

# HK-ISG-B17108 工业防火墙(1U 机架式/企业级)技术规格书

## 一、设备概述

本设备为 1U 机架式企业级工业防火墙，专为策克口岸中兴海关监管场场景设计，核心用于实现监管场现场计量数据（如地磅称重数据）、理化检验数据（如成分分析报告）的安全传输——通过公网链路接入酒钢内网管理系统，同时提供边界防护、数据隔离、协议适配等功能，保障工业数据传输的安全性、稳定性与合规性。

## 二、核心技术功能

### （一）边界安全防护

1. 支持状态检测防火墙技术，基于五元组（源 IP、目的 IP、源端口、目的端口、协议）对数据包进行实时检测，拦截非法访问请求，访问控制准确率 $\geq 99.8\%$ 。

2. 集成入侵防御系统（IPS），覆盖工业控制领域常见攻击（如 Modbus 协议异常指令、SCADA 系统数据篡改），攻击识别准确率 $\geq 99.5\%$ ，误报率 $\leq 0.1\%$ 。

3. 提供 DDoS 防护能力，支持对 SYNflood、UDPFlood、ICMPFlood 等常见 DDoS 攻击的检测与清洗，防护带宽 $\geq 100\text{Mbps}$ ，攻击响应延迟 $\leq 100\text{ms}$ 。

### （二）数据安全传输

1. 支持多协议 VPN 加密，包括 IPsecVPN（隧道加密）、SSLVPN（远程接入）、L2TPVPN（跨网接入），加密算法覆盖 AES-256（数据加密）、SHA-256（身份认证），确保公网传输数据不被窃取或篡改。

2. 内置数据防泄漏（DLP）模块，可对计量数据、检验报告等敏感数据进行规则化识别（支持关键字匹配、文件格式匹配），禁止未

授权敏感数据外传，数据拦截响应时间≤50ms。

3. 实现数据传输完整性校验，通过 CRC32（快速校验）、MD5（深度校验）等算法验证数据接收端与发送端的一致性，避免数据传输丢包或损坏，校验成功率 100%。

（三）工业协议适配

1. 原生支持工业控制协议解析与防护，覆盖 Modbus-RTU/TCP、Profinet、EtherNet/IP、OPCUA/DA、DNP3 等主流工业协议，可识别协议字段异常、指令越权等风险行为。

2. 提供协议转换功能，支持将监管场计量设备的串口协议（如 RS485/RS232）转换为 TCP/IP 协议，适配公网传输链路，协议转换延迟≤20ms，转换成功率 100%。

3. 支持工业数据优先级调度，可将计量数据、检验数据等核心业务数据设置为高优先级，非核心数据（如设备状态查询）设为低优先级，保障关键业务数据传输无延迟。

（四）细粒度访问控制

1. 基于角色（RBAC）与策略（ACL）的双重访问控制，可按“酒钢部门-监管场岗位-终端设备”三维度划分权限，仅允许酒钢内网管理系统指定 IP 段访问监管场数据节点，权限配置生效时间≤30s。

2. 支持时间策略管控，可设置数据传输的合法时间段（如仅 8:00-18:00 工作时间允许公网接入），非授权时段自动阻断公网链路，减少安全暴露风险。

3. 提供终端准入控制（EAC），仅允许已注册、合规（如安装指定杀毒软件、系统补丁版本达标）的计量设备/检验终端接入网络，未合规终端拦截率 100%。

三、硬件参数规格

| 类别 | 参数要求 | 备注 |
|----|------|----|
|----|------|----|

| 类别   | 参数要求                                       | 备注                   |
|------|--|----------------------|
| 外形规格 | 1U 机架式, 尺寸 438mm(宽)×43.6mm(高)×280mm(深)     | 符合标准 19 英寸机架安装要求     |
| 重量   | 单机重量≤5kg                                   | 不含包装重量               |
| 供电方式 | 双冗余电源(100-240VAC, 50/60Hz), 支持热插拔          | 电源故障时自动切换, 切换时间≤10ms |
| 接口配置 | 8 个千兆电口(RJ45)、2 个千兆光口(SFP)、1 个 Console 管理口 | 电口支持链路聚合, 光口支持冗余备份   |
| 性能指标 | 吞吐量≥2Gbps, 并发连接数≥100 万, 每秒新建连接数≥3 万        | 满负载下设备运行温度≤40℃       |
| 存储扩展 | 支持 1 个 MiniPCIe 插槽(可扩展 SSD), 最大支持 1TB 存储   | 用于本地日志存储、配置备份        |
| 冗余设计 | 支持端口冗余(LACP 链路聚合)、电源冗余, 无单点故障              | 保障设备连续运行, 无业务中断风险    |

#### 四、软件与管理特性

(一) 管理界面: 提供 Web 图形化管理界面(支持 HTTPS 加密访问)与 CLI 命令行管理, 支持中英文界面切换, 操作响应延迟≤1 秒, 适配 Chrome、Edge、Firefox 等主流浏览器。

(二) 日志与审计: 支持本地日志(存储容量≥10GB, 可保存 180 天日志)与远程日志(支持 Syslog 协议对接酒钢内网日志服务器), 可生成安全事件、数据传输、设备状态等标准化审计报表(支持 Excel/PDF 导出)。

(三) 高可用性: 支持 HA 双机热备(主备模式), 主设备故障时自动切换至备设备, 故障切换时间≤300ms, 确保业务不中断, 切换

过程无需人工干预。

（四）固件升级：支持在线固件升级（HTTP/HTTPS 协议），升级过程不中断数据传输，支持升级版本回滚（升级失败时自动恢复至原版本），升级成功率 100%。

## 五、环境适应性

（一）工作温度：0℃~45℃（无冷凝），温度波动范围 $\leq \pm 5^{\circ}\text{C}/\text{h}$ ，设备在极限温度下运行稳定，无性能下降。

（二）存储温度：-40℃~70℃，湿度 $\leq 85\%$ （非凝露），存储期 $\geq 12$ 个月，恢复工作后无功能异常。

（三）相对湿度：5%~95%（非凝露），湿度突变范围 $\leq \pm 10\%/\text{h}$ ，设备无凝露、无部件腐蚀风险。

（四）抗电磁干扰：符合 GB/T17626.2-2006（静电放电抗扰度，接触放电 $\pm 6\text{kV}$ ，空气放电 $\pm 8\text{kV}$ ）、GB/T17626.3-2006（射频电磁场辐射抗扰度，10V/m）标准，电磁干扰下设备无数据丢包、无功能异常。

（五）抗震等级：符合 GB/T2423.10-2019（正弦振动，频率10~55Hz，加速度 $50\text{m}/\text{s}^2$ ）要求，振动环境下设备连接稳定，无部件松动。

## 六、合规性要求

（一）符合《信息安全技术防火墙技术要求》（GB/T20281-2015）二级及以上标准，通过国家信息安全等级保护测评机构检测。

（二）符合《工业控制系统信息安全防火墙技术要求》（GB/T37952-2019）要求，适配工业场景安全防护需求。

（三）支持海关监管数据传输相关合规要求，可提供第三方检测机构出具的设备安全合规检测报告（检测项目含数据加密、访问控制、日志审计）。

## 七、附录

附录 1 设备接口定义表

| 接口标识      | 接口类型       | 核心功能   | 技术参数  | 连接要求   | 备注                       |
|-----------|------------|--|---|--|--------------------------|
| ETH0~ETH7 | 千兆电口（RJ45） | ETH0~ETH3：连接策克口岸监管场计量设备（地磅、成分分析仪）、理化检验终端；ETH4~ETH7：连接酒钢内网侧交换机或管理终端设备 | 速率：10/100/1000Mbps 自适应；标准：IEEE802.3u/802.3ab；模式：全双工/半双工自动切换、MDI/MDI-X 自动翻转      | 推荐使用超五类及以上非屏蔽双绞线（CAT5e+UTP）；单链路传输距离≤100米；ETH4~ETH7支持 LACP 链路聚合 | 电口均支持防雷击（接触放电±6kV）、防浪涌保护 |
| SFP0~SFP1 | 千兆光口（SFP）  | SFP0：连接公网链路（运营商光纤）；SFP1：备用公网链路或酒钢内网核心节点冗余连接                          | 速率：1000Mbps（固定）；光模块兼容性：单模（SM）/多模（MM）；单模传输：≤20km（1310nm 波长）；多模传输：≤550m（850nm 波长） | 单模链路：使用 G.652 标准单模光纤（纤芯直径 9/125 μm）；多模链路：使用 OM3 及以上多模光纤（纤芯直径   | 光口支持光功率监测，可实时查看链路信号强度    |

| 接口标识      | 接口类型            | 核心功能                                       | 技术参数   | 连接要求  | 备注                                 |
|-----------|-----------------|--|--|---|------------------------------------|
|           |                 |  |  | 50/125 μ m )；需搭配符合 SFP 协议的千兆光模块   |                                    |
| CONSOLE   | 串口（RJ 45 转 DB9） | 设备本地配置管理：通过串口线连接笔记本或配置终端，进行初始化设置、故障排查、版本回滚 | 接口标准：RS-232；波特率：9600~115200bps（默认 9600bps）；数据位：8；停止位：1；校验位：无 | 需使用 RJ45 转 DB9 串口线（线序：T568B）；仅支持本地物理连接，不支持远程访问；配置终端需安装串口工具（如 SecureCRT、PuTTY） | 仅用于设备维护，无数据传输功能；维护完成后建议断开连接，降低安全风险 |
| PWR1~PWR2 | 电源接口（AC）        | 设备供电：PWR1 为主电源，PWR2 为冗余备份电源；电源状态指          | 输入电压：100~240VAC（宽幅适配）；工作频率：50/60Hz；最大功耗：≤30W；                | 需连接独立的市电回路（避免与大功率设备共回路）；推荐  | 支持热插拔，更换电源时设备                      |

| 接口标识 | 接口类型 | 核心功能                                 | 技术参数              | 连接要求   | 备注          |
|------|------|--------------------------------------|-------------------|--|-------------|
|      |      | 示灯<br>(PWR1/PWR2): 绿色常亮(正常)、红色常亮(故障) | 电源效率:<br>≥85%(满载) | 搭配 UPS 电源(后备时间≥30 分钟), 避免断电导致设备下线; 电源连接线需符合国标(铜芯线<br>≥1.5mm <sup>2</sup> ) | 正常运行, 无业务中断 |

八、其他要求

(一) 若\_\_\_\_\_单位不中标, 本技术规格书自动失效, 双方互不承担任何责任。

(二) 本技术规格书内容经由甲乙双方于 2025 年\_\_月\_\_日\_\_时通过\_\_\_\_\_方式商定。

(三) 甲乙双方应当就签订本技术规格书的相关事宜保密, 不得将签订主体、时间、内容等信息透露给其他第三方。

本规格书一式四份, 甲乙双方各执两份, 双方签署后生效。