域智盾软件®

能源化工行业

网络准入控制解决方案



CONTENTS/目录

01 行业背景 ---------- 3

02 政策要求 ---------- 3

03 面临问题 ---------- 4

04 解决方案 ---------- 4

05 方案价值 ---------- 8

06 公司简介 ---------- 9

一、行业背景

随着两化融合推进，生产网与办公网之间的数据交换日益频繁，第三方运维、设备厂商现场服务、供应商与访客接入也成为常态。网络边界从传统的“围墙式”封闭，演变为需要对每一台接入设备做识别、校验与授权的精细化管理。

与此同时，勒索病毒、挖矿木马、非法外联等安全事件在能源化工行业多次发生，一旦生产网被非法终端接入并横向移动，可能影响 DCS、SCADA 等关键控制系统运行，造成停产、安全事故与监管责任。

二、政策要求

本方案对齐以下政策与标准要求：



另外，4.19 讲话强调“金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标”。“ 要全面加强网络安全检查，摸清家底、认清风险、找出漏洞、通报结果、督促整改。”

三、企业面临问题

- 入网设备身份不清晰：员工自带笔记本、运维人员设备、访客终端随意接入内网，缺乏统一认证与登记，网络中“有谁在线”无法准确掌握。
- 资产台账与现场不一致：IT 部门维护的 IP 表、设备清单与实际网络中活跃的终端存在较大偏差，事件发生后无法快速定位责任人。
- 违规外联与非法接入：办公终端私自接入生产网、员工电脑同时连接内外网，绕过了原本的网络隔离策略。
- 外来设备横向移动：第三方运维、设备厂商现场服务人员接入内网后可访问业务系统，操作范围与留存周期缺乏约束。
- IP 地址管理混乱：IP 冲突、私改 IP、跨网段接入频发，故障排查与事件溯源耗时。
- 长期离线与高风险设备无感知：已报废、长期不在线的终端仍保留网络权限，存在被冒用的风险。
- 缺乏统一视图：网络设备、服务器、办公终端、工控终端分散在多套系统中，安全团队无法在一张图上看清全网态势。

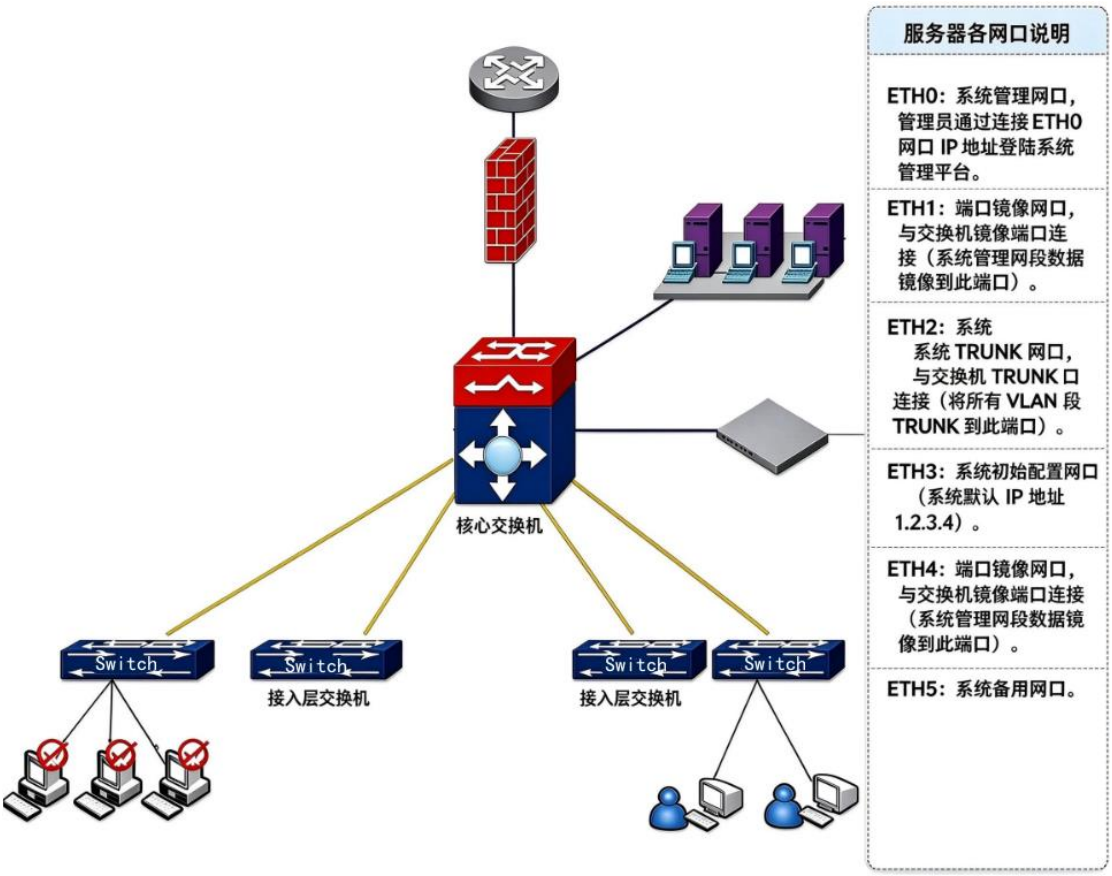
四、解决方案

本方案秉承“违规不入网，入网必合规”的理念，对能源化工企业内网中的每一台终端做识别、校验、授权与审计。

举例，某大型化工集团内网终端约 1500 台，月均收到 60 余起违规工单，涵盖 IP 冲突、私接路由器、外来设备接入等场景。违规事件发生后，IT 人员需要在交换机日志、门卫登记信息中人工比对，定位单台风险终端往往需要半天以上。如何快速定位、拦截风险？以下是域智盾软件的解决方案。

4.1 网络拓扑

系统采用旁路部署方式，在核心交换机镜像端口旁挂准入控制服务器，不改变现有网络拓扑，不串接业务流量。



4.2 核心功能

4.2.1 大屏展示

提供可视化大屏，集中展示全网资产数据分析、资产分类、安全趋势、24 小时态势、关键设备、在线终端数量、当日新入网与阻断事件等核心指标，为安全例会与应急指挥提供统一视图。

4.2.2 全网设备资产

自动采集并维护全网设备资产清单，展示 IP 地址、设备类型、操作系统、所属部门、MAC 地址、设备厂商、入网规则、最后活动时间。

支持按设备类型、部门、准入状态和关键设备的筛选选项，支持多条件组合查询，便于安全团队在数千台终端中快速定位目标设备，替代人工维护的 IP 表与设备台账。

4.2.3 查看设备事件

系统对全网资产安全态势做集中呈现，提供以下日志与视图：

- 新入网设备日志：记录报警主题、部门、基本信息、详细信息（如跟随 VLAN：拒绝入

网）；阻断设备日志：记录阻断设备、所属部门、所属 VLAN、详情、阻断方式、阻断事件；

- 安全风险设备日志：记录主体、部门、存在的高风险行为（私改 IP、变更系统等）、危险级别、报警时间。
- 设备信息变更日志：记录终端 IP 地址、MAC 地址、部门、事件详情、事件来源、发生时间。
- 关键设备离线日志：记录服务器、网络设备、工控终端等关键设备的离线事件。
- 关键设备风险态势：集中展示关键设备的在线状态、风险等级与最近一次告警。
- 来宾入网日志：记录来宾账户的申请、审批、接入与离场全过程。

4.2.4 IP 地址池

IP 地址管理页面集中展示设备列表中所有设备所在的 IP 网段，以及各网段内 IP 地址的使用情况。管理员可提前发现 IP 资源紧张与异常占用，减少 IP 冲突与私改地址带来的故障。

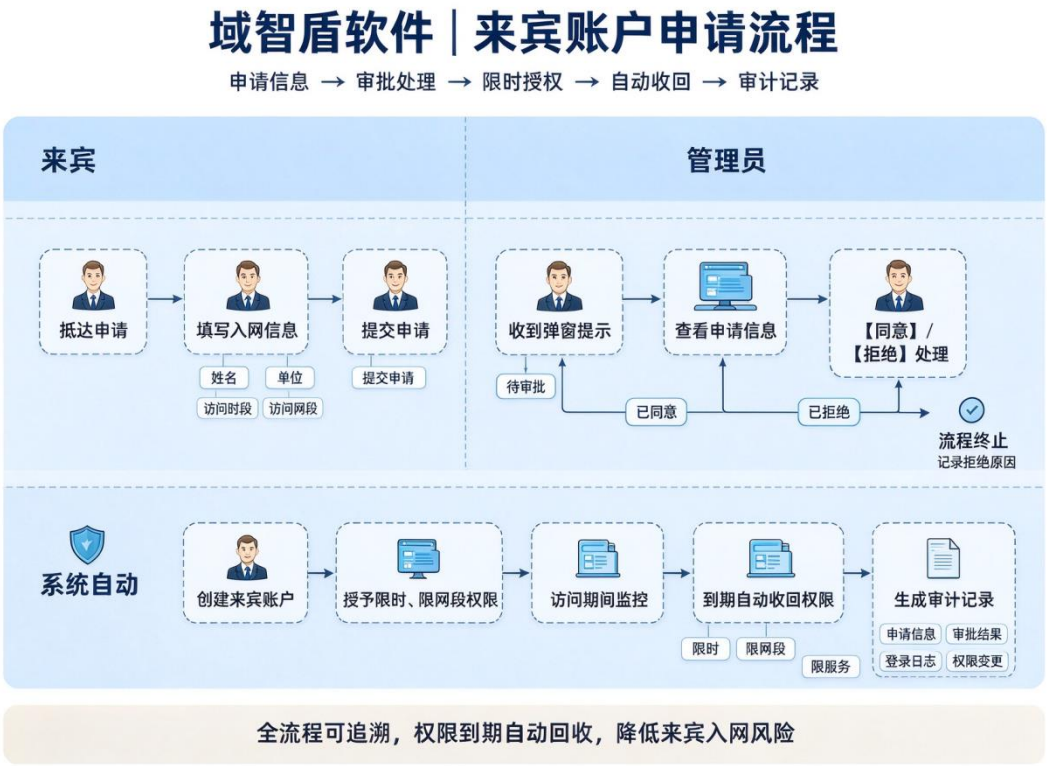
4.2.5 来宾账户申请

能源化工企业日常存在设备厂商现场服务、供应商交付、外部专家进厂指导、参观来访等场景，来宾设备如随意接入内部网络，将带来横向移动与数据外泄风险。

> **问题：**
>
> 能源化工企业日常存在设备厂商现场服务、供应商交付、外部专家进厂指导、参观来访等场景，来宾设备如随意接入内部网络，将带来横向移动与数据外泄风险。

域智盾软件通过来宾账户申请流程对这类接入做统一管理：

- 来宾抵达时：提交入网申请。
- 申请提交后：管控页面自动弹出提示信息，管理员可在左上角工具栏通过【同意】/【拒绝】按钮快速处理。
- 审批通过后：来宾终端获得限时、限网段的访问权限，到期自动收回。



4.2.6 终端安全合规体检

终端入网前自动执行安全基线校验，核查操作系统补丁状态、杀毒软件安装及病毒库更新情况、违规软件、外设管控策略、系统安全配置等。校验不通过的设备自动隔离至修复区，待隐患修复、复检合规后方可授予内网访问权限。

4.3 系统配置

4.3.1 系统管理配置

面向管理员提供以下系统级配置项：

- 管理账户可登录网段：限制管理员账户可以登录的 IP 地址范围，不设置时允许在所有可连通服务器的 IP 地址上登录。
- 密码错误尝试次数：限制管理员账户密码最大错误尝试次数，超过阈值自动锁定。
- 锁定违规账户时长：设置违规账户被锁定后的登录禁用时长。
- 服务器数据保留天数：服务器自动清除设定天数之前的历史数据，避免存储无限增长。
- 长期离线时长：超过设定时长未上线的设备自动标记为长期离线，并在资产列表中提示。
- 系统升级：管理员上传升级文件即可对系统进行版本升级。

- 重启服务器设备：通过控制台按钮远程重启服务器设备，无需现场操作。

4.3.2 网卡配置

支持对准入服务器的 ETH0 网卡进行 IP 地址、子网掩码与网关的配置，适配企业不同网段的部署要求。

4.3.3 系统状态

系统状态页面详细展示准入运行状态、服务器各网口网络连接状态、系统 CPU 占用、内存占用与磁盘占用情况，便于运维人员日常巡检与故障排查。



五、方案价值

（一）合规价值——满足等保与关保要求

形成可向主管部门提供的入网认证记录、资产清单与审计日志，支撑等保测评与关键信息基础设施检查。

（二）安全价值——收紧网络边界

未认证终端一律不得接入内网，来宾与运维人员限时、限网段访问，从源头减少非法接入与横向移动。

（三）管理价值——资产状态可视

全网终端、IP 网段、关键设备在线状态在一张图上可见，IT 部门从“被动响应”转向“主动管理”。

（四）效率价值——事件定位分钟级

违规外联、IP 冲突、外来接入等事件在控制台直接定位到设备、位置与责任人，减少跨部门人工排查。

（五）业务价值——保障生产连续

准入系统不串入生产流量，避免因安全设备故障影响 DCS、SCADA 等关键控制系统的稳定运行。

六、公司简介

河北中视新研软件开发有限公司始终坚持自主可控、技术创新驱动，深度契合国家网络安全战略与关键信息基础设施安全保护政策要求，以终端可信、边界可控、数据可管、行为可溯为核心建设理念，打通资产发现、准入认证、风险阻断、告警溯源、合规审计全闭环管理能力，有效抵御勒索病毒、非法外联、私接设备、数据外泄等安全威胁。

公司于石家庄设立研发与综合服务中心，打造全链路交付保障能力，贯通前期安全调研、试点落地验证、系统上线部署、常态化运维护航全流程，全国统一服务热线 400-097-8770，快速响应客户安全诉求，为项目稳定运行提供坚实后盾。

