基于深度学习的全流量高级可持续威胁智能分析技术研究及平台开发项目

**目录**

[1 项目技术建议书 4](#_Toc45131668)

[1.1 方案概述 4](#_Toc45131669)

[1.1.1 项目背景 4](#_Toc45131670)

[1.1.2 项目需求 5](#_Toc45131671)

[1.1.2.1 需求总结 5](#_Toc45131672)

[1.1.2.2 行业普遍需求 5](#_Toc45131673)

[1.1.3 项目建设目标 6](#_Toc45131674)

[1.2 需求分析 7](#_Toc45131675)

[1.2.1 电力行业信息安全政策和标准 7](#_Toc45131676)

[1.2.2 设备精准识别和分类管理 10](#_Toc45131677)

[1.2.3 异常/恶意行为发现和控制 11](#_Toc45131678)

[1.2.4 异常攻击行为溯源取证 11](#_Toc45131679)

[1.2.5 异常/恶意行为管理 11](#_Toc45131680)

[1.3 整体解决方案 12](#_Toc45131681)

[1.3.1 系统设计原则 12](#_Toc45131682)

[1.3.1.1 合规及国产自主可控 12](#_Toc45131683)

[1.3.1.2 支持多厂商/多平台网络设备及终端 12](#_Toc45131684)

[1.3.1.3 统一的集成化管理平台 12](#_Toc45131685)

[1.3.1.4 遵循ISO27001标准 13](#_Toc45131686)

[1.3.1.5 系统开放性 14](#_Toc45131687)

[1.3.1.6 系统易用性 15](#_Toc45131688)

[1.3.2 方案总体架构 16](#_Toc45131689)

[1.3.2.1 软件部署架构 16](#_Toc45131690)

[1.3.2.2 系统部署架构 17](#_Toc45131691)

[1.3.3 功能性需求设计 19](#_Toc45131692)

[1.3.3.1 设备精准识别和分类管理 19](#_Toc45131693)

[1.3.3.2 智能准入管理 19](#_Toc45131694)

[1.3.3.3 合规遵从检测 20](#_Toc45131695)

[1.3.3.4 攻击行为检测 20](#_Toc45131696)

[1.3.3.5 脆弱性检测 22](#_Toc45131697)

[1.3.3.6 异常行为检测 22](#_Toc45131698)

[1.3.3.7 流量分析 23](#_Toc45131699)

[1.3.3.8 风险处置及可视化管理 24](#_Toc45131700)

[1.3.4 非功能性需求设计 25](#_Toc45131701)

[1.3.4.1 系统性能 25](#_Toc45131702)

[1.3.4.2 系统可靠性 27](#_Toc45131703)

[1.3.4.3 系统安全性 29](#_Toc45131704)

[1.3.4.4 系统扩展性 29](#_Toc45131705)

[1.3.4.5 系统兼容性 30](#_Toc45131706)

[1.3.4.6 系统可维护性 30](#_Toc45131707)

[1.3.5 系统优势及价值 30](#_Toc45131708)

[1.3.5.1 系统优势 30](#_Toc45131709)

[1.3.5.2 系统价值 31](#_Toc45131710)

[2 功能测试报告 32](#_Toc45131711)

[2.1 设备统一管理 32](#_Toc45131712)

[2.1.1 网络设备发现 32](#_Toc45131713)

[2.1.2 终端发现 34](#_Toc45131714)

[2.1.3 终端类型识别 40](#_Toc45131715)

[2.1.4 终端自动分组 43](#_Toc45131716)

[2.1.5 终端快速定位 47](#_Toc45131717)

[2.1.6 摄像头展示 49](#_Toc45131718)

[2.1.7 IP地址管理 52](#_Toc45131719)

[2.2 准入控制 55](#_Toc45131720)

[2.2.1 PC终端准入部署（NACC） 55](#_Toc45131721)

[2.2.1.1 web友好引导重定向 55](#_Toc45131722)

[2.2.1.2 PC终端入网认证—AD联动 57](#_Toc45131723)

[2.2.1.3 PC终端安全检查 60](#_Toc45131724)

[2.2.1.4 访客接入 62](#_Toc45131725)

[2.2.1.5 AD智能准入 64](#_Toc45131726)

[2.2.1.6 深信服对接 66](#_Toc45131727)

[2.2.2 哑终端准入部署（NACC） 67](#_Toc45131728)

[2.2.2.1 AB准入认证 67](#_Toc45131729)

[2.2.2.2 流量行为检测 69](#_Toc45131730)

[2.2.2.3 视频码流黑白名单 72](#_Toc45131731)

[2.2.3 逃生机制（NACC） 73](#_Toc45131732)

[2.3 网络边界威胁感知 76](#_Toc45131733)

[2.3.1 攻击行为感知 76](#_Toc45131734)

[2.3.2 异常行为感知 81](#_Toc45131735)

[2.3.2.1 异常行为分析 81](#_Toc45131736)

[2.3.2.2 异常流量分析 82](#_Toc45131737)

[2.3.2.3 异常接入位置分析 83](#_Toc45131738)

[2.3.2.4 匿名共享 85](#_Toc45131739)

[2.3.2.5 疑似NAT设备 86](#_Toc45131740)

[2.3.3 域名分析 87](#_Toc45131741)

[2.3.4 流量分析 88](#_Toc45131742)

[2.3.5 弱口令检测 90](#_Toc45131743)

[2.3.6 取证报告 92](#_Toc45131744)

[2.3.7 强制下线 93](#_Toc45131745)

[2.4 终端数据防泄密 94](#_Toc45131746)

[2.4.1 终端外发通道管控 94](#_Toc45131747)

[2.4.2 敏感文件审计 95](#_Toc45131748)

[2.4.3 非授权外联控制（光驱、智能设备、其他外设） 97](#_Toc45131749)

[2.4.4 移动存储介质管理（U盘、移动硬盘） 98](#_Toc45131750)

[2.4.5 屏幕控制管理（防截屏、防拍照） 100](#_Toc45131751)

[2.4.6 终端屏幕录像审计 104](#_Toc45131752)

[2.4.7 即时通讯软件审计（QQ、微信外发） 105](#_Toc45131753)

[2.4.8 文档操作审计（HTTP及FTP外发、网络磁盘、本地操作） 107](#_Toc45131754)

[2.4.9 邮件审计（邮件外发方式） 109](#_Toc45131755)

[2.4.10 打印控制与审计（打印传真外发方式） 111](#_Toc45131756)

[2.5 终端桌面安全管理 113](#_Toc45131757)

[2.5.1 软件下发管理 113](#_Toc45131758)

[2.5.1.1 软件分发管理 113](#_Toc45131759)

[2.5.1.2 软件仓库 114](#_Toc45131760)

[2.5.2 资产/IT设备管理 115](#_Toc45131761)

[2.5.3 远程协助与维护 116](#_Toc45131762)

[2.5.4 终端安全加固管理 118](#_Toc45131763)

# 项目技术建议书

## 方案概述

### 项目背景

长期以来，病毒问题是困扰工业控制系统的一个棘手问题，全球工控安全事件频发逐年增加，2016年290起，2017年305起，2018年320起，平均是2010年伊朗震网事件爆发的8倍多，工控信息安全形势愈发严峻。从2008年到2017年发生的事件情况来看，主要是APT攻击、蠕虫病毒、特洛伊木马、恶意软件、勒索病毒等导致的安全事件。如果不针对工控网采取措施，极有可能成为下一个攻击目标，与传统IT不同，不但会导致系统DOWN机，还可能导致人身伤害。如：

1、2008年北京奥运会和2010年上海世博会等重要活动期间，我国电力系统受到了来自境外各种高密度、高强度的恶意网络渗透和攻击；

2、2011年5月1日，华能某电厂恶性电气误操作事件，导致1人死亡，1人重伤；

3、2014年10月17日，云南电网某供电局变电站误操作事故，导致1人触电死亡；

4、2015年，上海某电厂工程师感染病毒，导致监控数据采集异常，经调查确认是技术人员使用U盘拷贝数据造成。

5、2017年，山东43座风电、光伏电站由于电力监控系统安全防护和机组网络管理方面存在重大隐患，被强制断网；

6、2018年1月8日，黑龙江省电力调控中心一侧网络安全管理平台发出重要告警，告警来源为安达某40KMW光伏电站，涉及三套电力生产业务系统，国家能源局东北监管局高度重视，立即责成国网黑龙剑省电力调控中心就相关情况进行处理。

目前公司还缺乏针对全省集中开展网络安全分析、溯源和取证方面的能力，为提升省公司网络攻击、日志审计和关联分析能力和网络安全协同防护水平，通过利用数据分析和深度学习技术，通过研发一种基于深度学习的全流量网络安全智能分析平台，对公司系统网络流量数据采集、预处理、清洗、特征选择、深度神经网络训练和预测等一系列步骤来识别电力网络中的异常流量，对网络恶意流量的在线智能检测及未知威胁的发现具有重要理论意义和实际应用价值。

### 项目需求

#### 需求总结

* 提交面向深度学习的全量威胁数据处理子系统1套；
* 提交基于复杂线索关联分析技术的快速恶意流量侦测子系统1套；
* 提交基于深度神经网络技术的未知威胁检测与验证子系统1套；
* 提交网络威胁全流量回溯子系统1套；
* 提交基于大数据可视化技术的网络威胁和态势监控子系统1套；
* 建立以上模块的全流量网络安全智能分析平台；

#### 行业普遍需求

* 系统拓扑不清，家底不明：工业网络拓扑不清，原始设计拓扑未更新，数据链路不明确，设备资产现状（数量、配置规格）不清楚、应用系统步明确等，没有建立工业网络运维秩序，对工业信息网络本身的资产属性认识不足。
* 缺乏发现和管控不合规设备的手段：如开放了不该开放的服务，存在弱口令等。PLC安全漏洞（某知名品牌PLC默认开启TELNET\FTP\HTTP及RPC服务，这些服务均存严重的安全漏洞；如利用FTP登录后甚至能获取PLC内部的任意文件，包括VXWORKS内核文件。HMI设备漏洞：某知名品牌HMI默认开启Telnet、RDP远程桌面服务、WINDOWS共享服务，且部分服务存在严重的安全漏洞；通讯协议漏洞（暂时做不到）
* 生产网存在违规外联风险：某电厂可能为了方便运维管理，将重要的生产网工作站违规接入互联网，或交换机接入内网，同时接互联网，需及时发现并禁止；
* 存在非法内联风险：生产网、管理网用户非法接入或不合规终端接入，可能对网内其他的设施进行攻击。
* 无异常流量监测审计手段：未部署异常流量监测审计设备，无入侵监测设备，对于长期存在的入侵行为、无法获知、无力追究，不符合相关法律法规和标准规范要求。
* 关键设备日志管控不合规：关键设备日志未保存或保存不合规，没有达到日志保存时限要求，不具备日志关联分析能力，不符合36号文对电力监控系统日志保存分析的相关要求。
* 主机安全配置缺失：主机操作系统安全配置缺失，主机安全状况较差，未制定账号安全管理策略等
* 恶意代码防范手段失效：病毒库未更新（安装了基于黑名单机制的恶意代码防病毒软件，但病毒库老旧，大量恶意程序在生产控制大区操作员站和工程师站传播）、操作系统未加固（工程师站采用XP操作系统，微软停止更新补丁，操作系统无法应对新型恶意代码攻击）
* USB接口/网口五管控，移动存储介质滥用：运维人员使用U盘拷贝文件，引入病毒，容易导致敏感数据泄露
* 安全管理措施缺失、执行不到位：安全人员配置缺失、无安全管理制度、没有运维操作管理规程、制度执行不到位等

### 项目建设目标

通过镜像方式对流量进行捕获，研究从流量中提取资产主机指纹技术，主动探测网络中存活主机设备，提升资产识别的精准度，实现自动、智能、快速定位的资产管理, 并可视化动态绘制资产网络拓扑。通过调研国内外TensorFLow、Keras、CNTK等深度学习技术的发展方向以及恶意流量高级安全分析技术领域的应用情况；开展全流量、离线安全日志的威胁建模研究，分析电力行业恶意流量及离线日志中威胁的特征参数，研究特征向量降维和归一化预处理技术，针对恶意攻击不同场景设计多种类型的深度学习模型和算法来进行训练和威胁建模，并在线验证模型对恶意攻击和未知威胁检测的准确性和实用性；最终实现原型系统研发，基于深度学习算法、架构及威胁建模研究，研发基于机器学习的全流量网络安全智能分析原型系统，结合信息资产和威胁的深度分析，实现动态感知全网威胁的能力。主要包含以下内容：

（1）信息资产主动式识别技术研究；

（2）基础深度学习算法的恶意流量高级安全分析技术研究；

（3）全流量、离线安全日志的威胁建模研究；

（4）基于大数据的网络安全风险智能分析技术和可视化技术研究；

（5）信息系统生态环境（实现信息资产、网络拓扑的主动发现）感知平台研发；

（6）信息系统脆弱性感知平台研发；

（7）信息系统威胁感知平台研发；

（8）信息系统风险分析及安全态势综合展示平台研发。

## 需求分析

### 电力行业信息安全政策和标准

《国家信息安全规范机标准》

1、网络安全法：从立法层面，明确了能源等重要行业领域是国家关键基础设施，必须在等级保护的基础上，实施重点保护，如果运营者不履行法律将面临被处罚的问题；

2、等级保护管理办法及相关标准：特别是等级保护2.0明确提出了通用安全防护和扩展安全防护要求，如通用要求明确提出非法内联、非法外联等控制要求，在扩展要求中明确提出针对物联网、工业控制系统入侵安全防护等要求。等级保护通用要求：10个分类，5个级别的安全要求，包括安全物理环境（无线使用控制）、安全网络通信（网络架构、通信传输、边界防护、入侵防范、恶意代码防范、安全审计、集中管控、拨号使用控制、无线使用控制）、安全区域边界、安全计算环境（控制设备安全）、安全管理中心；安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理。

3、电力监控系统安全防护总体方案（国能安全2015 36号文件）：明确提出“安全分区、网络专用（独立的网络设备组网）、横向隔离、纵向认证、综合防护”，综合防护是结合国家信息安全等级保护工作的相关要求对电力监控系统从主机、网络设备、恶意代码防范、应用安全控制、审计、备份与容灾等多个层面进行信息安全防护的过程，包括入侵监测（NID）、主机与网络设备加固（SIMS/ACCESS）、应用安全控制、安全审计、专用安全产品的管理、备份与容灾、恶意代码防范、设备选型及漏洞整改

4、GB/T 36047-2018 电力信息系统安全检查规范（2018年3月15日）国家电力监督委员会提出，全国电力监管标准化技术委员会协调国家能源局相关部门起草，规范电力信息系统的检查流程、内容和方法，防范网络与信息安全攻击对电力信息系统造成的侵害，保障电力信息系统的安全稳定运行，保护国家关键信息基础设施的安全。检查内容包括：组织体系、规章制度、资金保障、人员安全管理、关键信息资产、服务外包管理、信息系统建设安全管理、信息系统运行安全管理、应急管理、安全分区防御体系、网络安全防护、主机和设备安全防护、应用系统和数据安全保护、物理环境安全保护、业务连续性保护等。

5、《关于加强电力行业网络安全工作的指导意见》2018年72号文件，明确要求落实企业网络安全责任主体，完善网络安全监督管理体制机制，加强全方位网络安全管理；强化关键信息基础设施安全保护；加强电力企业数据安全保护；提高网络安全态势感知预警及应急能力；支持网络安全自主创新及安全可控；积极推进电力行业网络安全健康发展，推进网络安全军民融合深度发展，加强网络安全认材队伍建设等

6、《工业控制系统信息安全防护指南（工信部28号）：明确对安全软件选择与管理、配置和补丁管理、边界安全防护、物理和环境安全防护、身份认证、远程访问安全、安全监测和应急预案演练、资产安全、数据安全、供应链管理、落实责任。

GB/T 36047-2018 电力信息系统安全检查规范（2018年3月15日）电力信息系统：与电力企业的生产、运营、管理、控制相关的信息系统（管理类和生产控制类）

1、管理信息类系统：支持电力企业的经营、管理和运营的信息系统，如门户网站、电力营销管理、财务管理、人力资源管理、物流管理、质量管理等，部署在管理信息大区，与互联网的隔离度为逻辑隔离。

2、生产控制类系统：用于监视和控制电网及电厂生产过程的、基于计算机及网络技术的业务处理系统及智能设备，如电力调度数据网络、电力数据采集与监控系统、能量管理系统、变电站自动化系统、换流站计算机监控系统、发电厂计算机监控系统、配电自动化系统、微机继电保护和安全自动装置、广域相量测量系统、负荷控制系统、水调自动化系统、水电梯级调度自动化系统、电能量计量系统、实时电力市场的辅助控制系统等，部署于生产控制区，与互联网的隔离近似于物理隔离。

3、控制区：具有实时监控功能、纵向联接使用电力调度数据网的实时子网或专用通道的各业务系统构成的安全区域；

4、非控制区：生产控制范围内，由在线运行但不直接参与控制作为电力生产过程的必要环节，纵向联接使用电力调度数据网的非实时子网的各业务系统构成的安全区域。

信息系统安全检查方案（概述、检查依据、技术思路、被检查系统的范围、业务情况、安全防护情况、检查内容和检查成员、工作计划和内容安排等）和信息系统安全检查工作表（列出所有检查内容）。

1、基本内容：全覆盖法、随机抽取法、重点项抽取法，人员访谈、文件查阅、配置核查、安全测试等

通用检查项（G）

•组织体系：第一责任人确立（电力企业主要负责人是否为本单位网络与信息安全的第一责任人/文档查阅）信息安全责任落实（是否设立信息安全管理工作的智能部门，包括安全主管、系统管理员、网络管理员、安全管理员等，是否文件确立职责，电力监控安全防护纳入日常安全生产管理体系落实分级负责的责任制/文档查阅）；专职机构及岗位设置（公安去哪哦工作领导机构、网络与信息安全岗及职责/文件查阅）、安全人员配置（专职/文档查阅）

•规章制度：整体安全策略及总体方案制定/文件查阅、制度制定及体系完整性（人员、资产、介质、建设安全、运维、外包服务、培训等）/文档查阅、操作规程规定、制度发布

•资金保障：经费预算、安全建设经费投入、安全运维经费投入

•人员安全管理：安全培训与考核、保密协议签订、人员审查、岗位调整管控

•服务外包管控：外包服务协议、外部人员访问管理、远程服务管控（书面审批、访问控制、在线监测、日志审计等）、现场开发管控

•关键信息资产管控：资产管理（识别所有与信息系统相关的资产，并编制准确的资产清单，明确每项资产管理责任人及职责）/文档查阅、查阅资产清单、资产责任人明确////资产报废维修管理（数据备份、清除）

•信息系统建设安全管理：技术监督与审核、上线安全测评、等级保护建设、等级测评开展情况（同步）、风险评估、产品采购使用（漏洞风险设备不能选用、符合国家有关规定、生产控制大区除安全接入区选用禁用无线功能的设备）、核心产品采购测试 、安全产品安全可靠

•信息系统运行安全管理：日常维护、安全审计（网络运行日志、操作系统日志、数据库访问日志、业务运行日志、安全设备系统运行日志等收集分析）、补丁管理（补丁升级策略，补丁测试环境、补丁已测的有效渠道）、安全监测（

•

管理信息类系统的检查项（M)

生产控制类系统的检查项（P）

2、补充检查内容：

《电力监控系统安全防护规定明确要求落实国家信息安全等级保护制度》

安全等级保护要求，坚持“安全分区、网络专用、横向隔离、纵向认证”原则，保障电力监控系统安全。

发电企业、电网企业：生产控制大区和管理信息大区，生产控制大区分为控制区（安全1区）、非控制区（安全2区）；管理信息大区内部在不影响生产控制大区的前提下，可以根据企业不同安全要求划分安全区。（避免不同安全区的纵向交叉联接。）

电力调度数据网应当在专用通道上使用独立的网络设备组网，在物理层面上实现与电力企业其他数据网及外部共用数据网的安全隔离。电力调度数据网划分逻辑隔离的实时子网和非实时子网，分别联接控制区和非控制区。

生产控制大区域管理信息大区之间必须设经国家制定部门检测认证的电力专用横向单向安全隔离装置

业务系统具有高安全高可靠，禁止使用安全风险高的通用网络服务功能，建立基于公钥技术的分布式电力调度数字证书及安全标签，生产大区重要业务采用认证加密机制。安全接入区外，选用无无线通信功能的设备。

### 设备精准识别和分类管理

实现所有设备的精准识别，对不同设备进行分类管理，如设备分类统计、设备运行状态管理、设备安全状态管理、IP地址统一管理等。

由于国网四川省信息内网网络规模大、网络分支多、哑终端接入未知分散，无法准确的获知全网的总体网络资产、终端资产、服务器资产的数量并进行设备类型识别与归类，无法第一时间获知设备运行状态、无法获知设备准确位置、无法获知故障原因，对IP冲突严重等管理上存在的漏洞也无法无法有效管控。

当前资产主要以国网桌面管理系统来进行发现与统计，只能对传统PC终端进行统计，对网络资产、各类哑终端设备、服务器资产无法进行有效的统计与管理，更无法对设备类型进行自动识别与归类，管理效率低下。

### 异常/恶意行为发现和控制

无法对网内终端异常/恶意行为进行感知，甚至缺乏有效的网络边界准入控制手段，不能及时发现和处置异常行为，导致风险扩大。

部署在网络出口的入侵防御等安全防护设备无法对内网的异常行为进行有效的识别与管理。

可以根据动态的威胁情报库自动化的对网内所有设备进行检测，对于符合威胁情报库内的行为实现告警提醒、网络控制等手段；并可通过大数据技术及时发现未知攻击行为，可通过智能幻影技术主动捕捉异常/恶意行为，并能及时对未知行为实现告警提醒、取证、网络控制等。

### 异常攻击行为溯源取证

对终端异常攻击行为无法进行有效的调查取证，固定攻击证据链，形成调查取证报告便于后续审计溯源追责。

### 异常/恶意行为管理

能够对接入设备行为进行监测和分析，形成画像，如接入时间、接入地点、接入访问等特征，一旦检测到异常行为可及时精准定位，并及时预警或自动阻断；另外也基于威胁情况、大数据两种方式发现网内恶意行为，实现从原来的被动防御转为主动防御。

* 网络层面：通过网络监测，了解谁进来了，干了什么，是敌是友，并可联动处置。
* 终端层面：可与终端管理平台对接，实现软件更新、补丁更新。 并可对设备外设、安全配置等进行管控。

## 整体解决方案

### 系统设计原则

首先，作为一个“网络智能防御系统”，Leagsoft(联软科技)认为有必要参考国际、国内的安全管理经验，来设计本方案。系统的建设应遵循以下原则。

#### 合规及国产自主可控

技术解决方案及系统部署应符合网络安全法、等级保护等相关法律法规和制度的要求，项目建成后满足法律法规和等级保护相关规定的要求，同时满足所属行业的各项要求。另外，考虑到本项目属信息系统安全类项目，为了响应国家“落实自主可控战略推进国产信息技术应用”以及总中心十三五规划“依靠国产信息安全技术产品构建完善的信息安全保障体系”的号召，系统应采用国产化产品。

#### 支持多厂商/多平台网络设备及终端

解决方案设计的系统要能够实现对主流厂商的网络设备、多种桌面操作系统的支持，是一个采用国际、国家或者行业标准的开放系统，以便将来的网络扩容、系统升级。

#### 统一的集成化管理平台

系统必须提供统一的、集成化管理平台。解决方案要向IT系统管理员提供一个统一的登录入口，有整体的终端安全视图，呈现整个计算机网络系统中所有终端设备的安全运行状况。管理员不仅可以看到自助终端安全的运行状况，终端的安全设置，也能够看到终端的软件配置、硬件配置、终端的物理位置等信息。

通过统一的集成化的管理平台，管理员可以完成所有与自助终端安全管理维护相关的各种任务，具体包括：

用户身份认证，网络准入控制；

网络拓扑发现，设备快速定位；

安全合规遵从检测，包括弱口令检测、状态监控等；

设备智能管理，包括设备分类统计、设备故障告警、设备/IP可视化管理等

异常行为发现控制，包括设备仿冒、IP/MAC伪装、异常访问等异常行为的发现和控制；

恶意行为发现控制，包括APT攻击行为、勒索病毒等恶意行为

风险处置，包括异常告警、网络控制、取证报告等。

统一的集成化管理平台对管理员的各种操作，应提供审计功能，以备事后审计。

#### 遵循ISO27001标准

首先，我们认为有必要参考国际、国内的安全管理经验，来设计网络智能防御系统。ISO27001作为信息系统安全管理标准，已经成为全球公认的安全管理最佳实践，成为全国区域大型机构在设计、管理信息系统安全时的实践指南。

ISO27001认为，设计信息安全系统时，必须掌握以下安全思路：

* 相对安全
* 没有100%的信息安全，安全是相对的，在安全保护方面投入的资源是有限的；
* 保护的目的是要使信息资产得以有效利用，不能为了保护而过度限制对信息资产的使用；
* 分级/分组保护
* 对信息系统分类，不同对象定义不同的安全级别；
* 首先要保障安全级别高的对象；
* 全局性
* 解决安全问题不只是一个技术问题；
* 要从组织、流程、管理上予以整体考虑、解决；

ISO27001中，除了安全思路之外，给出了许多非常细致的安全管理指导规范。在ISO27001中有一个非常有名的安全模型，称为PDCA安全模型。PDCA安全模型的核心思想是：信息系统的安全需求是不断变化的，要使得信息系统的安全能够满足业务需要，必须建立动态的“计划、设计和部署、监控评估、改进提高”管理方法，持续不断地改进信息系统的安全性。



用户网络及终端管理，也将是一个持续、动态、不断改进的过程，安全管控系统将为用户提供统一的、集成化的平台和工具，帮助用户对其网络、终端等资产进行统一的安全控制、安全评估、安全审计及安全改进策略部署。

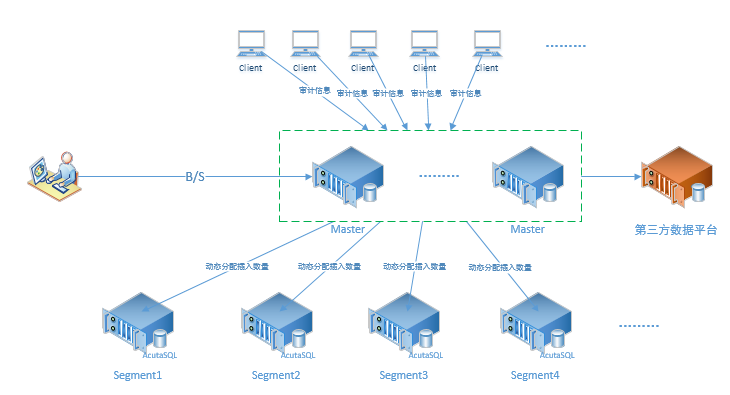
#### 系统开放性

解决方案设计的系统要能够实现对主流厂商的网络设备、主机设备、网络安全设备、应用系统和各种自助终端的管理，是一个采用国际、国家或者行业标准的开放系统，以便能够支持升级后的IT系统管理。

应用软件除满足基本的功能和性能要求外，要具有一定的业务前瞻性、技术前瞻性。

联软网络智能防御系统是联软企业安全保护平台的一部分，联软企业安全保护平台共分为八大部署，满足企业现在及未来的安全保护需求。

同时，为满足企业功能和性能要求，联软科技通过自身创新，不停的优化平台功能，提高系统性能，如为提高海量数据处理速度独立研发的AcutaDB，使处理速度可以达到常规数据库十倍以上的处理速度。



满足产品稳定性、可靠性及安全性要求，系统功能可增配、可扩展，联软网络智能防御系统和联软终端安全管控系统使用了同一个一体化的管理平台，便于用户扩展其他功能。

#### 系统易用性

管控系统应使用统一的管理界面，运维人员通过单一系统即可使用所有管理，管理界面与客户端节目简单易用，符合使用系统，无需额外增加学习成本。

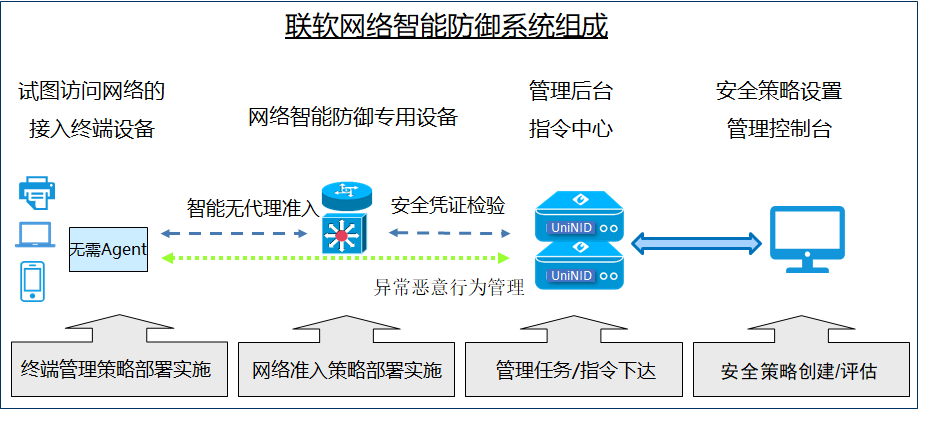


### 方案总体架构

联软网络智能防御系统使用主流技术实现，架构上具有先进性，管控流程清晰，结构明确。其功能可以满足用户所有要求。



#### 软件部署架构



联软科技为用户设计的自网络智能防御系统共包含终端设备、网络智能防御专用设备、管理后台及管理控制台四个部分，四个部分相互联动，实现用户网络及终端的安全管控要求。

终端：包含PC终端、IOT终端等设备，无需在终端安装Agent就可实现设备识别和分类管理、准入控制等功能。

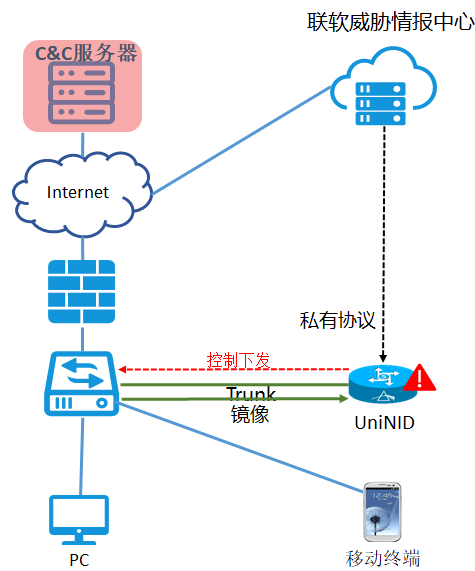
网络智能防御专用设备：网络智能防御专用设备流量镜像，自带RAIDIUS提供用户和终端进行接入认证，异常恶意行为信息报送给管理后台统一分析。

管理后台：包含系统应用、数据库、存储系统等，用于管控策略执行，收集存储异常恶意行为和终端相关信息，向管理员展示分析整理的数据，并为其提供Web管理页面。

管理控制台：管理控制台通过B/S架构实现，由管理后台提供给管理员Web界面，管理员在内部具有权限的终端上登录，供管理员进行数据查看、策略下发等操作。

#### 系统部署架构

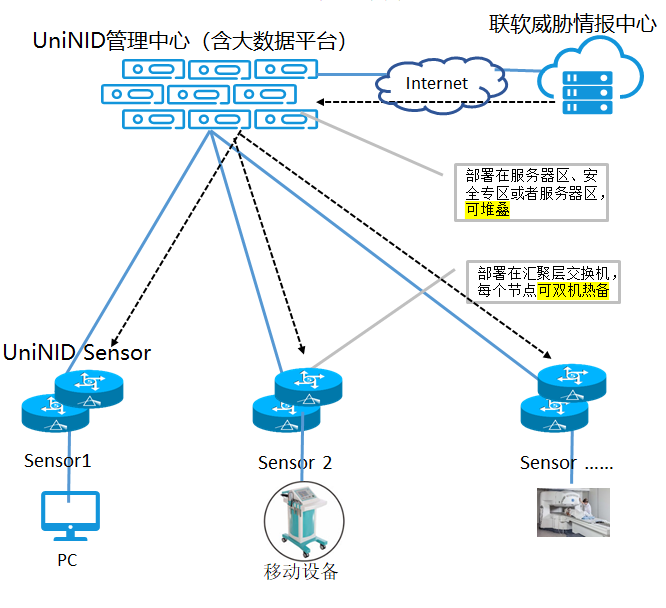
考虑项目单位实际情况，建议采用集中部署方式，系统部署如下图：



部署说明：

* 用户核心交换机旁部署1套网络智能防御管控平台，由2台设备组成，采用双机热备模式部署。
* 网络智能防御设备通过端口镜像方式接收网络流量，实现终端准入控制和异常/恶意行为检测。
* 采用智能幻影技术，主动捕捉异常/恶意行为，并联动准入进行控制。

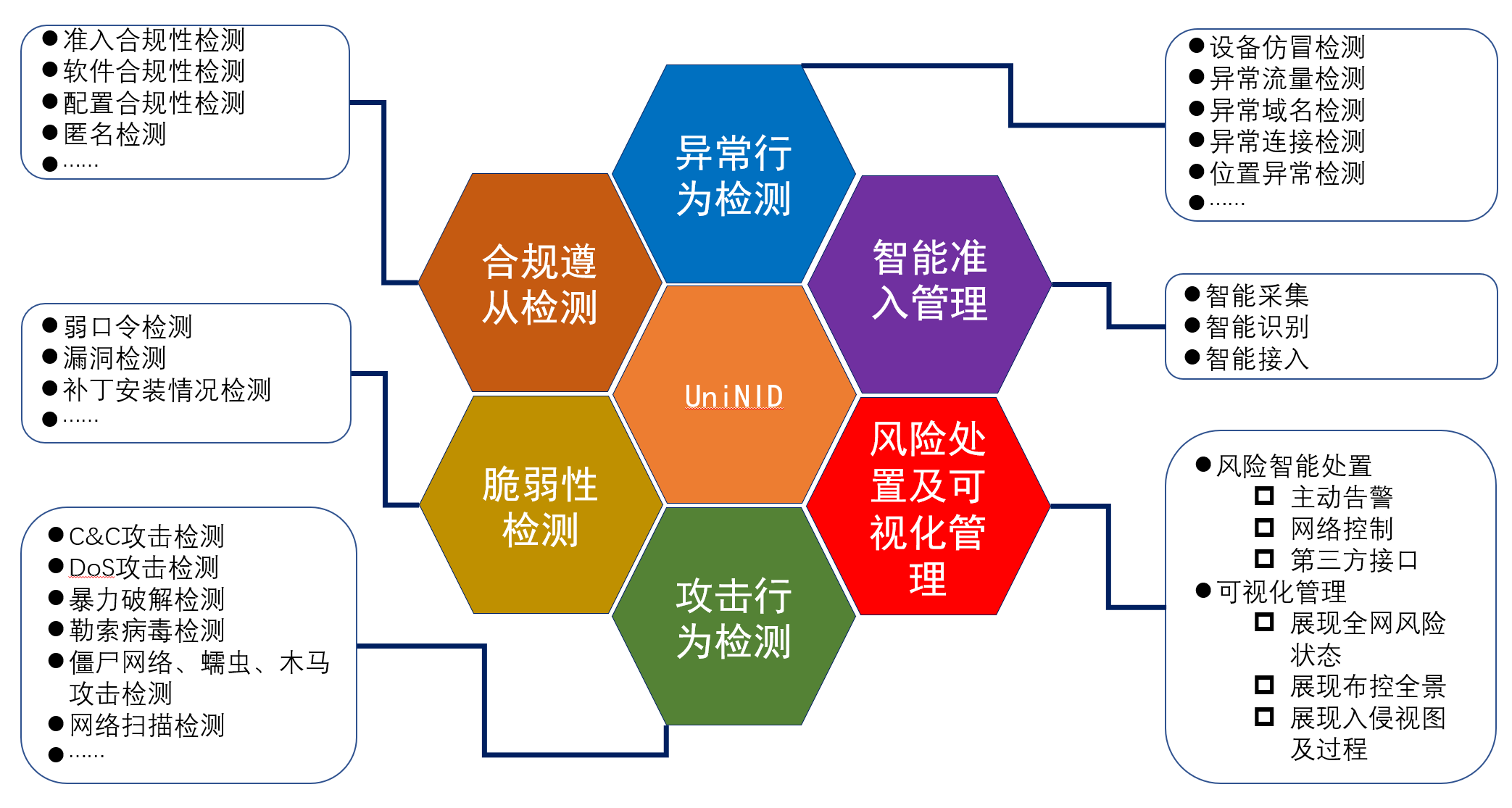
考虑到项目单位情况，建议采用分布式部署，部署情况如下图：



部署说明：

* 总部核心交换机旁部署1套网络智能防御管控平台，由2台高端设备组成，采用双机热备模式部署。
* 各分支机构分别部署1套网络智能防御管控平台，由2台中低端设备组成，采用双机热备模式部署。
* 网络智能防御设备通过端口镜像方式接收网络流量，实现所在地终端准入控制和异常/恶意行为检测。
* 总部和各分支机构采用智能幻影技术，主动捕捉异常/恶意行为，并联动准入进行控制。

### 功能性需求设计



#### 设备精准识别和分类管理

* 智能采集：基于主动和被动信息采集技术，智能采集设备（IP/MAC）信息、路由信息、身份信息、主机名、操作系统、位置信息、流量信息等。
* 智能识别：基于联软自主研发的设备画像技术，智能识别网络拓扑、设备的类型、设备厂家、设备状态（新设备/在线设备/离线设备）、设备安全状态（安全、较安全、不安全）、设备之间的连接关系等，支持对PC设备、网络设备、移动设备、IoT设备（含视频终端等）、ICS设备等主流设备类型和厂家的识别。

#### 智能准入管理

* 支持基于AD域或Email的智能准入。
* 支持传统的基于802.1x、EoU/NACC的准入方式；
* 支持基于指纹的准入方式；认证方式支持LDAP/RADIUS/AD等。

#### 合规遵从检测

* + 准入合规性检测：支持发现未开准入的交换机/路由器/未开准入的交换机端口、未开准入的网段、未准入的设备等，发现未准入的情况立即告警或者阻断。
  + 软件合规性检测：支持发现未安装防病毒软件的终端设备，支持发现未安装企业合规的软件或者安装违规软件的设备，发现软件违规的设备立即告警或者阻断。
  + 配置合规性检测： 支持发现未正确配置DNS的终端设备和违规的DNS服务器；支持发现违规的AD服务器、未加入域的设备、加入域但未登录域的设备；支持发现未设置或者设置错误的WSUS服务器的Windows终端设备，发现配置违规的设备立即告警或者阻断。
  + 匿名检测：支持发现匿名共享服务器和匿名的FTP服务器，发现违规开启匿名访问的设备立即告警或者阻断。
  + NAT设备检测：支持发现网络内部私设的网中网（违规使用网络共享，违规开启无线AP接入等），发现违规的NAT设备时可立即告警或者阻断。
  + 违规共享：支持发现违规的网络共享服务器，发现违规共享时可立即告警或者阻断。
  + 设备接入时间检查：支持发现非工作时间接入网络的PC设备、移动终端设备等，发现时可立即告警或者阻断。
  + Telnet合规性检查：支持发现Telnet服务器，发现时可立即告警或者阻断。

#### 攻击行为检测

* + C&C攻击检测：支持检测设备与C&C（命令与控制服务器）的连接行为，发现时可立即告警或者阻断；
  + DoS攻击检测：支持SMTP/MYSQL/RDP/DNS/HTTP等协议的DOS攻击检测，发现时可立即告警或者阻断；
  + 暴力破解检测：支持RDP/SSH/FTP等协议的暴力破解攻击检测，发现时可立即告警或者阻断；
  + 勒索病毒检测：支持检测WantCry等勒索病毒的检测；
  + 僵尸网络、蠕虫、木马攻击检测：支持僵尸网络、病毒、蠕虫等攻击行为检测，发现时可立即告警或者阻断；
  + 网络扫描检测：支持常见的Nmap、Nessus、Nikto等常见扫描工具的端口、数据库、Web页面扫描，操作系统探测等扫描行为检测，发现时可立即告警或者阻断；
  + Shellcode攻击检测：支持常见的Shellcode攻击检测，如利用SHELL编写一段代码，发送到服务器利用代码的特定漏洞获取权限，发现时可立即告警或者阻断;
  + 恶意软件攻击检测：支持检测间谍软件、仿冒的防病毒软件等恶意软件，发现时可立即告警或者阻断；
  + 权限破解攻击检测：支持检测普通或者超级管理员的权限破解攻击，发现时可立即告警或者阻断；
  + 视频语音协议攻击检测：支持检测视频和语音协议的攻击，发现时可立即告警或者阻断。
  + 新增Xbash检测功能：支持Xbash恶意软件的检测，发现时发现时可立即告警或者阻断。

#### 脆弱性检测

* + 弱口令检测：支持检测Web/SSH/TELNET/FTP等应用的弱口令，支持用户导入自主的账号和密码字典；支持摄像头弱口令检测，内置原厂默认账号和密码。
  + 漏洞检测：与联软LeagView平台联动，可以发现终端、服务器等的漏洞情况。
  + 补丁安装情况检测：与联软LeagView平台联动，可以发现终端、服务器等的补丁修复情况。

#### 异常行为检测

* 设备仿冒：基于联软自主研发的设备画像技术，支持基于设备类型、IP、MAC、设备名、操作系统、系统服务、流量特征、行为特征的设备仿冒检测。发现设备仿冒时，系统会发出告警或者自动阻断。
* 异常连接：基于联软独创的无监督机器自学习技术结合威胁情报，能自动学习网络中设备之间的连接关系以及访问互联网的行为，自动构建用户正常的访问行为模式，智能发现异常的连接。发现异常连接时，系统会发出告警或者自动阻断。
* 异常流量：基于联软独创的无监督机器自学习技术，能自动学习网络中设备之间的流量行为特征以及访问互联网的流量特征，在某一时间段内流量发生异常时，系统会发出告警或者自动阻断。
* 异常协议：可及时发现异常协议的访问（如80端口，跑的是非http协议流量），可立即报警并阻断。
* 异常在线时间：基于联软独创的设备画像技术，能自动学习设备的在线时长，一旦发现设备在线时间异常，可立即报警或阻断。
* 异常接入位置：对于服务器、哑终端设备、IoT设备等接入位置相对固定的设备，一旦发现设备接入位置发生变化，会立即报警或阻断。
* 异常域名：系统采用机器学习和威胁情报相结合的方式，对域名进行可疑度分析，发现恶意域名立即告警或者阻断。
* 智能幻影：基于联软独创的幻影技术，可以按比例自动幻影出与在线设备一致的设备类型和数量（如果IP地址不够用，生成的数量会少于在线的设备数），支持手动创建幻影设备；支持自动或手动生成幻影网络；发现恶意访问幻影设备立即告警或者阻断；
* 幻影AD：基于联软独创的幻影技术，可以在网络中幻影出一台或者多台AD服务器，管理员可以在幻影AD服务器中放置诱饵文件；发现恶意访问幻影AD服务器立即告警或者阻断；
* RDP面包屑：该功能要与手动幻影功能相配合，先手动幻影RDP服务器，然后生成RDP面包屑；面包屑通过AD域控制器或者桌面管理软件下发给每个终端，并自动运行；发现恶意访问幻影RDP服务器立即告警或者阻断；

#### 流量分析

* 支持显示实时流量，上下行速率，实时连接关系，TOP流量主机、应用层协议、服务器端口流量等
* 支持总流量分析：总流量信息，数据包（TCP/UDP/IP）分析、应用层协议分析、ICMP/ARP协议分析等；
* 活动会话分析：包含客户端、服务端、会话持续时间、4层协议类型、应用层协议、吞吐量，以及总流量；
* 主机流量分析：展示IP地址、设备名称、持续时间、吞吐量、总流量；
* 网段列表：展示网段名称、主机数量、持续时间、吞吐量、总流量；
* 支持互联网流量地图：访问互联网的流量，支持以地图方式展现。

#### 风险处置及可视化管理

1. 智能处置

对存在风险的设备，系统可以根据安全系数变化情况，采用以下几种方式进行智能处置：

* 主动告警：可通过SMS/Email/Web等方式通知管理员和使用者，及时做出响应；
* 网络控制：可以根据系统预设置的策略，对设备阻断，重认证或跳转到安全区域进行修复；
* 第三方接口：可以通过Syslog/SNMP Trap等方式通知事件中心，如SOC/SIEM等。

（2）可视化管理

* + - * 展现全网风险状态：系统会根据设备的异常行为、攻击行为、合规性、脆弱性的严重程度和分布情况，采用机器学习的算法，实时计算每台设备的安全系数；系统会依据设备的价值，根据机器学习的算法实时计算企业全网的安全系数；并可以定性或者定量的方式展现设备以及全网风险状态；
      * 展现布控全景：系统会实时跟踪并展现智能准入、异常行为感知、合规感知、攻击行为感知、脆弱性感知等主要安全防护模块的运行情况（开启、关闭、数量）；
      * 展现入侵视图及过程：支持展示全网设备分布图、攻击链分析视图、准入状态视图、不合规设备趋势图、异常行为设备趋势图、攻击行为设备趋势图、幻影设备趋势图以及流量视图、域名分析视图等；与LeagView系列产品联动可展示攻击路径图；
      * 取证报告：支持导出取证报告，包含设备的安全指数，设备的基本信息、不合规信息、攻击行为信息、异常行为信息、网络连接行为信息、IP地址及其它相关辅助信息等。支持风险分析报告（按天、周、月和自定义时间导出）导出功能。

### 非功能性需求设计

#### 系统性能

联软网络智能防御系统单台设备最大支持20000台无代理软件设备安全管理，可支持瘦终端、IoT设备、ICS设备，最大认证并发数不低于2000个/秒。网络流量性能参数如下：

按100台终端数量，通过对需占用网络流量的功能进行流量定量分析如下表所示：

网络流量性能参数

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **功能** | **频率** | **数据量**  **(100台)** | **峰值流量** | **平均流量** | **备注** |
| 拓扑  发现 | 1次/月 | 100×100字节 | 上行8Kbps | 约等于零 | 可定为在下班后执行，峰值按10s完成计算 |
| 设备  发现 | 1次/5分钟 | 100×100字节 | 上行8Kbps | 上行267bps | 可设定开市交易期间不执行 |
| 网络  准入 | 3次/天 | 100×1500字节 | 上行4kbps | 约等于零 | 按照上班时间5分钟内开机 |
| 心跳 | 1次/60s | 100×64字节 | 上行、下行850bps | 上行下行850bps | 可忽略 |
| 策略  下传 | 2次/天 | 100×1500字节 | 下行20Kbps | 约等于零 | 峰值按照60s心跳平均 |

根据上述分析，可以发现100台系统产生的流量上行峰值为20Kbps，下行峰值为20Kbps，如果20000台终端，则上行峰值为4000KBps，下行峰值为4000KBps。目前设备最大设备处理并发流量可达40G，完全可以满足要求。

备注：

联软网络智能防御系统单台设备最大支持5000台视频终端安全管理，网络流量性能参数如下：

按100台视频终端数量，通过对需占用网络流量的功能进行流量定量分析如下表所示：

网络流量性能参数

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **功能** | **频率** | **数据量**  **(100台)** | **峰值流量** | **平均流量** | **备注** |
| 拓扑  发现 | 1次/月 | 100×100字节 | 上行8Kbps | 约等于零 | 可定为在下班后执行，峰值按10s完成计算 |
| 设备  发现 | 1次/5分钟 | 100×100字节 | 上行8Kbps | 上行267bps | 可设定开市交易期间不执行 |
| 网络  准入 | 3次/天 | 100×1500字节 | 上行4kbps | 约等于零 | 按照上班时间5分钟内开机 |
| 心跳 | 1次/60s | 100×64字节 | 上行、下行850bps | 上行下行850bps | 可忽略 |
| 策略  下传 | 2次/天 | 100×1500字节 | 下行20Kbps | 约等于零 | 峰值按照60s心跳平均 |
| 视频流量 | 秒 | 8M | 8Mbps | 约等于零 | 带宽占有大 |

根据上述分析，可以发现100台视频终端产生的视频流量最大，其他流量可忽略不计，100台视频终端（高清）产生的流量上行峰值为800Mbps，如果5000台终端，则上行峰值为40Gbps，下行峰值可忽略不计。目前设备最大设备处理并发流量可达40G，完全可以满足要求。

#### 系统可靠性

##### 双机主备

采用VRRP协议，将主、备网络智能防御专用设备虚拟成一套系统，系统对外提供统一的服务。当主机出现故障时候，备机会自动接管主机提供服务。具体切换方式如下：

1. 网络智能防御系统有两台专用设备进行主备；
2. 主、备网络智能防御专用设备通过VRRP的方式对外提供一个IP地址；
3. 各客户端通过虚IP连接到网络智能防御专用设备，当主IP出现故障时自动与备IP连接，通过备网络智能防御专用设备替代主网络智能防御专用设备。
4. 主网络智能防御专用设备修复后，可自动/手动切回主设备，从而确保整个系统的高可用性。

##### DB主备

主备网络智能防御专用设备的数据采用事务日志同步的方式时刻保持一致，数据同步时间应低于30秒，以确保备网络智能防御专用设备能够及时代替主网络智能防御专用设备运行；

##### 第三方认证系统状态检测

网络智能防御系统与第三方认证系统联动，系统配置后。会自动检测第三方认证系统的可用性。



（1）自动应急

检测到第三方认证系统没有响应或者不可用时，系统会自动进入应急状态，并将第三方认证系统标记为Dead状态。

（2）自动恢复

自动进入应急状态后，会持续对第三方认证系统进行可用性检测。如果检测到第三方认证系统恢复可以状态，系统会标记为Active状态，恢复正常认证请求。

（3）系统应急模式

当出现紧急情况，无法定位故障问题点的时候。系统提供“一键逃生”按钮，快速进入应急状态。

（4）系统告警机制

为了能让管理员快速的知道系统运行状态，网络智能防御系统提供系统告警功能。支持SYSLOG、SNMPTRAP，SMS，E-Mail、微信等多种接受告警的方式。

##### 一键逃生

系统需要支持自动／手动的应急方式，系统检测到运行中出现的异常和故障需要能够自动逃生，允许设备直接接入网络，确保企业网络的可用性。另外接入控制逃生可不依靠网络设备，通过自身也可实现。



##### 系统易用性

为了便于使用人员比较容易使用网络智能防御系统，我司采取了以下措施：

一是菜单简单逻辑清晰。我司网络智能防御系统的用户功能菜单简单易懂，逻辑清晰，菜单不超过三级；

二是系统自带帮助说明。在系统界面上对菜单、选项、按钮等具有相关使用说明，用户初次使用时参考界面上的使用说明可较容易的使用系统。错误操作均有代码及文字的错误提示。输入框应记录常用输入内容以简化输入工作，提供下拉列表方式便于用户选择。

三是系统快速故障诊断。系统提供的接入记录应该清晰显示，如接入状态、接入时间、接入设备类型、接入失败原因等，管理员可以快速判断失败原因。

另外，系统首页提供技术支持热线电话和常见问题解答。系统提供“关于”说明，对本系统的版本号、承建商、上线日期等基本信息进行了说明。

#### 系统安全性

网络智能防御系统采取了以下措施确保系统自身的安全：

一是自带WAF功能，提高自身Web应用的安全防御能力；

二是三权分立，管理员角色分为系统管理员、安全管理员、审计员，职责分离，减少越权访问和操作发生的机率，保障运维安全。

三是防攻击，系统具备针对DDoS攻击、Syn Flood、Ack Flood、Http/Https Flood(CC攻击)的防御能力；系统具备针对SQL注入、命令注入的防御能力；系统具备针对目录遍历的防御能力。

#### 系统扩展性

网络智能防御系统在部署上、功能上都可扩展，具体如下：

一是系统容量扩展性强。系统自身扩展性强，用户可根据终端数量灵活选择，目前单台设备依据型号可提供200、500、1000、2000、5000、20000（非视频终端）台终端，且系统支持分布式部署，可通过增加设备实现横向扩展，以适应用户实际终端管控需要和网络环境的实际情况。

二是系统功能可扩展。系统除支持准入、终端发现和管理等基本功能外，还支持基于威胁情报库的恶意行为发现和控制等功能，并支持威胁情报库的在线或离线更新。

三是参数及配置可自定义。用户显示界面可参数化配置，如下拉菜单中的选项可配置， 业务流程和业务规则可配置，以适应业务流程和业务规则的不断调整。

#### 系统兼容性

网络安全态势感知系统不但与用户现网环境中所有主流的终端、网络等设备兼容，同时可与用户现有的系统集成。

一是设备兼容性：不但可兼容主流的IOT设备、ICS设备等终端设备，还可兼容思科、华为、华三、锐捷、迈普等主流网络设备。

二是可与用户现有系统集成：通过标准接口可与用户OA、AD、SOC等系统集成。

#### 系统可维护性

为便于管理员运维，系统除了支持集中管理、数据集中展示、系统集中监控等功能外，还提供了ping、抓包、traceroute等丰富的网络诊断工具。具体如下：

一是集中管理。支持设备集中管理，如集中软件升级等，也支持数据集中展示，由管理后台集中采集设备上报的信息，并进行集中管理和统一展示。

二是系统监控。系统拥有自监控模块，能够检测系统硬件资源使用情况，系统模块可用性检测；支持第三方监控平台，如支持通过SNMP监控、支持Zabbix监控；支持系统运行状态监控，如有异常可通过页面、短信、邮件、微信等方式发出告警。

### 系统优势及价值

#### 系统优势

**风险精准识别**

* 黑名单识别：黑名单包括自主与第三方威胁情报
* 动态“陷马坑”：能够准确捕获网络攻击行为
* 通过高质量的大数据与AI算法实现精准识别，高质量表现为数据自行从源头直接采集、加工，避免数据失真；另外高质量还表现为数据维度多，包括设备的类型、安全状态、使用者、接入位置、接入时间、网络行为、访问对象、使用习惯等信息

**发现未知类型攻击**

* 动态“陷马坑”：通过诱捕方式发现攻击，不需要知道攻击类型即可捕获
* 通过大数据和机器学习算法发现未知类型攻击，包括画像式发现、关联分析、可疑域名分析等

**安全可视化**

* 资产可视化：自动发现网络资产，识别高价值资产（如数据库、源代码服务器、域控服务器、ERP服务器等），可视化展现资产的状态、类型、位置、使用者等信息
* 行为可视化：自动识别设备与用户行为，可视化展现访问关系和使用习惯
* 攻击可视化：智能识别网络攻击，可视化展现攻击入侵路径、横向移动过程、攻击方式等

**部署简单、扩展性强**

* 设备采用旁路部署的方式，无需修改现有的网络拓扑，配置简单，开箱即用
* 终端电脑上无需安装任何的客户端软件和插件，无需修改任何配置
* 单台设备最大支持40Gbps网络流量，支持分布式部署和集中部署，管理中心支持线性扩展（集群）

#### 系统价值

**准确及时发现入侵，**保护高价值资产，防止数据破坏与泄密

**提高效率，自动化智能化让安全**合规和安全管理工作更简单

**高投资回报，**系统和NAC系统融合，一套系统解决多方面问题

**安全防御智能化是趋势，NID是****新一代的网络安全基础设施**

# 功能测试报告

## 设备统一管理

### 网络设备发现

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-001-001 | 名称 | 网络设备发现 |
| 内容 | 通过SNMP能够发现全网中网络设备信息，包括管理IP地址、管理Mac地址、设备类型、设备厂商、端口数量、未开启准入端口、Hub端口； | | |
| 特殊要求或配置 | 网络环境已搭建，各设备正常运行； | | |
| 测试步骤 | 1、UniNID接入网络中，配置系统SNMP团体字；  2、配置网络设备SNMP团体字，以Cisco为例；  3、测试网络设备SNMP连通性；  4、进行拓扑发现； | | |
| 预期结果 | |  |  |  |  | | --- | --- | --- | --- | | 测试项目 | | 预期目标 | 真实结果 | | 网络设备展示 | 设备名 | 能够自动发现 | ☑能/□否/□有误 | | IP地址 | 能够自动发现 | ☑能/□否/□有误 | | MAC地址 | 能够自动发现 | ☑能/□否/□有误 | | 设备类型 | 能够自动发现 | ☑能/□否/□有误 | | 设备厂商 | 能够自动发现 | ☑能/□否/□有误 | | 端口数量 | 能够自动判断 | ☑能/□否/□有误 | | 未开启准入端口 | 能够自动判断 | ☑能/□否/□有误 | | HUB端口 | 能够自动判断 | ☑能/□否/□有误 | | | |
| 测试截图 | 配置系统SNMP团体字；    网络交换机图形化面板信息：  D:\百度云同步盘\职场\联软\支持项目\税友 截图\测试截图\QQ截图20181214164906.bmp  拓扑发现过程； | | |
| 结论 | ■通过□部分通过□不通过□未测试  通过项目：全部通过。  未通过项目：无。  相关功能可开发项：  相关额外功能： | | |
| 备注 |  | | |

### 终端发现

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-001-002 | 名称 | 终端发现 |
| 内容 | 产品可以扫描管控网段的所有终端，并且能够发现终端的设备名（历史设备名）、状态、IP地址（历史所用IP地址）、MAC地址（网卡厂商）、操作系统、部门信息、认证账号、安全状态、阻断状态、所连接的交换机端口（历史接入位置）、设备在网时间统计图； | | |
| 特殊要求或配置 | 准入系统需要交换机端口信息读权限，或者具备端口镜像ARP/DHCP流量； | | |
| 测试步骤 | 1、拓扑发现结束后，调整新设备发现时间间隔；  2、抓包查看镜像口是否具备设备的ARP/DHCP流量；  3、将各类终端接入网络，测试能否快速发现接入终端，并获取联网终端的设备名（历史设备名）、状态、IP地址（历史所用IP地址）、MAC地址（网卡厂商）、设备类型、操作系统、部门信息、用户信息、安全状态、阻断状态、接入位置（历史接入位置）、开放端口、设备在网时间统计图、IP地址连接关系列表； | | |
| 预期结果 | |  |  |  |  | | --- | --- | --- | --- | | 测试项目 | | 预期目标 | 真实结果 | | 终端发现 | 新接入设备发现 | 一分钟内 | ☑能/□否/□有误 | | 设备切换端口  重新发现 | 一分钟内 | ☑能/□否/□有误 | | 设备名 | 能够自动发现 | ☑能/□否/□有误 | | 状态 | 能够自动发现 | ☑能/□否/□有误 | | IP地址 | 能够自动发现 | ☑能/□否/□有误 | | MAC地址 | 能够自动发现 | ☑能/□否/□有误 | | 操作系统 | 能够自动发现 | ☑能/□否/□有误 | | 部门信息 | 能够自动发现 | ☑能/□否/□有误 | | 用户信息 | 能够自动发现 | ☑能/□否/□有误 | | 安全状态 | 能够自动发现 | ☑能/□否/□有误 | | 阻断状态 | 能够自动发现 | ☑能/□否/□有误 | | 接入位置 | 能够自动发现 | ☑能/□否/□有误 | | 开放端口 | 能够自动发现 | ☑能/□否/□有误 | | 设备在网时间 | 能够自动发现 | ☑能/□否/□有误 | | IP地址连接关系 | 能够自动发现 | ☑能/□否/□有误 | | | |
| 测试截图 | 调整新设备发现间隔时间；  （默认启用ARP、DHCP流量更新设备）    全网设备展示：  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\全网设备.bmp  设备详细信息展示 | | |
| 结论 | ■通过□部分通过□不通过□未测试  通过项目：全部通过。  未通过项目：无。  相关功能可开发项：  相关额外功能： | | |
| 备注 |  | | |

### 终端类型识别

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-001-003 | 名称 | 终端类型识别 |
| 内容 | 产品能够对终端类型识别库进行规则定义，基于多种方式识别设备类型； | | |
| 特殊要求或配置 | 网络环境已搭建，各设备正常运行； | | |
| 测试步骤 | 1、测试设备接入网络，被发现成新设备接入，并处于未识别状态；  2、配置主动探测自动进行扫描或者手动扫描；  3、设备自动更新设备类型； | | |
| 预期结果 | |  |  |  |  | | --- | --- | --- | --- | | 测试项目 | | 预期目标 | 真实结果 | | 终端类型识别库管理 | 基于MAC厂商库识别 | 能够识别 | ☑能/□否/□有误 | | 基于NMAP协议识别 | 能够识别 | ☑能/□否/□有误 | | 基于NETBIOS协议识别 | 能够识别 | ☑能/□否/□有误 | | 基于SNMP协议识别 | 能够识别 | ☑能/□否/□有误 | | 基于流量识别 | 能够识别 | ☑能/□否/□有误 | | 支持导入规则 | 能够导入 | ☑能/□否/□有误 | | 主动探测/被动探测 | 自动/手动扫描 | ☑能/□否/□有误 | | | |
| 测试截图 | 1、启用主动探测，定期探测设备；    2、手动探测，设备自动更新    3、设备类型识别分类  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\设备信息.bmp  4、摄像头识别  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\摄像头.bmp | | |
| 结论 | ■通过□部分通过□不通过□未测试  通过项目：全部通过。  未通过项目：无。  相关功能可开发项：  相关额外功能： | | |
| 备注 |  | | |

### 终端自动分组

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-001-004 | 名称 | 终端自动分组 |
| 内容 | 对于发现到的终端，能够自动基于IP地址范围、网段、所在部门、MAC地址范围、设备类型、设备状态进行设备分组； | | |
| 特殊要求或配置 | 设备概要有设备记录； | | |
| 测试步骤 | 1、设备已经被发现，并且被识别出来的情况下；  2、配置自动分组条件，比如：根据IP地址范围、Mac地址范围、网段、部门、设备类型、开放端口、设备状态等；  3、分组信息定期1小时更新设备信息（或者重新点击保存）； | | |
| 预期结果 | |  |  |  |  | | --- | --- | --- | --- | | 测试项目 | | 预期目标 | 真实结果 | | 终端自动分组 | 基于IP地址范围自动归类设备 | 能够自动归类 | ☑能/□否/□有误 | | 基于网段自动归类设备 | 能够自动归类 | ☑能/□否/□有误 | | 基于部门自动归类设备 | 能够自动归类 | ☑能/□否/□有误 | | 基于MAC地址自动归类设备 | 能够自动归类 | ☑能/□否/□有误 | | 基于终端类型自动归类设备 | 能够自动归类 | ☑能/□否/□有误 | | 基于设备状态自动规则设备 | 能够自动归类 | ☑能/□否/□有误 | | | |
| 测试截图 | 启用自动分组，填写自动发分组条件； | | |
| 结论 | ■通过□部分通过□不通过□未测试  通过项目：全部通过。  未通过项目：无。  相关功能可开发项：  相关额外功能： | | |
| 备注 |  | | |

### 终端快速定位

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-001-005 | 名称 | 终端快速定位 |
| 内容 | 产品支持终端快速定位，支持以交换机面板与终端互联方式、交换机真实面板+端口列表方式呈现终端定位，支持面板切换交换机端口状态； | | |
| 特殊要求或配置 | 网络环境已搭建，各设备正常运行； | | |
| 测试步骤 | 1、准入系统接入网络中，对全网设备进行扫描；  2、查看页面所展示的终端分布图的正确性； | | |
| 预期结果 | |  |  |  |  | | --- | --- | --- | --- | | 测试项目 | | 预期目标 | 真实结果 | | 终端快速定位 | 端口与终端互联视图 | 能够自动显示 | ☑能/□否/□有误 | | 交换机面板+端口列表 | 能够自动显示 | ☑能/□否/□有误 | | 终端管理列表快速定位 | 能够快速定位 | ☑能/□否/□有误 | | 面板端口开关 | 能够实时切换 | □能/☑否/□有误 | | | |
| 测试结果 | 交换机面板展示； ifAdminStatus = 1，表示交换机端口处于no shutdown; ifOperStatus = 1，表示交换机端口下连接设备；    点击端口，显示该端口下连接； | | |
| 结论 | ■通过□部分通过□不通过□未测试  通过项目：  未通过项目：  相关功能可开发项：  相关额外功能： | | |
| 备注 |  | | |

### 摄像头展示

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-001-007 | 名称 | 摄像头展示 |
| 内容 | 产品支持以地图形式呈现摄像头地理位置；  支持手动填写GPS坐标、百度坐标，或者填写地理位置等方式； | | |
| 特殊要求或配置 | 适用范围：摄像头设备； | | |
| 测试步骤 | 1、需要先识别成摄像头设备，并在摄像头列表展示；  2、填写摄像头设备地理位置/或者GPS坐标，查看摄像头地图；  3、导入摄像头位置； | | |
| 预期结果 | |  |  |  |  | | --- | --- | --- | --- | | 测试项目 | | 预期目标 | 真实结果 | | 摄像头  地图 | 地理位置 | 能够在地图展示 | ☑能/□否/□有误 | | GPS坐标 | 能够在地图展示 | ☑能/□否/□有误 | | 百度坐标 | 能够在地图展示 | ☑能/□否/□有误 | | 导入摄像头位置 | 导入成功，并且能在地图展示 | ☑能/□否/□有误 | | | |
| 测试截图 | 摄像头列表；    填写设备位置，加载经纬度；      导入摄像头位置； | | |
| 结论 | ■通过□部分通过□不通过□未测试  通过项目：全部通过。  未通过项目：无。  相关功能可开发项：  相关额外功能： | | |
| 备注 |  | | |

### IP地址管理

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-001-008 | 名称 | IP地址视图 |
| 内容 | 产品支持IP地址视图呈现，以视图形式呈现IP地址在线、离线、IP地址当前设备类型； | | |
| 特殊要求或配置 | 网络环境已搭建，各设备正常运行； | | |
| 测试步骤 | 1、调整新设备发现时间间隔，获取网络设备的ARP信息；  2、设备概要信息中所有设备都获取到vlan网段信息； | | |
| 预期结果 | |  |  |  |  | | --- | --- | --- | --- | | 测试项目 | | 预期目标 | 真实结果 | | 全网IP地址视图管理 | IP地址视图呈现 | 能够自动呈现 | □能/□否/☑有误 | | 在线设备 | 能够视图展示 | □能/□否/☑有误 | | 离线设备 | 能够视图展示 | □能/□否/☑有误 | | 未分配IP地址 | 能够视图展示 | □能/□否/☑有误 | | IP地址所属设备类型 | 能够视图展示 | ☑能/□否/□有误 | | | |
| 测试截图 | 必须通过SNMP获取网络设备ARP表；    查看网段信息；    网段设备分布图； | | |
| 结论 | ■通过□部分通过□不通过□未测试  通过项目：全部通过。  未通过项目：无。  相关功能可开发项：  相关额外功能： | | |
| 备注 |  | | |

## 准入控制

### PC终端准入部署（NACC）

#### web友好引导重定向

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-002-001-001 | 名称 | Portal门户认证 |
| 内容 | 在PC终端使用客户端模式下，使用NACC 端口镜像准入技术，支持多种认证源方式进行身份验证； | | |
| 特殊要求或配置 | 端口镜像； | | |
| 测试步骤 | 1. 配置接入场景； 2. 配置NACC模式设置； 3. 新增准入认证范围； 4. 准入设备接入网络中，网络受限，访问Web跳转重定向页面； 5. Web页面自动跳转引导进行准入身份认证，使用内置账号认证； 6. Web页面自动跳转引导进行准入身份认证，使用LDAP/AD账号认证； | | |
| 预期结果 | 在无客户端模式下，网络受限，Web跳转认证界面，认证通过，网络放开；认证失败/不认证都无法正常上网； | | |
| 测试截图 | 配置接入场景    配置NACC模式设置    终端web重定向页面  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\web重定向1.bmp | | |
| 结论 | ■通过□部分通过□不通过□未测试  通过项目：全部通过。  未通过项目：无。  相关功能可开发项：  相关额外功能： | | |
| 备注 |  | | |

#### PC终端入网认证—AD联动

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-002-001-002 | 名称 | PC终端入网认证—AD联动 |
| 内容 | 针对PC终端入网需要进行身份认证，身份认证体系能与AD域进行联动 | | |
| 特殊要求或配置 | AD认证联动与组织架构同步； | | |
| 测试步骤 | 1. 配置AD联动认证配置：域名、IP、管理权限 2. 配置身份认证联动方式、组织架构同步方式 3. 客户化助手开启AD单点登录配置 4. 终端使用AD账户认证登录 5. 查看所同步的组织架构情况 | | |
| 预期结果 | 能够同步AD组织架构，能够使用AD账户进行身份认证，并支持AD单点登录 | | |
| 测试截图 | AD身份认证联动与单点身份认证：    组织架构同步：    是否加入AD进行检查 | | |
| 结论 | ■通过□部分通过□不通过□未测试  通过项目：全部通过。  未通过项目：无。  相关功能可开发项：  相关额外功能： | | |
| 备注 |  | | |

#### PC终端安全检查

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-002-001-003 | 名称 | PC终端安全检查 |
| 内容 | 针对windows PC终端进行入网安全检查； | | |
| 特殊要求或配置 | LV7000与NID系统联动； | | |
| 测试步骤 | 1、配置接入场景；  2、配置安全检查策略；  3、PC终端接入网络，安装客户端，进行入网认证、安全检查； | | |
| 预期结果 | Windows PC接入网络，身份认证通过后需要进行安全检查，符合管理员安全检查规范要求，如安装指定防病毒软件、补丁等，符合要求才能正常入网； | | |
| 测试截图 | 终端安全检查不通过及引导修复：  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\安检失败引导提示页面.bmp  终端安全检查合规：  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\认证安检合规.bmp | | |
| 结论 | ■通过□部分通过□不通过□未测试  通过项目：全部通过。  未通过项目：无。  相关功能可开发项：  相关额外功能： | | |
| 备注 |  | | |

#### 访客接入

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-002-001-004 | 名称 | 访客接入 |
| 内容 | 通过提供访客入网机制，实现对访客灵活便捷的入网及授权控制； | | |
| 特殊要求或配置 | 端口镜像； | | |
| 测试步骤 | 1、配置访客入网自助账户申请的流程；  2、配置访客审批策略  3、访客通过自助申请访客账户接入  4、管理员审批访客账户  5、管理员查看访客记录 | | |
| 预期结果 | 访客接入可通过web页面进行访客账户自助申请，管理员审批后进行入网，管理员可对访客访问时长、访问资源进行限制，并能够对访客的入网、审批、拜访等全系列信息进行跟踪审计。 | | |
| 测试截图 | 访客账户申请：  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\访客申请.bmp  访客等待审批  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\访客等待审批.bmp  访客审批放行：  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\访客审批放行终端页面.bmp | | |
| 结论 | ■通过□部分通过□不通过□未测试  通过项目：全部通过。  未通过项目：无。  相关功能可开发项：  相关额外功能： | | |
| 备注 |  | | |

#### AD智能准入

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-002-001-005 | 名称 | AD智能准入 |
| 内容 | 通过收集设备与AD服务器协议数据包，获取域账号信息，自动生成认证凭据，实现基于AD账号的智能接入； | | |
| 特殊要求或配置 | 端口镜像； | | |
| 测试步骤 | 1、启用AD智能接入功能；  2、新增准入认证范围；  3、接入设备登陆域桌面，网络受限；  4、等待重认证间隔，设备重新认证，网络放行，显示AD智能接入； | | |
| 预期结果 | 设备刚登陆域桌面后，网络受限，Web跳转认证界面；  等待重认证间隔，设备重新上线，认证直接通过，显示AD智能接入； | | |
| 测试截图 | 启用AD智能接入；    配置准入认证范围；接入设备登陆域桌面，网络受限；等待重认证间隔，设备重新上线，认证直接通过，显示AD智能接入； | | |
| 结论 | ■通过□部分通过□不通过□未测试  通过项目：全部通过。  未通过项目：无。  相关功能可开发项：  相关额外功能： | | |
| 备注 |  | | |

#### 深信服对接

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-002-001-006 | 名称 | 深信服对接 |
| 内容 | 通过与深信服平台做对接，实现单点登录，只需要在联软服务器认证成功后，便可直接上网； | | |
| 特殊要求或配置 | 保证联软服务器和深信服AC能够正常通讯； | | |
| 测试步骤 | 1、联软页面配置第三方上网行为IP地址；  2、设备接入网络，被重定向到认证界面；  3、认证成功后，联软服务器通知第三方上网行为服务器用户上线；  4、第三方上网行为在线用户管理显示设备上线；  5、设备正常上网； | | |
| 预期结果 | 在联软服务器认证成功后，设备正常上网； | | |
| 测试截图 | 启用上网行为功能； | | |
| 结论 | ■通过□部分通过□不通过□未测试  通过项目：全部通过。  未通过项目：无。  相关功能可开发项：  相关额外功能： | | |
| 备注 |  | | |

### 哑终端准入部署（NACC）

#### AB准入认证

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-002-002-001 | 名称 | IAB准入认证 |
| 内容 | 对于哑终端设备，可以采用基于IAB免检白名单方式进行认证； | | |
| 特殊要求或配置 | 策略路由、端口镜像； | | |
| 测试步骤 | 1、配置接入场景；  2、新增免检白名单设备IP地址，基于设备类型分配相应网络权限；  3、配置NACC模式设置；  4、新增准入认证范围；  5、设备接入网络后，认证通过，显示免检认证； | | |
| 预期结果 | 设备接入网络后，正常放行，认证信息显示免检认证； | | |
| 测试截图 | 配置接入场景；    新增免检列表；    配置准入认证范围；    设备接入网络后，认证通过，显示免检认证； | | |
| 结论 | ■通过□部分通过□不通过□未测试  通过项目：全部通过。  未通过项目：无。  相关功能可开发项：  相关额外功能： | | |
| 备注 |  | | |

#### 流量行为检测

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-002-002-002 | 名称 | 流量行为检测 |
| 内容 | 通过分析接入设备的访问行为流量，匹配对应设备类型的流量检测规则，检测是否存在设备被仿冒的现象； | | |
| 特殊要求或配置 | 端口镜像； | | |
| 测试步骤 | 1、配置免检白名单；  2、启用仿冒监测，配置流量检测规则；  3、新增准入认证范围；  4、测试设备访问流量检测规则中定义的异常访问流量； | | |
| 预期结果 | 产生违规记录，并且网络受限，重定向到特定URL； | | |
| 测试截图 | 配置免检白名单    启用仿冒监测，配置流量检测规则    配置准入认证范围；    产生流量行为范围告警；    仿冒设备列表； | | |
| 结论 | ■通过□部分通过□不通过□未测试  通过项目：全部通过。  未通过项目：无。  相关功能可开发项：  相关额外功能： | | |
| 备注 |  | | |

#### 视频码流黑白名单

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-002-002-004 | 名称 | 视频码流黑白名单 |
| 内容 | 基于协议特征的白名单控制机制，只允许授信的视频码流相关的协议在网络中传输，可识别SIP、RTSP、RTP/RTCP、NTP、HTTP、FTP等控制信令及传输协议； | | |
| 特殊要求或配置 | 端口镜像； | | |
| 测试步骤 | 1、配置基于协议的访问权限；  2、测试设备与视频服务器产生视频码流协议； | | |
| 预期结果 | 1、视频服务器接收到视频码流协议的数据； | | |
| 测试截图 | 配置基于协议的访问权限； | | |
| 结论 | ■通过□部分通过□不通过□未测试  通过项目：全部通过。  未通过项目：无。  相关功能可开发项：  相关额外功能： | | |
| 备注 |  | | |

### 逃生机制（NACC）

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-003-001 | 名称 | 一键逃生 |
| 内容 | 测试服务器准入功能异常时，快速逃生功能； | | |
| 特殊要求或配置 |  | | |
| 测试步骤 | 1、当UniRadiusd认证模块异常时；  a) 停掉UniRadiusd模块，或者配置不存在UniRadiusd IP地址；  2、手动切换逃生；   1. 登录Web界面，找到服务管理-逃生模式； 2. 点击逃生模式按钮；   3、断开UniNID镜像口； | | |
| 预期结果 | 1、当UniRadiusd认证模块异常时，自动切换到down\_policy\_acl，更新状态，同时放行所有网络；  2、手动切换逃生，放行所有网络；  3、断开UniNID镜像口，所有接入设备都不受控制； | | |
| 测试截图 | 测试UniRadiusd连通性；    Radius处于down状态，设备自动逃生；    页面切换逃生/或者拔掉镜像线； | | |
| 结论 | ■通过□部分通过□不通过□未测试  通过项目：全部通过。  未通过项目：无。  相关功能可开发项：  相关额外功能： | | |
| 备注 |  | | |

## 网络边界威胁感知

### 攻击行为感知

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-003-001 | 名称 | 攻击行为感知 |
| 内容 | 通过采集镜像过来的流量，匹配攻击行为内置规则，对匹配到攻击规则的行为进行告警展示； | | |
| 特殊要求或配置 | 端口镜像 | | |
| 测试步骤 | 1. 端口镜像流量到NID设备 2. 开启设备自动发现，发现全网设备 | | |
| 预期结果 | 设备能够及时发现全网设备异常攻击行为：  能发现设备伪造、网络扫描攻击、shellcode攻击、cnc攻击、疑似APT、疑似勒索病毒、账户权限破解、木马蠕虫、匿名共享、异常域名访问等各种异常行为，形成统计告警数据、并形成攻击链及攻击取证报告。 | | |
| 测试截图 | 1.设备风险概述  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\设备风险概述.bmp  2.网络扫描攻击  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\网络扫描.bmp  3.CNC攻击  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\CC攻击行为.png  4.shellcode攻击  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\shellcode 攻击.bmp  5.疑似APT僵尸主机  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\疑似僵尸主机.bmp  6.疑似勒索病毒  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\疑似勒索病毒2.bmp  7.攻击链分析  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\攻击链分析.bmp  8.攻击设备分析  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\攻击设备分析.bmp | | |
| 结论 | ■通过□部分通过□不通过□未测试 | | |
| 备注 |  | | |

### 异常行为感知

#### 异常行为分析

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-003-002-001 | 名称 | 异常行为 |
| 内容 | 无监督机器自学习技术，能自动学习网络中设备之间的连接关系，当发现异常访问幻影设备/幻影AD时、设备仿冒时，产生告警； | | |
| 特殊要求或配置 | 端口镜像信息； | | |
| 测试步骤 | 1、默认启用异常行为分析功能；  2、测试设备访问幻影IP地址，例如：SSH、nmap；  3、收集网内设备仿冒行为 | | |
| 预期结果 | 1、，测试设备使用SSH访问幻影设备、或出现设备仿冒时，产生告警； | | |
| 测试截图 | 异常接入—设备仿冒  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\异常行为--设备仿冒.bmp  SSH幻影设备时，产生告警； | | |
| 结论 | ■通过□部分通过□不通过□未测试 | | |
| 备注 |  | | |

#### 异常流量分析

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-003-002-002 | 名称 | 异常流量 |
| 内容 | 无监督机器自学习技术，能自动学习网络中设备的网络流量行为特征，当设备出现异常的流量时，产生告警； | | |
| 特殊要求或配置 | 端口镜像信息； | | |
| 测试步骤 | 1. 默认启用异常流量分析功能； 2. 配置工作时间定义，比如9:00-18:00为上班时间； 3. 测试设备在休息时间内产生流量； | | |
| 预期结果 | 1、测试设备在休息时间内产生流量，产生告警； | | |
| 测试截图 | 配置工作时间；    产生告警； | | |
| 结论 | ■通过□部分通过□不通过□未测试 | | |
| 备注 |  | | |

#### 异常接入位置分析

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-003-002-003 | 名称 | 异常接入位置 |
| 内容 | 对于服务器、哑终端设备、IoT设备等接入位置相对固定的设备，一旦发现设备接入位置发生变化，会立即报警或阻断。 | | |
| 特殊要求或配置 | 端口镜像信息； | | |
| 测试步骤 | 1、默认启用异常接入位置分析功能；  2、修改新设备发现时间间隔，比如调整为30S；  3、调整测试设备的接入位置； | | |
| 预期结果 | 1、调整测试设备的接入位置，产生告警； | | |
| 测试截图 | 设备接入位置发生变化  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\异常行为--设备接入位置IOT设备发生变化.bmp | | |
| 结论 | ■通过□部分通过□不通过□未测试 | | |
| 备注 |  | | |

#### 匿名共享

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-003-002-004 | 名称 | 异常接入位置 |
| 内容 | 对于服务器、哑终端设备、IoT设备等接入位置相对固定的设备，一旦发现设备接入位置发生变化，会立即报警或阻断。 | | |
| 特殊要求或配置 | 端口镜像信息； | | |
| 测试步骤 | 1、默认启用异常接入位置分析功能；  2、修改新设备发现时间间隔，比如调整为30S；  3、调整测试设备的接入位置； | | |
| 预期结果 | 1、调整测试设备的接入位置，产生告警； | | |
| 测试截图 | 设备接入位置发生变化  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\异常行为--设备接入位置IOT设备发生变化.bmp | | |
| 结论 | ■通过□部分通过□不通过□未测试 | | |
| 备注 |  | | |

#### 疑似NAT设备

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-003-002-005 | 名称 | 疑似NAT设备 |
| 内容 | 对网内NAT设备能够进行自动发现 | | |
| 特殊要求或配置 | 端口镜像信息； | | |
| 测试步骤 | 1、网内终端开启360随身wifi、手机模拟器；  2、接入无线NAT小路由器； | | |
| 预期结果 | 1、调整测试设备的接入位置，产生告警； | | |
| 测试截图 | 疑似NAT设备  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\发现疑似NAT设备.png  通过NAT设备接入的终端信息  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\NAT设备信息.bmp | | |
| 结论 | ■通过□部分通过□不通过□未测试 | | |
| 备注 |  | | |

### 域名分析

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-003-003 | 名称 | 域名分析 |
| 内容 | 通过匹配威胁情报恶意域名库，对网络中产生的域名访问记录进行分析，判断是否合法，并且能够定位到网络中的可疑设备； | | |
| 特殊要求或配置 | 需要保证服务器能否联网，同步到公有云的威胁情报恶意域名库； | | |
| 测试步骤 | 1、测试设备访问恶意域名或者恶意IP地址；  2、根据恶意域名/恶意IP地址，追溯访问者的信息； | | |
| 预期结果 | 1、测试设备访问恶意域名或者恶意IP地址，产生告警信息；  2、根据恶意域名/恶意IP地址，追溯访问者的信息； | | |
| 测试截图 | 访问可疑域名告警:  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\可疑域名访问分析.bmp | | |
| 结论 | ■通过□部分通过□不通过□未测试 | | |
| 备注 |  | | |

### 流量分析

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-003-004 | 名称 | 弱口令检测 |
| 内容 | 通过对网络中发现到的设备流量进行统计、分析，分析互联网流量、内网流量、实施流量等详细信息 | | |
| 特殊要求或配置 |  | | |
| 测试步骤 | 1、端口镜像流量； | | |
| 预期结果 | 1、能实时统计全网终端互联网流量地图、内网流量地图、实时流量情况；  2、能形成直观的流量连接图； | | |
| 测试截图 | 流量地图  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\流量地图.bmp  互联网流量：  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\互联网流量.bmp  内网流量：  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\内网流量.bmp | | |
| 结论 | ■通过□部分通过□不通过□未测试 | | |
| 备注 |  | | |

### 弱口令检测

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-003-005 | 名称 | 弱口令检测 |
| 内容 | 通过对网络中发现到的摄像头设备进行Web登录界面暴力破解，检测是否存在弱口令现象； | | |
| 特殊要求或配置 | 适用范围：摄像头； | | |
| 测试步骤 | 1、配置密码数据字典，填写多种出厂密码；  2、点击开始扫描，对已识别到的摄像头设备自动扫描； | | |
| 预期结果 | 1、如果摄像头Web界面登录信息为常规的厂商密码，则产生告警，并输出匹配到的结果；  2、如果摄像头Web界面登录信息不为常规的厂商密码，则扫描到结束； | | |
| 测试截图 | 配置密码数据字典；    开启扫描，扫描完，更新状态；  D:\百度云同步盘\职场\联软\支持项目\苏州科达\测试截图\弱口令扫描.bmp | | |
| 结论 | ■通过□部分通过□不通过□未测试 | | |
| 备注 |  | | |

### 取证报告

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-003-006 | 名称 | 取证报告 |
| 内容 | 以报告形式输出设备的详细信息，以及安全状态，支持导出HTML格式； | | |
| 特殊要求或配置 |  | | |
| 测试步骤 | 1、查看取证报告； | | |
| 预期结果 | |  |  |  |  | | --- | --- | --- | --- | | 测试项目 | | 预期目标 | 真实结果 | | 取证报告 | 设备安全指数 | 能够自动呈现 | 口能/口否/口有误 | | 基本信息 | 能够视图展示 | 口能/口否/口有误 | | 安全感知详情 | 能够视图展示 | 口能/口否/口有误 | | 其他参考信息 | 能够视图展示 | 口能/口否/口有误 | | | |
| 测试截图 | 取证报告： | | |
| 结论 | ■通过□部分通过□不通过□未测试 | | |
| 备注 |  | | |

### 强制下线

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-003-07 | 名称 | 强制下线 |
| 内容 | 通过跟NACC进行联动，对产生告警的设备下发控制命令； | | |
| 特殊要求或配置 | 必须结合NACC准入； | | |
| 测试步骤 | 1、启用VFW过滤，配置限制接入参数；  2、测试设备产生告警（合规检查、异常行为、攻击行为等告警）；  3、启用风险级别设定自动执行NAC强制下线功能； | | |
| 预期结果 | 1、实现控制阻断，下发ACL和重定向URL；  2、严重级别以上告警自动执行NAC强制下线； | | |
| 测试截图 | 强制下线： | | |
| 结论 | ■通过□部分通过□不通过□未测试 | | |
| 备注 |  | | |

## 终端数据防泄密

### 终端外发通道管控

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-004-001 | 名称 | 终端安全管理 |
| 内容 | ■功能 □性能 □安全性 □人机界面 □其它 | | |
| 特殊要求或配置 | 终端外发通道管控测试 | | |
| 测试步骤 | 创建策略并进行外设操作 | | |
| 预期结果 | 支持对终端的外发通道，如端口外设、上网行为、移动存储介质管理等文件外发行为进行管控。 | | |
| 测试截图 | **测试满足；**  支持非授权外联策略、文件读写操作审计策略、打印控制策略、屏幕审计策略、屏幕控制、即时通讯审计、敏感文件审计、文档追踪审计、系统登录审计、邮件审计、移动存储管理等终端外发通道的管控。测试截图如下： | | |
| 结论 | ■通过 □部分通过 □不通过 □未测试 | | |
| 备注 |  | | |

### 敏感文件审计

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-004-002 | 名称 | 终端安全管理 |
| 内容 | ■功能 □性能 □安全性 □人机界面 □其它 | | |
| 特殊要求或配置 | 敏感文件审计 | | |
| 测试步骤 | 配置策略，扫描终端敏感信息及操作行为 | | |
| 预期结果 | 能够对终端敏感信息及时发现并归类 | | |
| 测试截图 | **测试结果说明：**  能够对终端存在的敏感信息及操作行为进行审计  **测试截图：**   1. **敏感信息配置策略：**   **D:\百度云同步盘\职场\联软\联软产品测试截图\数据防泄漏截图\敏感数据基础配置.jpg**  **D:\百度云同步盘\职场\联软\联软产品测试截图\数据防泄漏截图\敏感文件审计配置1.jpg**  **D:\百度云同步盘\职场\联软\联软产品测试截图\数据防泄漏截图\敏感文件审计配置2.jpg**   1. **敏感文件审计信息**   **D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\敏感信息图纸类审计.bmpD:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\敏感信息自查信息.bmp** | | |
| 结论 | ■通过 □部分通过 □不通过 □未测试 | | |
| 备注 |  | | |

### 非授权外联控制（光驱、智能设备、其他外设）

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-004-003 | 名称 | 非授权外联控制 |
| 内容 | ■功能 □性能 □安全性 □人机界面 □其它 | | |
| 特殊要求或配置 | 1. 能够禁止Modem、USB存储设备、可刻录光驱、GPRS、CDMA、红外、蓝牙、1394、串行接口、并行接口、3G、WIFI的使用； 2. 能够禁止同时使用两个以上网络端口，并可以在某些场景下进行例外设置，例如：VPN拨号情况下允许多个网络端口。 3. 支持任意外设接口接入新设备的审计功能 | | |
| 测试步骤 | 创建策略并进行外设操作 | | |
| 预期结果 | 支持非授权外联处理 | | |
| 测试截图 | **测试满足；**测试截图如下：    D:\百度云同步盘\职场\联软\支持项目\宁波华翔\截图\非授权外联.png | | |
| 结论 | ■通过 □部分通过 □不通过 □未测试 | | |
| 备注 |  | | |

### 移动存储介质管理（U盘、移动硬盘）

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-004-004 | 名称 | 终端安全管理 |
| 内容 | ■功能 □性能 □安全性 □人机界面 □其它 | | |
| 特殊要求或配置 | 能对等存储设备管理。支持对U盘管控：禁用、注册、审计、加密等管控 | | |
| 测试步骤 | 配置移动存储介质管理策略，设置网站外发审计，将策略下发到测试终端。 | | |
| 预期结果 | 终端收到策略后插入U盘，U盘不能使用，后台有相应操作审计信息，只有注册U盘才能正常使用；可对U盘使用范围、期限进行设置； | | |
| 测试截图 | **测试满足；**  联软LV70000支持对移动存储介质进行管理，测试截图如下：  1、U盘注册提示信息  D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\未注册U盘注册提示.bmp  2、U盘注册登记信息  D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\U盘注册申请.bmp  3、U盘注册信息待审批记录  D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\U盘待审批信息.bmp  4、U盘注册管理信息  D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\U盘注册信息管理.bmp  D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\注册U盘审批通过后.bmp5、U盘注册审批成功后重点提示信息 | | |
| 结论 | ■通过 □部分通过 □不通过 □未测试 | | |
| 备注 |  | | |

### 屏幕控制管理（防截屏、防拍照）

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-004-005 | 名称 | 终端安全管理 |
| 内容 | ■功能 □性能 □安全性 □人机界面 □其它 | | |
| 特殊要求或配置 | 1. 水印功能可以自定义配置水印形式、水印信息内容、大小、位置及应用范围等；可提供的水印类型，至少需提供屏幕水印、打印水印； 2. 水印类型支持明文、图片、二维码、矢量等多种展现方式 3. 配置禁止截屏策略 | | |
| 测试步骤 | 登录控制台，查看水印方案的相关页面配置。 | | |
| 预期结果 | 1. 支持自定义调整水印信息，密度、透明度、位置等基本属性； 2. 支持明文数字水印，可自定义水印内容，文字大小、颜色、显示位置、排版效果等，并能进行水印效果预览； 3. 水印内容支持宏定义，不同的用户终端可以看到不同的水印信息； 4. 支持二维码水印，可以将水印信息编写为二维码； 5. 支持图片水印，可以将图标、Logo等图片信息设置为水印； 6. 支持矢量水印技术，可以将水印信息编码为矢量点阵水印，在减小用户阅读影响的同时，进行有效管理。 7. 支持禁止终端通过软件或快捷键截屏 | | |
| 测试截图 | **测试满足；**测试截图如下：  1.水印方案    2.终端数字、二维码、矢量水印效果  D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\屏幕数字矢量二维码水印.bmp  3.数字水印效果  D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\屏幕水印.bmp  4.矢量水印效果  D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\屏幕矢量水印.bmp  5.Mac电脑屏幕水印  D:\百度云同步盘\职场\联软\支持项目\上海连尚网络--wifi万能钥匙\wifi万能钥匙测试截图\水印屏幕.jpg  D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\屏幕矢量水印审计信息.bmp6.矢量水印追溯  7.禁止截屏  D:\百度云同步盘\职场\联软\联软产品测试截图\数据防泄漏截图\禁止截屏提示.jpg | | |
| 结论 | ■通过 □部分通过 □不通过 □未测试 | | |
| 备注 |  | | |

### 终端屏幕录像审计

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-004-006 | 名称 | 终端安全管理 |
| 内容 | ■功能 □性能 □安全性 □人机界面 □其它 | | |
| 特殊要求或配置 | 运行指定进程时屏幕录像；访问指定网址时录屏录像； | | |
| 测试步骤 | 1. 配置屏幕录像策略，设置启动录屏进程、访问网址时进行屏幕录像，并将策略下发到测试终端。 2. 测试终端上启动录屏进程，查看是否进行屏幕录像。 3. 测试终端上停止录屏进程，查看屏幕录像是否停止。 4. 访问http://www.XXXX.com时，进行屏幕录像。 5. 停止访问http://www.XXXX.com时，终止屏幕录像。 | | |
| 预期结果 | 1. 启动录屏进程时，进行屏幕录像。 2. 停止录屏进程时，终止屏幕录像。 3. 访问http://www.XXXX.com时，进行屏幕录像。 4. 停止访问http://www.XXXX.com时，终止屏幕录像。 | | |
| 测试截图 | **测试满足；** 测试截图如下：  1.屏幕审计策略：  D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\屏幕审计信息.bmp  2.屏幕审计效果 | | |
| 结论 | ■功能 □性能 □安全性 □人机界面 □其它 | | |
| 备注 |  | | |

### 即时通讯软件审计（QQ、微信外发）

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-004-007 | 名称 | 即时通讯软件审计 |
| 内容 | ■功能 □性能 □安全性 □人机界面 □其它 | | |
| 特殊要求或配置 | 对终端的的即时通讯审计信息、文件传输进行审计与控制 | | |
| 测试步骤 | 配置即时通讯审计策略、敏感信息关键字及条件库并在即时通讯审计策略进行匹配 | | |
| 预期结果 | 能够对终端的即时通讯审计软件如QQ、微信、RTX等常用即时通讯聊天软件的聊天信息、传输文件进行审计，对匹配敏感信息的可进行审计、上传、阻止。 | | |
| 测试截图 | **测试满足；**测试截图如下：  1、即时通讯软件审计策略  D:\百度云同步盘\职场\联软\支持项目\江南布衣测试截图\即时通讯审计策略.bmp  2、即时通讯软件QQ审计信息  D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\即时通讯QQ聊天信息审计.bmp  D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\即时通讯微信聊天审计信息.bmp  D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\即时通讯QQ聊天信息审计列表显示.bmp3.即时通讯微信聊天审计信息 | | |
| 结论 | ■通过 □部分通过 □不通过 □未测试 | | |
| 备注 |  | | |

### 文档操作审计（HTTP及FTP外发、网络磁盘、本地操作）

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-004-008 | 名称 | 终端安全管理 |
| 内容 | ■功能 □性能 □安全性 □人机界面 □其它 | | |
| 特殊要求或配置 | 对终端的文档读写操作进行审计 | | |
| 测试步骤 | 配置文档操作策略、敏感信息关键字及条件库，测试终端通过HTTP、FTP、网络共享磁盘、本地操作等行为涉及到敏感信息文件的情况进行测试 | | |
| 预期结果 | 能够对终端的涉及敏感信息的文档操作内容进行审计、阻止、上传等控制。 | | |
| 测试截图 | **测试满足；**测试截图如下：  1、文档操作策略  D:\百度云同步盘\职场\联软\支持项目\江南布衣测试截图\文档操作审计控制策略.bmp  2、文档操作审计信息  D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\文档操作审计到 不可识别文件.bmpD:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\文档操作审计信息.bmp | | |
| 结论 | ■通过 □部分通过 □不通过 □未测试 | | |
| 备注 |  | | |

### 邮件审计（邮件外发方式）

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-004-009 | 名称 | 终端安全管理 |
| 内容 | ■功能 □性能 □安全性 □人机界面 □其它 | | |
| 特殊要求或配置 | 对终端的邮件发送行为进行审计 | | |
| 测试步骤 | 配置邮件审计策略，对终端通过web、outlook、foxmail等方式进行发送的邮件进行审计 | | |
| 预期结果 | 能够对终端的邮件发送松下进行审计，支持审计邮件正文、附件、标题等详细内容 | | |
| 测试截图 | **测试满足；**测试截图如下：   1. 邮件审计策略   D:\百度云同步盘\职场\联软\支持项目\江南布衣测试截图\邮件审计策略.bmp  2、终端发送邮件时提示界面信息  D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\邮件审计信息.bmp  D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\邮件审计信息1.bmp   1. 邮件审计信息   D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\邮件审计信息2.bmpD:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\邮件审计信息3.bmp | | |
| 结论 | ■通过 □部分通过 □不通过 □未测试 | | |
| 备注 |  | | |

### 打印控制与审计（打印传真外发方式）

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-004-0010 | 名称 | 终端安全管理 |
| 内容 | ■功能 □性能 □安全性 □人机界面 □其它 | | |
| 特殊要求或配置 | 对客户端通过打印传输敏感信息的事件进行检查：  支持对网络打印机、串口打印机，打印涉密或非涉密文档（5种以上的文档格式）的行为进行审计管控。 | | |
| 测试步骤 | 1. 配置打印控制策略，选择指定的关键字模板，配置当符合关键字模板时禁止并审计。打印机型号选择所有打印机； 2. 自定义配置弹出提示，配置策略生效场景为在线离线都生效； 3. 分别用网络打印机、串口打印机，打印涉密或非涉密文档； 4. 查看打印控制审计信息。 | | |
| 预期结果 | 1. 针对打印文件可以进行禁止、审计、备份等管控操作；审计打印文件时，对打印的页数、份数做针对性处理； 2. 可对其打印文件进行敏感检查，涉及敏感数据可阻止、审计。 | | |
| 测试截图 | 1. 打印审计信息   D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\打印控制审计信息.bmp  D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\打印矢量水印审计信息.bmp  2、打印加载矢量水印效果  D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\打印数字水印信息.bmp  3、打印加载数字水印效果  D:\百度云同步盘\职场\联软\支持项目\苏州科达\科达 防泄密测试截图\打印矢量水印信息.bmp | | |
| 结论 | ■通过 □部分通过 □不通过 □未测试 | | |
| 备注 |  | | |

## 终端桌面安全管理

### 软件下发管理

#### 软件分发管理

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-005-001-001 | 名称 | 终端安全管理 |
| 内容 | ■功能 □性能 □安全性 □人机界面 □其它 | | |
| 特殊要求或配置 | 1. 软件下发：支持MSI,EXE等常规软件的下发，自动安装，支持通过网段、OU进行批量下发。 2. 断点续传：桌面管理系统软件分发支持断点续传，如果在软件分发过程中网络断开或者终端设备被关机，当网络连接正常后，桌面管理系统客户端代理能够从原来的文件下载点开始继续下载软件。 3. 分发模式：管理员为某个软件分发任务设置的应用范围可以是IP地址范围、网段、部门、某类设备、某类操作系统等。桌面管理系统会根据设置的应用范围自动将软件分发到目标终端。 4. 软件分发过程监控：桌面管理系统可以让管理员查看某个软件分发任务的执行情况，包括软件分发任务执行统计信息和每台终端设备的执行状态。 | | |
| 测试步骤 | 创建软件派发策略并进行派发 | | |
| 预期结果 | 支持对软件派发进行管理 | | |
| 测试截图 | 联软LV7000软件分发支持windows\linux\macos,支持合规软件正版化的软件仓库管理，支持软件发布、软件分发、授权及套件订单管理；测试截图如下：    D:\百度云同步盘\职场\联软\支持项目\哔哩哔哩\哔哩哔哩测试\14.png  D:\百度云同步盘\职场\联软\支持项目\哔哩哔哩\哔哩哔哩测试\16.png | | |
| 结论 | ■通过 □部分通过 □不通过 □未测试 | | |
| 备注 |  | | |

#### 软件仓库

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-005-001-002 | 名称 | 终端安全管理 |
| 内容 | ■功能 □性能 □安全性 □人机界面 □其它 | | |
| 特殊要求或配置 | 1. 支持软件仓库管理，创建单位内部的合法、正版化软件来源库； 2. 支持对软件仓库内的软件进行软件派发，在终端助手界面有软件商城界面，支持对管理员分发的软件进行安装，管理端拥有完整的统计信息； 3. 支持一些常用系统维护工具的派发，便于终端用户自助运维管理。 | | |
| 测试步骤 | 上传合规化软件，并进行发布、派发 | | |
| 预期结果 | 支持对软件商城进行管理 | | |
| 测试截图 |  | | |
| 结论 | ■通过 □部分通过 □不通过 □未测试 | | |
| 备注 |  | | |

### 资产/IT设备管理

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-005-002 | 名称 | 终端安全管理 |
| 内容 | ■功能 □性能 □安全性 □人机界面 □其它 | | |
| 特殊要求或配置 | 1. 系统至少支持采集网络打印机、终端的计算机名称、所安装的操作系统、应用软件、IP地址、CPU信息、内存信息、磁盘信息、品牌等配置信息。 2. 系统至少能够对终端软件信息进行收集，形成软件库信息列表并支持导出。 3. 支持软件授权、正版化、免费软件商业软件管理。 | | |
| 测试步骤 | 查看资产信息 | | |
| 预期结果 | 支持对软硬件资产进行有效管控 | | |
| 测试截图 | **测试满足；**  联软LV7000支持软硬件资产收集、设备全生命周期管理，测试效果截图如下：  D:\百度云同步盘\职场\联软\支持项目\哔哩哔哩\哔哩哔哩测试\8.png  D:\百度云同步盘\职场\联软\支持项目\哔哩哔哩\哔哩哔哩测试\10.pngD:\百度云同步盘\职场\联软\支持项目\哔哩哔哩\哔哩哔哩测试\9.png | | |
| 结论 | ■通过 □部分通过 □不通过 □未测试 | | |
| 备注 |  | | |

### 远程协助与维护

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-005-003 | 名称 | 终端安全管理 |
| 内容 | ■功能 □性能 □安全性 □人机界面 □其它 | | |
| 特殊要求或配置 | 1. 管理员通过桌面管理系统的管理界面可以直接登录到远程终端，实时看到远程终端的屏幕、操作远程终端的鼠标和键盘。桌面管理系统实现：（1）远程监控（2）远程协助。（3）远程文件管理 2. 终端可自助申请远程协助管理，向在线管理员或所属部门的分级管理员进行远程协助申请，提高远程协助效率。 | | |
| 测试步骤 | 1. 管理员远程管理终端用户 2. 终端用户主动发起远程申请 | | |
| 预期结果 | 支持远程协助的主动、被动申请管理 | | |
| 测试截图 | **测试满足；**  联软LV7000支持远程协助，并支持mac远程,且支持由用户主动发起远程协助申请；并支持NAT环境下远程协助，测试截图如下：      D:\百度云同步盘\职场\联软\支持项目\爱奇艺\截图\mac系统远程.pngD:\百度云同步盘\职场\联软\联软产品测试截图\数据防泄漏截图\远程协助.jpg | | |
| 结论 | ■通过 □部分通过 □不通过 □未测试 | | |
| 备注 |  | | |

### 终端安全加固管理

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | NID-005-004 | 名称 | 终端安全管理 |
| 内容 | 通过配置终端安全管理策略，实现终端桌面安全管控 | | |
| 特殊要求或配置 |  | | |
| 测试步骤 | 1. 配置桌面终端安全管理各项策略； 2. 利用终端安全管理系统来进行桌面终端运维管理； | | |
| 预期结果 | 能够实现对桌面终端的管理，加强终端安全加固，简化桌面运维； | | |
| 测试截图 | **测试满足；**  C:\Users\GONGYI~1\AppData\Local\Temp\1540447829(1).png | | |
| 结论 | ■通过□部分通过 □不通过 □未测试 | | |
| 备注 |  | | |

|  |  |
| --- | --- |
| 平结论 | ■通过□部分通过□不通过□未测试 |
| 备注 |  |