 3600

安全隔离与信息交换系统 (国产化版本)

产品彩页

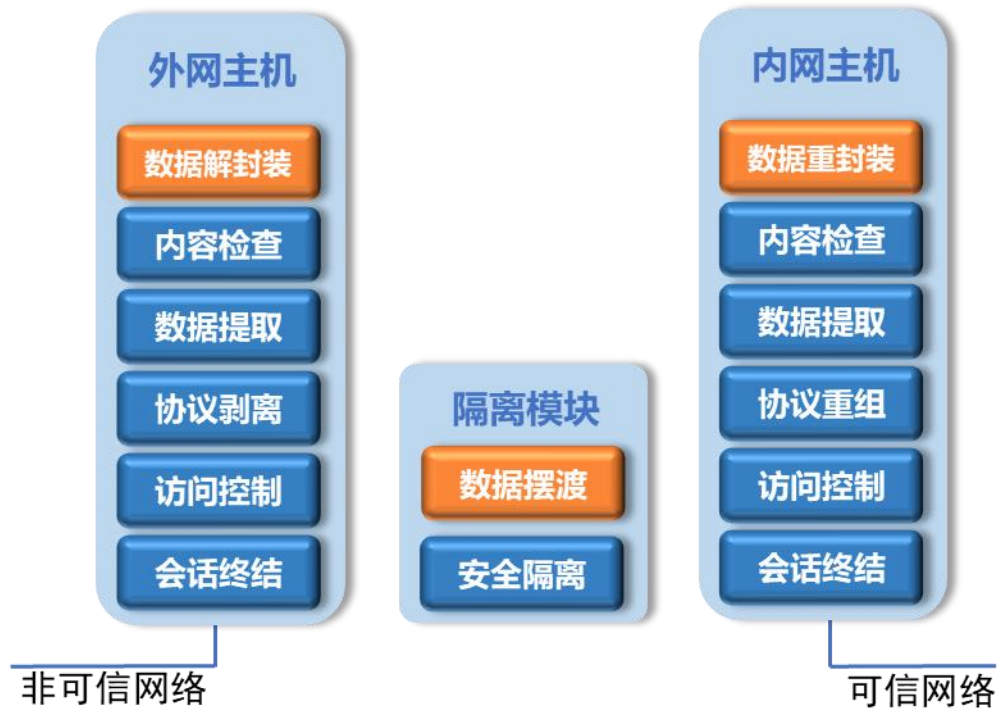
地址：北京市西城区西直门外南路26号院1号

邮编：100044

1. 产品概述

网神 SecSIS 3600 安全隔离与信息交换系统国产化系列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。

信息通过网闸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，首先由网闸实现 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网闸；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，只能被网闸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：



网神 SecSIS 3600 安全隔离与信息交换系统国产化系列通过专有的隔离交换卡实现内外网主机模块的缓冲区内映射功能，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。

2. 国产化架构

1.1 飞腾硬件平台

产品基于飞腾硬件平台，平台采用片上并行系统（PSoC）体系结构，集成了飞腾自主高性能计算核心、高效片上网络、高带宽低延迟存储系统和高速 I/O 接口，性能卓越、功耗适度，集成 ARMv8 指令集兼容处理器核 FTC660，提供领先的事务处理能力和单位功耗性能。



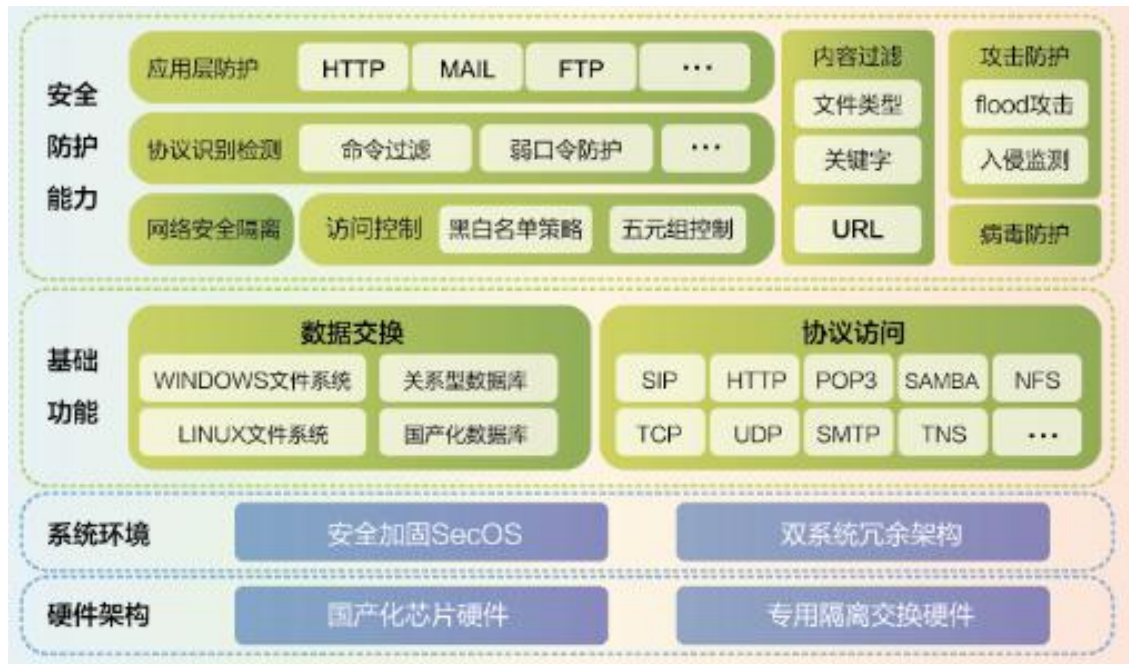
1.2 麒麟操作系统

麒麟操作系统是 863 计划重大攻关科研项目，目标是打破国外操作系统的垄断，研发一套中国自主知识产权的服务器操作系统。系统支持软、硬 RAID，支持 RAID0、RAID1、RAID5、RAID10 等多种模式。支持网络冗余，提供多模式网卡绑定功能，满足不同场景的网络需求。支持全量、增量的备份还原，支持基于 GRUB 的备份还原，兼容 Linux 平台上的应用。符合 POSIX 系列标准，并兼容 Linux 目标代码，Linux 平台上的大型应用如图形环境、Oracle 数据库服务等都可以直接运行在麒麟安全操作系统平台上，有力拓展了应用面，系统是目前我国通过认证的安全等级最高的操作系统，已广泛应用于军工、政府、金融、电力、教育、大型企业等众多领域，为我国的信息化建设保驾护航。

3. 功能介绍

1.3 功能简介

网神 SecSIS 3600 安全隔离与信息交换系统由内端机、外端机和隔离交换模块组成，其架构图如下：



1) 信息摆渡：数据交换模块由分别插在内/外网主机模块 PCI-E 接口上的交换卡和其之间的连接线组成，其负责在两个主机模块之间进行信息摆渡，保证在任一时刻，内网主机模块和外网主机模块不会出现直接或间接的物理连接。由于对通用网络协议进行检测的复杂度较高，有效性较低，因此系统不进行任何通用协议的转发和路由。只对应用层的业务数据进行交换。考虑到实现的机制、复杂度和对应用层数据检测的有效性。支持阻断视频专网与其他专网之间的所有通信协议，保证视频专网与其他专网之间的网络隔离。

对视频数据与控制信令严格区分，分别处理后进行传输。支持视频数据双向传输模式和控制信令双向传输模式。支持视频信令协议格式、视频传输协议格式及主流视频监控公司的私有协议视频信令协议格式等。

2) 文件同步

设备提供文件交换功能，通过 NFS、SMB、FTP 传输协议完成内外端机指定目录下指定文件的单向、双向文件传输，并实现关键字过滤及内容过滤。

3) 安全浏览

网神 SecSIS 3600 安全隔离与信息交换系统通过安全浏览模块实现对互联网访问，安全浏览模块在接收到来自客户端或者服务器的数据包后，都将进行协议剥离工作，从中提取出应用层纯数据。对应用层纯数据进行上述内容过滤后，然后通过信息摆渡功能进行信息交换。另一边主机模块接收到应用层纯数据后，重新构建 HTTP 协议将内容发生出去。

4) 安全 FTP

实现对两个不同安全域之间 FTP 访问，上传及下载文件，安全 FTP 模块在接收到来自客户端或者服务器的数据包后，都将进行协议剥离工作，从中提取应用层纯数据。对应用层纯数据进行上述内容过滤后，然后通过信息摆渡功能进行信息交换。另一边主机模块接收到应用层纯数据后，重新构建 FTP 协议将内容发生出去。

5) 用户认证

管理接口进行远程管理，提供 B/S 架构的系统管理和审计功能，且对远程会话采用基于 HTTPS 的加密机制，能与接入认证服务器和用户认证服务器配套使用。

管理采用加密方式，远程管理时分角色管理，即分为系统管理员和审计员。系统管理员负责系统参数配置，审计员负责日志的审计。系统管理员和审计员可修改登录口令。对设备进行远程管理时，采用用户名和密码鉴别；提供鉴别失败锁定机制，若连续 3 次鉴别失败，则系统自动锁定该账户 10 分钟；提供超时退出机制。

6) 系统管理

系统管理员可以采用 HTTPS 方式远程管理系统。支持 IPV4 和 IPV6 协议。管理员可以进行必要的网络配置、文件同步模块配置、安全浏览模块配置、安全 FTP 模块配置及邮件访问配置，以及其他一些辅助工具的配置，如导入、导出配置、查看系统状态等功能。

7) 日志审计

产品提供完善的日志记录和审计功能，日志分为配置管理日志和业务运行日志两大类，方便审计员对该设备的运行和配置情况进行审计。日志审计提供按条件审

计、删除、备份等功能。

1.4 功能列表

分类	特性/功能	主要功能描述
产品架构	国产化硬件体系架构	基于飞腾硬件平台及麒麟操作系统
	硬件架构	采用“2+1”模块结构设计，即包括外网主机模块、内网主机模块和隔离交换模块；内外端机为网络协议终点，彻底阻断各种网络协议，保证信任网络和非信任网络之间链路层的断开，彻底阻断 TCP/IP 协议以及其他网络协议；自主研发的基于安全芯片的专用隔离部件，无操作系统，外部无法编程控制，全硬件交换；内外网主机系统与专用隔离部件之间采用高性能 PCI-E 总线连接，消除性能瓶颈
	系统架构	支持双系统冗余架构，可通过 WEB、console 口进行主备系统切换，当主系统发生故障可切换至备系统进行工作；
管理维护	安全管理	提供基于 https 的图形化安全管理，支持用户名/口令、数字证书、U-KEY 等多种认证以及用户名/密码+U-KEY、用户名/密码+数字证书双因子认证方式； 支持带内管理，可通过业务口进行网闸管理工作；用户可自行选择是否启用带内管理功能；支持管理员登录失败锁定次数、锁定时间和超时时间的设定
	集中监控	支持集中监管平台，可对多台网闸进行统一监控，记录每台设备的系统资源运行情况； 支持自定义告警策略，可通过自定义方式设置监控对象各项指标告警阈值； 支持多种告警方式，如弹框告警、邮件告警、SNMPTrap、syslog 告警等；

		<p>集中监管告警信息支持 XML、CSV、XLS 等多种格式导出；</p>
	<p>便捷运维</p>	<p>支持配置管理，能够对单独模块及全部模块配置进行配置导入导出</p> <p>具有系统补丁管理功能</p> <p>支持设备诊断信息导出</p> <p>支持许可证下载，方便维护管理</p> <p>支持 NTP 网络时间同步</p> <p>提供调制工具，其中包括：trace、connect、tcpdump、ping、arp 等</p> <p>提供设备运行状态检测、系统资源监控</p> <p>支持对网络接口模式进行设定（支持网闸同一侧网络接口桥模式设定或 bonding 设定）、MTU 修改，进行灵活部署</p> <p>支持默认路由、静态路由及基于源地址的策略路由功能</p> <p>支持 IP/MAC 地址绑定和自动探测</p>
<p>功能模块</p>	<p>文件交换</p>	<p>支持通过客户端或无客户端两种方式实现高效安全的文件交换；</p> <p>支持 NFS、SMB、FTP 等多种文件传输协议实现文件同步。</p> <p>支持不同文件传输协议之间的文件同步；</p> <p>支持多种同步模式：完全一致、完全复制、首次复制+新增、源端移动、源端删除等多种模式。</p> <p>支持子目录同步控制和二进制文件同步控制。</p> <p>提供关键字、黑白名单信息过滤，发送白名单、发送黑名单、接收白名单、接收黑名单等多种组合控制方式。</p> <p>支持文件名及后缀名过滤，同时支持文件类型识别过滤，即不基于后缀名的过滤。</p>

		<p>文件安全策略细分到任务，可按需配置全局任务或细分任务；</p> <p>支持病毒检测功能；</p>
	<p>数据库同步</p>	<p>支持 Oracle、SQL Server 等多种主流数据库同步</p> <p>支持达梦、人大金仓、神通等国产数据库同步；</p> <p>支持客户端、无客户端多种部署方式实现数据库同步；</p> <p>无客户端方式同步由网闸主动发起并完成，不需要第三方软件支持（无需在数据库安全任何第三方软件），支持 windows、linux、unix 等多种数据库操作系统类型。</p> <p>支持异构数据库同步，实现不同表结构和不同数据库类型之间的转化</p> <p>支持周期复制、实时复制、增量更新等多种同步方式。</p> <p>支持大字段和二进制字段的数据同步</p> <p>支持字段级同步</p>
	<p>邮件访问</p>	<p>支持 SMTP、POP3、IMAP 等邮件协议；</p> <p>支持垃圾邮件过滤，支持对邮件地址、主题、内容及附件关键字过滤</p> <p>支持对邮件的数字签名</p> <p>能够对邮件访问的源/目的地址、端口进行访问控制</p> <p>支持病毒检测功能；</p>
	<p>数据库访问</p>	<p>支持 SQL、ORACLE、DB2、SYBASE、POSTGRESQL 等主流数据库的访问</p> <p>支持达梦、人大金仓、神通等国产数据库访问</p>

		<p>支持 ORACLE、SQL SERVER 访问用户名过滤、数据库命令控制、数据库库名控制、数据库表控制，可以根据用户与数据库表对应关系，进行相应数据库操作过滤；</p>
	<p>FTP 模块</p>	<p>支持透明模式、代理模式及混合模式多种部署方式实现安全的 FTP 访问；</p> <p>支持 FTP 主动、被动工作模块转换</p> <p>支持对访问用户的限制</p> <p>不仅支持传输文件扩展名过滤，而且可以根据文件内容识别进行文件类型过滤。</p> <p>支持 PORT 命令端口范围控制</p> <p>支持传输文件中文件名控制</p> <p>支持 FTP 访问命令过滤</p> <p>支持访问时间控制</p> <p>支持对访问的 FTP 服务器地址的重定向</p> <p>支持病毒检测功能；</p>
	<p>安全浏览</p>	<p>支持代理模式、透明模式多种部署方式实现安全的网页浏览；</p> <p>支持 URL 后缀黑白名单控制</p> <p>支持 MIME 类型细粒度控制，如网页中的应用程序、视频、音频、图像、文本等进行细粒度控制</p> <p>支持对 HTML 细粒度控制，如网页中的 Script 脚本、ActiveX 脚本、java applet、cookie 等</p> <p>支持 HTTP 方法控制，如 POST、GET、HEAD、CONNECT 等。</p> <p>支持断点续传控制（提供功能截图）</p> <p>支持用户名口令认证、LDAP、RADIUS 等多种认证方式</p> <p>支持用户上网的 IP 控制</p>

		<p>支持用户上网时段限制</p> <p>支持病毒检测功能</p>
	定制模块	<p>支持基于标准 TCP/UDP 协议的定制服务；支持源地址绑定、网络接口地址绑定功能；支持源地址、源端口、目的地址、目的端口过滤功能；</p> <p>支持组播的定制服务，支持广泛的基于 TCP/UDP 视频应用</p>
	视频传输	<p>阻断视频专网与其他专网之间的所有通信协议，保证视频专网与其他专网之间的网络隔离。</p> <p>对视频数据与控制信令严格区分，分别处理后进行传输。支持视频数据双向传输模式和控制信令双向传输模式。</p> <p>提供视频信令协议格式、视频传输协议格式及主流视频监控公司的私有协议视频信令协议格式等。</p>
安全 审计	日志审计	<p>具有详细的日志审计功能，独立的审计用户；</p> <p>日志支持标准 Syslog、FTP 方式日志外发；</p> <p>支持多种日志导出格式，html、txt、cvs；</p> <p>支持数据轨迹查询，可以查询、追溯摆渡数据的源与目的；</p>
	告警中心	<p>提供告警，支持声音告警、邮件告警、trap 等告警方式；</p> <p>支持多种告警类型：病毒告警、攻击告警、硬件异常、系统异常、资源异常、配置变化、日志告警</p>

<p>可靠性</p>	<p>双机负载</p>	<p>支持双机热备及超过双机的多机热备功能</p> <p>支持宕机切换、拔线切换等多种切换机制</p> <p>支持 ping、connect 等多种主动链路探测，发现异常便实现主备切换，</p> <p>支持双机配置同步功能，可将主闸配置主动同步到备闸，方便配置管理</p> <p>支持多机（最多 32 台）负载均衡，支持负载分担、负载信息查看、自动切换、自动恢复等。</p> <p>支持端口和链路的冗余：无需其他设备支持和配合，实现了在一条链路故障时，业务能够切换到另一条链路上。</p>
<p>攻击防御</p>	<p>病毒防护</p>	<p>支持双引擎病毒模块，可根据用户需求选择需要的病毒引擎；</p> <p>支持在线升级、离线升级等病毒库升级方式。可针对文件交换、安全浏览、FTP 访问、邮件访问等多种模块进行病毒防护。</p> <p>支持私有云病毒联动查杀；</p>
	<p>入侵检测</p>	<p>支持入侵检测功能，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。</p>
	<p>弱口令防护</p>	<p>支持弱口令防护功能，针对网闸隔离保护的服务器，防止暴力破解密码；</p> <p>支持防护阈值设置、防护动作设置，可以根据阈值设置条件，自动触发防护动作；</p> <p>防护动作可自定义永久、时间锁定等</p>
	<p>攻击防护</p>	<p>支持 tcp flood、udp flood 攻击防护；</p> <p>支持设定防护范围，根据地址、端口、每秒最大连接数、每秒包个数等参数，并在触发范围时，自动触发防护动作；</p> <p>防护动作可自定义永久、时间锁定等；</p>

4. 产品型号与指标

国产化系列 银河麒麟+飞腾			
新型号		GZ3000-FT20	GZ10000-FT20
性能 指标	吞吐量	≥2Gbps	≥9Gbps
	高清最大并发数	≥500 路	≥2000 路
	标清最大并发数	≥900 路;	≥3500 路;
	视频数据误码率	<0.05%	<0.05%
	视频流传输时延	<50ms	<50ms
	延时	<2ms	<2ms
	MTBF (小时)	50,000	50,000
	接口	网络口	内网接口: 4 个千兆电口, 4 个千兆 SFP 光口插槽, 2 个扩展槽 外网接口: 4 个千兆电口, 4 个千兆 SFP 光口插槽, 2 个扩展槽
管理口		2	2
HA 口		2	2

	console 口	2	2
	USB 口	4	4
硬件配置	CPU	飞腾 FT20	飞腾 FT20
	内存	32GB	64GB
	操作系统	麒麟	麒麟
硬件特性	机箱	标准 2U 机箱	标准 2U 机箱
	重量 (KG)	15.2	15.2
	液晶面板	支持	支持
	电源	冗余电源	冗余电源

