AVCOMM™恩创®

工业防火墙S5500系列
Datasheet

恩创致力于将先进的信息技术带入工业控制与工业信息领域。

安通恩创信息技术（北京）有限公司 www.avcomm.cn

电子邮箱: sales@n-tron.com.cn

电话： （010）- 82859971

地址：北京市海淀区马甸东路19号金澳国际公寓3105

恩创工业防火墙（S5500）系列产品

产品概述

随着中国制造2025计划、互联网+和工业4.0的不断推进，工业互联网时代已经到来，IT和OT已经深度融合，越来越多的工控设备接入到互联网，导致传统安全威胁可以迅速渗透到工业网络中，危害工控系统的正常运行。办公信息网与控制网络之间的访问隔离、工业互联网出口的安全威胁防护已经成为当前工业网络安全整体方案中不可忽略的关键点。通过具备多种威胁防御的一体化安全网关产品，在第一时间发现来自外 部的安全风险，感知工业网络核心设施的威胁态势，构建纵深防御的工业网络安全体系成为重要的发展趋势。

恩创S5500系列工业防火墙基于自主可控的操作系统和高性能硬件平台，采用访问控制、入侵防御、病毒过滤等融合的安全技术，重点监控工业网络中互联网边界、MES层边界的网络流量，发现并阻 断已知和未知的网络攻击行为，保护工业网络内部核心设施，从而构建可管、可信和可视的工业网络系统， 为工业用户提供安全智能的边界安全防护方案。

工业防火墙S5510

工业防火墙S5520

工业防火墙S5530

工业防火墙S5550

产品特点

深度业务感知，工业流量可视化及资产管理

通过自主研发的深度数据包解析引擎，恩创工业防火墙能够检测出AB、Siemens、 Emerson、GE、OMRON、Yokogawa、Honeywell、Schneider等主流厂商的100+的工控协议和工控设 备类型，基于协议和设备类型实现工业流量的可视化和资产管理。

丰富网络特性，适应复杂工业环境复杂网络

恩创工业防火墙基于高性能硬件平台和智能工控安全操作系统（IICS-OS），融合了丰富的网络 特性，在满足IPv4/IPv6双协议栈的同时，配合DDNS、智能路由、链路负载均衡、服务器负载均衡等特性，

可在802.1Q、GRE 、RIP、OSPF、VRF、多ISP等各种复杂的工业网络环境中灵活组网，也更符合工业互联网时代的业务发展趋势。

一体化检测引擎，全面精准防御安全风险

恩创S5500系列工业防火墙集成了访问控制、负载均衡、入侵防御、病毒过滤、VPN接入、 威胁可视化等功能，能够为工业用户提供一个灵活、高效、全面的边界安全解决方案。

通过超过4000种预定义的攻击特征库、攻击特征自定义能力、高性能病毒检测引擎和报文的深度还原 解析技术，S5500系列工业互联防火墙具备从数据链路层到应用层的入侵攻击防御和已知/未知病毒实时 检测拦截能力，从而有效的阻断针对工业网络有目的的攻击行为，全方位保护工业网络中的核心设施，保障 工业生产系统持续运行。

功能规格

网络基础功能

- 支持透明网桥、路由、旁路、混合部署
- 支持源地址、目的地址NAT，支持一对一、一对多、多对多地址转换
- 支持链路负载均衡和服务器负载均衡
- 支持支持静态路由、动态路由(RIP\OSPF\BGP)、策略路由、应用路由、智能选路、VRF路由
- 支持IPv4及IPv6特性

入侵防御

- 内置4000多条入侵攻击规则库，支持自定义规则
- 支持拒绝服务、木马后门、间谍软件、蠕虫病毒、缓冲区溢出、安全扫描等网络层攻击防护
- 支持HTTPS防护、DDoS攻击、Web攻击、0-day攻击、CGI攻击等应用层攻击防护

Web攻击防护

- 支持SQL注入、系统命令注入、LDAP注入、SSI注入、邮件注入、请求体PHP注入等注入式攻击
- 支持检测恶意攻击者对WEB站点的扫描行为
- 支持会话劫持检测、木马检测等攻击防护
- 支持OWASP TOP10威胁的防护

工业协议识别

- 100+工业协议识别
- 工业流量可视化

访问控制

- 基于7元组以及时间的访问控制策略
- 基于应用+行为+动作+关键字的四维访问控制
- 基于URL分类的访问控制

威胁可视化

- 基于用户、应用的流量趋势统计、分布统计和TOP排名
- 基于设备CPU、内存、转发流量、会话数趋势统计，接口状态展示
- 支持对IPS事件，DDoS攻击时间，AV事件的趋势图统计
- 基于网络状态，用户行为，网络安全多种维度生成的审计报表
- 支持审计防火墙的操作日志
- 支持攻击防护日志，IPS日志，AV日志；

用户管理

病毒防护

- 支持HTTP，FTP，POP3，SMTP，IMAP协议的病毒查杀
- 支持查杀最高压缩20层ZIP/RAR等压缩文件
- 支持300万余种病毒查杀，病毒库定期更新

流量管理

- 支持虚拟线路和分级带宽管理，支持4级通道嵌套
- 支持基于用户/应用/服务/IP/时间的带宽限制
- 支持每IP限速、带宽保障和多优先级管理
- 支持三权分立的用户管理模式
- 支持树形结构展示用户组织结构
- 支持在线用户状态显示
- 支持SNMP、ARP扫描、Radius、LDAP等方式同步用户

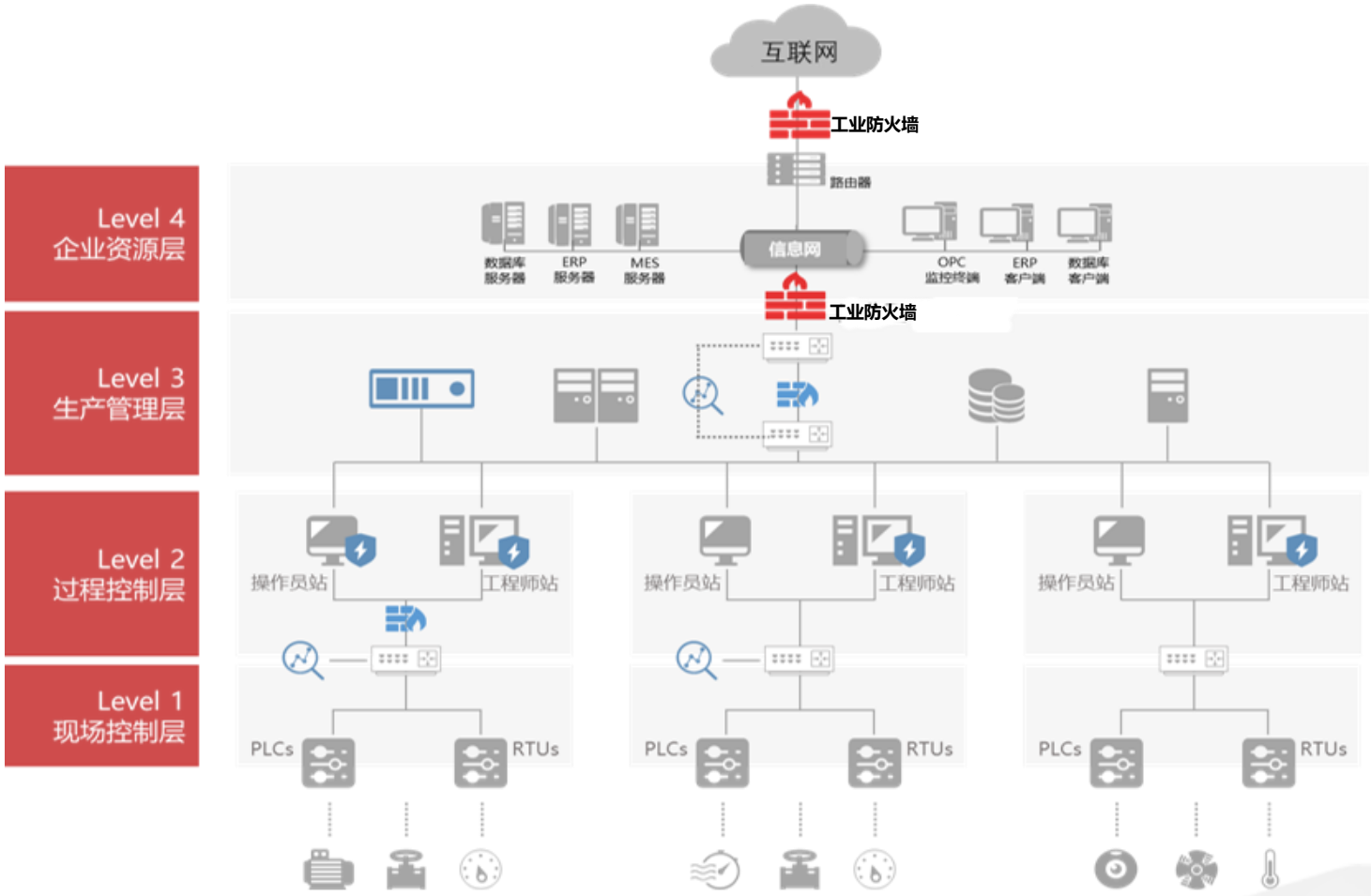
用户认证

- 本地认证：Web 认证、用户名/密码认证
- 第三方认证：RADIUS、LDAP等
- 支持短信认证、APP认证、微信认证、混合认证

详细规格

存储	500G 企业级 HDD	500G 企业级 HDD	500G 企业级 HDD	1T 企业级 HDD
业务接口	6*千兆 RJ45	2GE(Combo)+ 10*千兆 RJ45	12*千兆 RJ45+12*千兆 SFP	12*千兆 RJ45+12*千兆 SFP +2*万兆 SFP
Bypass	无	1 组	1 组	1 组
管理接口	任一业务接口	任一业务接口	专用带外管理 1*千兆 RJ45	专用带外管理 1*千兆 RJ45
串口	1*Console	1*Console	1*Console	1*Console
USB 接口	1*USB	1*USB	1*USB	1*USB
MTBF	10 万小时	10 万小时	10 万小时	10 万小时
输入电流	1 路 100-230V AC	1 路 100-230V AC	2 路 100-230V AC	2 路 100-230V AC
平均功率	15W	25W	120W	120W
宽*深*高	280*152*44mm	440*263*44mm	440*263*44mm	440*330*88mm
部署类型	桌面式部署	1U、机架式部署	1U、机架式部署	2U、机架式部署
工作环境	温度：5℃～45℃；湿度：20%～90%（非凝结）			
储存环境	温度：-10℃～70℃；湿度：5%～95%（非凝结）			

应用场景



工业互联网出口边界防护

- 以路由方式在线部署于工业网络互联网出口
- 抵御来自外部网络的入侵攻击行为，对网络中的病毒进行过滤查杀
- 网络带宽优化，保障关键应用和业务的带宽使用
- 支持VPN/MPLS/ VLAN/PPPoE/4G等复杂网络环境；
- 支持设备本地日志记录和集中分析处理，分布式部署统一管理

工控网络和信息网络边界隔离

- 以串行路由或者透明方式部署于MES层和办公信息网之间
- 对进入工控网络的访问行为进行检查和控制
- 阻止来自外部的安全威胁进入工控网络
- 集中管理运维，支持分布式部署统一管理

可销售部件

部件名称	描述
S5510	6 个千兆电接口，1U 高度，SOHO 机箱，配延长挂耳可上机架，网络吞吐率 2Gbps，并发连接：30 万，含防病毒、防攻击、上网 行为管理、Web 安全防护等增强特性授权；
S5520	2 个千兆 Combo 接口，10 个千兆电接口，1U 标准机架，网络吞吐率 2.5Gbps，并发连接：200 万，含防病毒、防攻击、上网行为 管理、Web 安全防护等增强特性授权；
S5530	12 个千兆电接口，12 个千兆光接口，1U 标准机架，冗余电源，网络吞吐率 8Gbps，并发连接数：300 万，含防病毒、防攻击、上网 行为管理、Web 安全防护等增强特性授权；
S5550	12 千兆电接口，12 千兆光接口，2 万兆 SFP+光口，2U 标准机架，冗余电源，网络吞吐率 10Gbps，并发连接数：500 万，含防 病毒、防攻击、上网行为管理、Web 安全防护等增强特性授权；
LIC-IPS-12	IPS 特征库 12 个月升级服务
LIC-AV-12	AV 病毒特征库 12 个月升级服务
LIC-URL-12	URL（含恶意 URL）和应用识别特征库 12 个月升级服务
LIC-WAF-12	WEB 攻击特征库 12 个月升级服务
LIC-IPS-36	IPS 特征库 36 个月升级服务
LIC-AV-36	AV 病毒特征库 36 个月升级服务
LIC-URL-36	URL（含恶意 URL）和应用识别特征库 36 个月升级服务
LIC-WAF-36	WEB 攻击特征库 36 个月升级服务
SSL-100	100 个 SSL VPN 用户数授权（缺省含 10 个用户数）
SSL-500	500 个 SSL VPN 用户数授权（缺省含 10 个用户数）
Centralized Manager	统一安全管理平台软件，支持工业互联防火墙和入侵检测系统
TEG-Bypass	外置光 BYPASS 设备，最大支持 4 路
Optic-GE-850nm	千兆多模光模块，850nm，100m
Optic-GE-1310nm-10KM	千兆单模光模块，1310nm，10KM
Optic-10GE-850nm	万兆多模光模块，850nm，100m