**产品白皮书**

**360 安全隔离与信息交换系统**

**本文档解释权归 360 企业安全集团所有**

**目 录**

[1.产品概述 3](#_bookmark0)

[2.产品特点 3](#_bookmark1)

[3.主要功能 5](#_bookmark2)

[4. 产品资质 8](#_bookmark3)

[4.1 产品资质 8](#_bookmark4)

[4.2 产品荣誉 9](#_bookmark5)

# 1.产品概述

360安全隔离与信息交换系统能够有效实现内外网络的安全隔离，数据只能以专有数据块 方式静态的在内外网络间进行“摆渡”，从而切断了内外网络之间的所有直接连接，保证内外 网数据能够安全、可靠地交换。该系统可广泛应用于政府、企业、军队、电力等需要实施网络 安全隔离和数据交换的场合。

# 2.产品特点

**安全高效的体系架构**

360 安全隔离与信息交换系统采用“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、外网主机模块具有独立运算单元和存储单元，分别连接可信及不 可信网络，对访问请求进行预处理，以实现安全应用数据的剥离。隔离交换模块采用专用的双 通道隔离交换卡实现，通过内嵌的安全芯片完成内外网主机模块间安全的数据交换。内外网主 机模块间不存在任何网络连接，因此不存在基于网络协议的数据转发。

**专用的隔离交换模块**

网闸产品核心部件为隔离交换模块，360 安全隔离与信息交换系统隔离交换模块基于专用 安全芯片设计，全硬件交换；360 隔离交换模块是业界首家研发并使用高效 PCI-E 接口的交换 模块，此交换模块采用 PCI-E x4 通道设计，单向最高带宽大约是 10Gbps，消除性能瓶颈；360 隔离交换模块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。

**操作系统安全可靠**

内外网主机模块采用专用的 360 自主研发的多核并行安全加固操作系统 SecOS2，此系统 具备强大的抗攻击能力，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。同时，360 网闸采用双系统冗余架构，可平滑在主备系统之间进行切换，当 主系统出现问题时，可切换至备系统继续工作，保证业务系统的可持续运行。

**IPV4/IPV6 双协议支持技术**

360 网闸全面支持 IPV4 和 IPV6 双栈接入各类网络环境，支持通过 IPV4 和 IPV6 协议管理

网闸，无需改变现有网络设备和结构，即可实现 IPV4 和 IPV6 网络间的相互通信。

**业界唯一安全高效的数据库同步技术**

360 数据库同步模块，采用业界唯一内嵌数据库同步模块设计，数据库同步由网闸主动发 起并完成，不需要第三方软件支持。优势一：数据库同步请求完全由网闸主动发起，网闸无需 开发任何端口，更具安全性；优势二：无需在内外端机数据库服务器上安装任何软件，对数据 库服务器性能无任何影响，对数据库服务器本身运行的应用程序不存在任何兼容性问题。

**业界唯一融合加密、认证、授权多安全技术于一身的网闸产品**

360 网闸通过专用 SSL 通道客户端拨入，拨入链路通过 SSL 协议进行加密，认证通过后， 结合拨入终端应有的权限，对拨入用户进行授权，即为此终端用户应具有的访问权限，通过授 权防止方法用户的非法访问。认证保证终端用户访问身份的合法性、加密保证数据传输的私密 性、授权保证终端用户访问业务系统的合法性、加之网闸固有的协议转换、双通道结构等众多 安全特性，最大程度保证高安全域网络的安全性。

**灵活多样的认证方式**

360 网闸针对不同的用户需求设计了多种认证方式，包括：地用户名及口令认证、U-Key 认证、基于数字证书的认证、RADIUS 远程访问认证及 LDAP 认证以及多方式结合的双因子认证。 多样化的认证方式保证业务系统的合法访问。

**强大的网络适应能力**

360 网闸针对不同的软件模块具有多种部署方式，支持代理方式、透明方式等多种部署方 式，可以根据用户网络的特殊性采用不同的实现方式进行灵活部署。

**深度应用层解析过滤能力**

360 网闸针对 HTTP 协议、FTP 协议、POP3 协议、SMTP 协议、TNS 协议等多种应用层协议 进行深度解析及过滤，满足用户安全性需求。

**深度应用层攻击防御能力**

360 网闸具有防病毒功能模块，针对文件交换模块、FTP 访问模块、安全浏览模块、邮件 访问模块具有防病毒功能，能够支持本地升级及远程升级。360 网闸防病毒模块基于差异化病 毒库的理念，采用双引擎设计，用户可根据自身特点选择采用不同的防病毒引擎进行防护。

360 网闸具有入侵检测功能，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。

**强大的网络适应能力**

360 网闸具有多种功能模块，用户可以根据网络需求选用相应的功能模块；360 网闸每个 功能模块具有多种实现方式，用户可以根据网络需求选用相应的实现方式。如：文件交换模块 支持 FTP、SMB、NFS 等多种文件传输协议，支持无客户端方式及有客户端方式等；360 网闸双 机热备、负载均行功能通讯接口可以设置为 HA 接口、网络接口等，支持宕机切换、抜线切换， 支持 ping、connect 等多种主动链路探测，可以适应各种复杂的双机及负载网络环境需求；

**丰富的应用模块**

360 安全隔离与信息交换系统采用模块化的系统结构设计，根据不同的应用环境，量身定 制多个功能模块，以满足用户的不同需求。

# 3.主要功能

|  |  |  |
| --- | --- | --- |
| **分类** | **特性/功能** | **主 要 功 能 描 述** |
| **产品 架构** | **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 PCI-E 总线连接，消除性能瓶颈 |
| **系统**  **架构** | 采用基于 linux 内核的多核并行安全操作系统 SecOS2，支持软硬件多核 技术；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 等多种认证管理方式;  支持用户名/密码+U-KEY、用户名/密码+数字证书多种双因子认证方式； 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 监管** | 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； 集中监管告警信息支持 XML、CSV、XLS 等多种格式导出； |
| **便捷 运维** | 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 具有系统补丁管理功能  支持设备诊断信息导出 支持许可证下载，方便维护管理 支持 NTP 网络时间同步  提供调制工具，其中包括：trace、connect、tcpdump、ping、arp 等  提供设备运行状态检测、系统资源监控 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 支持默认路由、静态路由及基于源地址的策略路由功能  支持 IP/MAC 地址绑定和自动探测 |
| **功能 模块** | **文件 交换** | 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；  支持 NFS、SMB、FTP 等多种文件传输协议实现文件同步。 支持不同文件传输协议之间的文件同步；  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。  支持子目录同步控制和二进制文件同步控制。  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。 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。  支持病毒检测功能； |
| **数据库 同步** | 支持 Oracle、SQL Server 等多种主流数据库同步 支持客户端、无客户端多种部署方式实现数据库同步； 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。 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 支持周期复制、实时复制、增量更新等多种同步方式。 支持大字段和二进制字段的数据同步  支持字段级同步 |
| **邮件 访问** | 支持 SMTP、POP3 等邮件协议； 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 支持对邮件的数字签名 能够对邮件访问的源/目的地址、端口进行访问控制 支持病毒检测功能； |

|  |  |  |
| --- | --- | --- |
|  | **数据库 访问** | 支持 SQL、ORACLE、DB2、SYBASE 等主流数据库的访问 支持达梦、人大金仓、神通等国产数据库访问 支持访问用户名过滤、ORCLE 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； |
| **FTP**  **模块** | 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； 支持 FTP 主动、被动工作模块转换  支持对访问用户的限制  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。  支持 PORT 命令端口范围控制 支持传输文件中文件名控制 支持 FTP 访问命令过滤  支持访问时间控制  支持对访问的 FTP 服务器地址的重定向 支持病毒检测功能； |
| **安全 浏览** | 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； 支持 URL 后缀黑白名单控制  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  支持对 HTML 细粒度控制，如网页中的 Script 脚本、ActiveX 脚本、java applet、cookie 等  支持 HTTP 方法控制，如 POST、GET、HEAD、CONNECT 等。  支持断点续传控制（提供功能截图） 支持用户名口令认证、LDAP、RADIUS 等多种认证方式 支持用户上网的 IP 控制  支持用户上网时段限制 支持病毒检测功能 |
| **定制**  **模块** | 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； 支持组播的定制服务，支持广泛的基于 TCP/UDP 视频应用 |
| **SSL 通道** | 支持 SSL 隧道访问模式，针对 FTP 访问模块、数据库访问模块、邮件访  问、定制模块等模块，通过网闸实现访问客户端认证、授权及访问链路 加密，保证客户端访问合法性及访问链路的安全性。认证方式支持用户 名口令认证及证书认证。 |
| **SOCKS 代理** | 支持 Socks4、Socks5 版本代理功能； 支持本地用户认证、radius 等认证方式； 能够实现基于源地址、目的地址、源端口、目的端口的访问控制 |

|  |  |  |
| --- | --- | --- |
| **安全 审计** | **日志 审计** | 具有状态日志审计功能，能够对 CPU、内存、设备信息、许可证信息、  运行时间、交换卡状态、网络接口状态、功能模块运行状态等进行阀值 设定并基于阀值进行日志审计。  具有独立审计用户，支持标准 Syslog 日志审计方式，支持 Syslog 端口 自定义  支持标准的 SNMP 协议安全管理 支持状态日志配置，通过设置硬件信息使用率进行日志记录及暂停使用 |
| **告警中心** | 设备提供告警，支持声音告警、邮件告警等告警方式 |
| **可靠性** | **双机 负载** | 支持双机热备及超过双机的多机热备功能 支持宕机切换、抜线切换等多种切换机制  支持 ping、connect 等多种主动链路探测，发现异常便实现主备切换， 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  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。 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。 |
| **攻击 防御** | **防护 设置** | 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； 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。 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。  抗 Dos 攻击功能设置 ICMP 应答功能设置 |

# 4. 产品资质

## 4.1 产品资质

 公安部计算机信息系统安全专用产品销售许可证(三级)

 国家保密局涉密信息系统产品检测证书

 国家信息安全测评信息技术产品安全测评证书（EAL3+）

 军用信息安全产品认证证书（军 B 级）

 中国国家信息安全产品认证证书（二级）

 公安部安全与警用电子产品质量检测中心（GB/T28181-2011）

 参与《军用网络安全隔离交换产品通用要求》标准编制，具有证明文件

 计算机软件著作权登记证书

 多核并行安全操作系统软件著作权证书

 国家应用安全联盟会员

## 4.2 产品荣誉

 北京市自主创新产品证书

 军用隔离产品标准编制成员

 2016 中国网络安全市场年度创新产品奖

 基于国产 CPU 的高性能安全隔离网关立项证书