工业防火墙

产品概述

工业防火墙是专用于工业网络中不同安全级别或不同网络安全域之间进行安全隔离防护的产品。产品主要基于对工业网络协议深度解析，利用机器学习技术识别工业资产和应用协议。结合白名单、黑名单、安全域划分、 IP/MAC 地址绑定等技术，抵御工业网络中各类已知和未知的恶意攻击行为，为工业网络中各类生产系统和业务系统的稳定运行提供安全保障。

产品特点

- 深度工业协议解析

支持对 OPC UA、OPC DA、SNMP、 Ethernet/IP、Modbus/ TCP、Profin、IEC104、DNP3、 MMS、S7、GOOSE、SV 等 10 多种常用工业协议深度解析，并支持自定义扩展私有协议。网络适应好

- 智能构建可信策略

通过流量自学习，建立可信的工 控网络安全策略基线，简化策略配置流程，降低人工部署难度，提高现场配置部署效率。简便性

- 强大的网络适应性

支持透明模式、路由模式、工作模式、测试模式。各模式间可快速切换，适应复杂的工业 网络环境要求，方便实施部署。

- 指令精准解析与控制

支持主流工业协议 Mod bus TCP、OPC、Profinet、DNP3 等多种工业控制网络协议的数据包深度解析与精准控制。

- 多重防护机制

具备传统网络 DoS/DDoS 恶意攻击防护能力，并基千工控威胁特征识别技术、黑名单特征库匹配机制构建多重防护，抵御针对工控系统的各类攻击。

- 高可靠性

硬件设计中增加成对的 bypass 端口，遇设备掉电、宅机等情况仍能保障业务连续性。全系列产品标配双电源，确保设备供电稳定。采用无风扇设计，保障硬件长时间可靠运行。产品可灵活定制硬件接口并可按需拓展处理性能。

- 内置专业反病毒引擎

专业脱壳引擎及解压缩引擎，结合特征码扫描、启发式扫描及行为判断技术快速检测各种已、未知病毒威胁。支持对 JS、VBS、SH、Python、PHP、BAT 等多种格式的脚本进行扫描，快速准确检测 Shellcode 威胁。宏病毒引擎可清除 Office 文件中的恶意宏代码，正确修复文档。

典型部署

串联部署在现场监控网与生产管理网之间串联部署在工控网络内部核心控制系统出口

江南三体河北信息安全技术有限公司

地址：河北省廊坊市广阳区友谊路462号

网址：http://www.stiot.net

邮箱：jnst@jnsanti.net