ICS 33.040.01
CCS I6540

T/NIDA

全 球 固 定 网 络 创 新 联 盟

T/NIDA 002-2024

智慧园区网络智能化运维能力技术要求

Technical Requirements for Intelligent O&M Capability of Smart Campus Networks

2024-12-25 发布 2024-12-25 施行

全球固定网络创新联盟（NIDA）发布

目　次

前　言

本文件按照 GB/T 1.1-2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利权和著作权。本文件的发布机构不承担识别专利和著作权的责任。全球固定网络创新联盟不对标准涉及专利的真实性、有效性和范围持有任何立场；不涉足评估专利对标准的相关性或必要性；不参与解决有关标准中所涉及专利的使用许可纠纷等。

本文件由全球固定网络创新联盟技术委员会提出并归口。

本文件起草单位：中国信息通信研究院、中国联合网络通信有限公司研究院、江苏省未来网络创新研究院、华为技术有限公司、中宇联云计算服务（上海）有限公司 、深圳未来智联网络研究院、科大讯飞股份有限公司、苏州盛科通信股份有限公司。

本文件主要起草人： 马军锋、韩赛、刘春、王春生、张力、邓小军、袁新星、汪国进、王祥光、谢乐权、康俊燕、黄川、鲍中帅、王俊杰。

智慧园区网络智能化运维能力技术要求

1 范围

本文件规定了智慧园区网络智能化运维能力技术要求，涵盖园区无线和有线网络，包含自动化、运维排障、体验保障、安全运营、绿色节能等不同维度基于AI大模型的智能化运维场景和技术要求。

本文件适用于智慧园区网络运维，主要用于智慧园区网络智能运维系统的设计、研发、评估、测试等。。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

[1]. YD 0229-2023 信息通信网运营管理智能化水平分级技术要求 通用部分
[2]. YD 1653-2022 信息通信网运营管理智能化水平分级评估技术要求 通用部分

3 术语和定义

3.1 智慧园区智能运维术语

3.1.1

园区网络 campus network

本文中使用“园区网络”泛指企业或者机构的内部网络，主要由路由和交换基础设施组成，将办公相关的计算机、服务器、打印机等，和管理服务设施相关的摄像头、闸机等，以及无线控制器、无线接入点等设备连接到网络，实现园区企业设备互联和信息互通。

3.1.2

网络运营管理大模型 network operation and management large model

本文中使用“网络运营管理大模型”泛指结合网络运营管理领域数据和通用大模型训练得到的一种行业大模型，可适配网络运营管理领域的特定任务和场景需求。

3.1.3

自智网络等级 autonomous networks level

本文中使用“自智网络等级”泛指用于评估网络运维智能化等级的指标，定义了自智网络的5个等级。

4 缩略语

下列缩略语适用于本文件。

Agent 代理（Agent）

AI 人工智能（Artificial Intelligence）
AP 无线接入点（Access Point）()
AR 接入路由器（Access Router))
CASB 云访问安全代理（Cloud Access Security Broker）
Copilot 辅助系统（Copilot System）
DHCP 动态主机配置协议（Dynamic Host Configuration Protocol）
EDR 端点检测与响应（Endpoint Detection and Response）
EPP 企业防病毒（Enterprise Protection Platform）
ESN 唯一设备序列号（Electronic Serial Number）
FME 现场维护工程师（Field Maintenance Engineer）
FW 防火墙（Firewall）
HIPS 主机入侵检测系统（Host Intrusion Prevention System）
IAM 身份和访问管理（Identity and Access Management）
ICT 信息通信技术 （Information and Communication Technology））
IDS 入侵检测系统（Intrusion Detection System）
iFIT 随流检测（In-situ Flow Information Telemetry）
IP 网际互连协议（Internet Protocol）
IPS 入侵防护系统（Intrusion Prevention System）
LLDP 链路层发现协议（Link Layer Discovery Protocol）
LSW 三层交换机（Layer 3 Switch）
MAC 媒体存取控制位址（Media Access Control Address）
NDR 网络威胁检测（Network Threat Detection）
QoS 服务质量（Quality of Service）
SDN 软件定义网络（Software Defined Network）
SOAR 安全自动化编排与响应（Security Orchestration, Automation, and Response）
SSE 安全资源池（Security Services Edge）
SWG 上网行为管理（Secure Web Gateway）
VLAN 虚拟局域网（Virtual Local Area Network）
VN 虚拟网络（Virtual Network）
VPN 虚拟专业网（Virtual Private Network）
VXLAN 虚拟扩展局域网 （Virtual Extensible Local Area Network）
ZTNA 零信任网络访问（Zero Trust Network Access）
ZTP 零接触部署（Zero Touch Provisioning）

5 智慧园区网络智能化运维目标场景

5.1 以“体验为中心”的运维

园区当前以设备为中心的“救火式”运维，无法感知体验，被动响应“故障”发生，依赖现场定位和修复，故障恢复时间长，无法满足智慧园区数字化新空间的运维需求，需要升级为“以体验为中心”的运维。

“以体验为中心”的 运维，包含两个方面的能力提升：一方面是感知体验，对体验进行可视化管理，包括对单用户和全局用户的360°体验可视化和旅程回放；另一方面是主动识别用户和业务的体验问题，发

现潜在故障并识别根因，最终给出修复建议甚至自动修复，主动响应故障发生。

基于“以体验为中心”的运维理念构建的园区网络架构，相比较传统的园区网络运维方案，有如下变化：

— 通过网络智能分析器基于大数据和 AI 的智能分析，感知用户和应用的体验，发现故障和潜在故障并识别根因，并将结果通过符合 IT 运维人员的工作思路，友好地展示出来。
— 为了支撑网络智能分析器的智能分析，网络设备具备数据采集和一定边缘智能分析能力，并进行实时数据上报。

5.2 无人值守园区

AI与运维的结合正在彻底重塑传统的运维模式。这种变革基于大数据的感知与采集，通过大模型与小模型的协同作用，实现实时与预测性分析。在这一过程中，人工智能正逐步取代人工进行高效的沟通、分析与决策，推动向更为精准、前瞻的智能运维模式演进。大模型的应用对园区网络运维的提升主要体现在如下方面：

— 数据感知与认知：在智能运维的领域中，实时、准确、全面的数据感知与认知，为运维决策提供数据支撑。园区运维智能体通过全面感知和高效采集 ICT 设施的状态、连接关系及相关变化，结合数字孪生技术，将物理实体数字化，形成虚拟孪生的数字世界。这种物理与虚拟空间的相互映射，为运维提供全新的视角，提升了 ICT 设施的可观测性、可分析性和可预测性，从而实现园区 ICT 设施的高效管理和控制。
— 故障智能处置：随着园区创新业务的蓬勃发展，ICT 故障对业务运营造成的潜在经济损失愈发显著，这使得园区对故障处理效率的要求日益严苛。传统运维方式在短时间内只能处理少量数据，在涉及跨域联合定位效率更低，难以满足高效故障处理的需求。智能故障处置通过实时收集和分析设备或系统的运行数据，能够自动检测、诊断和处理故障，从而减少对人工干预的依赖，提高故障处理的效率和准确性。

6 智慧园区智能运维架构

智慧园区数智化需求的演变，以及 AI 大模型、数字孪生、跨领域融合等技术的持续创新，推动智慧园区网络运维面向智能化构建新的技术能力。智慧园区网络智能化运维架构图 1 所示：

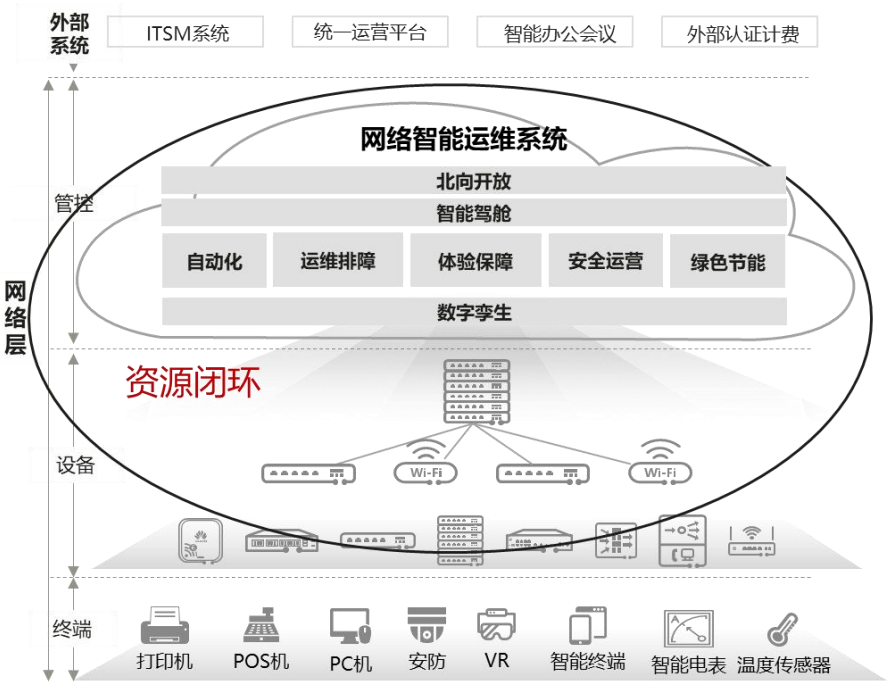

图 1智慧园区智能运维架构

智慧园区网络智能化运维架构，以网络智能运维系统为园区网络新大脑来构建基于资源闭环的智能运维关键能力。该运维系统北向对接各类OSS/BSS外部系统，通过服务化接口提供网络级服务能力；南向对接不同网络设备以获取终端、网元、用户的各类信息，基于数字孪生体和智能驾舱对园区网络执行管理、控制和分析等运维操作。

作为园区网络的运维新大脑，网络智能运维系统应具备网络自治关键特征，自下而上包括：

—数字孪生：园区物理网络和数字网络无缝衔接、协同是园区智能化、智慧化的特点。智慧园区网络运维的数字孪生是通过创建园区物理网络的虚拟模型，对园区物理网络相关的数据建模，完善数字空间，进而形成相关的运维服务。围绕上述物理网络到数字网络的映射过程，数字孪生具备感知多维化、数字建模、虚实协同，智能分析等关键能力。

—运维能力：通过数字孪生和智能驾舱的融合，实现智慧园区网络在自动化、运维排障、体验保障、安全运营、绿色节能等运维场景中意图、感知、分析、决策、执行、验证的网络自治资源闭环能力，覆盖规划、建设、维护、优化、运营的各个网络运维环节。智慧园区网络的智能运维涵盖如下场景：

- 自动化：智慧园区网络规模和复杂度增加，自动化诉求相应增大。从物理网络建设阶段的分支极简开局，到终端用户接入阶段的业务策略自动化部署，以及面向多业务园区的逻辑网络自动化是智慧园区网络实时自动化的重点场景。
- 运维保障：面向“无人值守园区”的运维目标，通过 AI 和大模型，注智到告警、故障定界定位、报表等通用运维排障场景，构建运维排障的智能化闭环处理能力。
- 体验保障：以“体验为中心”，是在智慧园区的多维状态可视、用户级和应用级体验以及可视化巡检等方面增强体验，建立可视、可分析、可优化、可实施的闭环能力。
- 安全运营：智慧园区不断丰富的业务类型使得园区安全成为运维重点。智慧园区的安全运维闭环要覆盖安全策略布防、高精度威胁检测和快速威胁响应的闭环。
- 绿色节能：智慧园区网络智能运维增强绿色节能能力，是智慧园区运维运营的重点需求。

—智能驾舱：基于网络大模型和生成式AI，围绕园区运维智能化，构建E2E决策闭环体验的智慧操作能力，可以准确识别园区网络运维意图，实现园区智慧化运维处置，达到TTM&MTTR最优。

—开放生态：面向智慧园区网络的智能运维闭环是智慧园区实现自智网络的一部分，通过开放生态与其他系统在API开放、数据开放、准入开放进行集成，达成园区整体智能运维。

7 智慧园区智能运维能力技术要求

7.1 自动化

7.1.1 物理网络自动化

7.1.1.1 网元自动化发现

智慧园区场景复杂，包含简单业务园区、多业务园区、分支互联园区不同场景，要求网络快速规划部署，以支持新建、搬迁等常见场景。ZTP极简开局可以有效缩短网络开通周期，提高网络开通准确性。ZTP极简开局主要是通过多种开局方式支持不同类型园区的多种设备即插即用，关键能力定义如下：

a) 支持ZTP极简开局
   1) 支持通过APP的ZTP极简开局，适用于AP设备；
   2) 支持DHCP方式的ZTP极简开局，适用于AP、LSW、AR设备；
   3) 支持注册查询中心方式的ZTP极简开局，适用于AP、LSW、AR、FW设备；
   4) 支持邮件开局方式的ZTP极简开局，适用于SD-WAN场景。
b) 支持免录入ESN开局
   1) 支持基于LLDP扫描方式免录入ESN开局；
   2) 支持基于DHCP方式免录入ESN开局。

7.1.1.2 设备配置自动化下发

在园区场景中，海量分支配置类同，单次配置修改多次重复操作导致配置下发效率低且容易出错。设备配置自动化关键能力定义如下：

a) 支持多层次模板化配置方式，支持海量分支批量配置复制下发。

7.1.1.3 网络变更自动化

园区网络针对业务量变化实时针对性的带宽规划能提高网络承载力的同时有效降低网络成本。网络变更自动化关键能力定义如下：

a) 支持链路带宽自动规划，通过对网络带宽使用情况进行深度分析，精准规划网络带宽。

7.1.2 业务策略自动化

7.1.2.2 终端智能管理

智慧园区中海量终端接入，打破了物联边界，传统的基于人工采集终端MAC地址并录入认证系统的方式，导致终端接入慢，且无法有效识别仿冒、私接等安全隐患，同时也增加了故障定位精细化管理难度。终端智能管理是指通过物联终端AI聚类识别技术实现终端的准确识别并支持终端安全接入，关键能力定义如下：

a) 支持识别动态接入和静态接入的终端，包括但不限于计算机、移动终端、摄像头等；
b) 支持识别终端类型、厂商、型号、操作系统等；

c) 支持终端认证授权，支持零仿冒、零私接，包括但不限于HUB防私接、路由器防私接、WIFI共享防私接；
d) 支持异常终端自动化阻断，包括但不限于MAC阻断、端口shutdown阻断等；
e) 支持与第三方厂家联动提供终端安全检查功能，包括但不限于奇安信等。

7.1.2.1 用户接入认证

在智慧园区中，大量用户接入，终端类型丰富，接入方式多样化。支持用户接入认证主要是提供多种认证方式和不同的接入策略控制，关键能力定义如下：

a) 支持多种认证方式，包括但不限于portal认证、对接第三方portal认证、802.1认证、PPSK认证、MAC认证等；
b) 支持多种用户身份来源，包括但不限于自建账号、对接社交媒体网站、对接第三方数据库、对接第三方HTTP服务器、对接第三方Radius服务器，对接Token服务器，证书认证等；
c) 支持智能策略，基于用户身份、接入位置、接入时间、终端类型、设备属性和接入方式实现精细化的权限、带宽、QoS、应用和安全控制。

7.1.2.4 访客管理

支持访客管理是对访客进行全生命周期管理，满足不同场景需求，关键能力定义如下：

a) 支持访客注册、审批、账号分发、注销；
b) 支持访客认证，包括但不限于匿名认证、用户名/密码认证、手机验证码认证、社交媒体认证；
c) 支持访客审计，包括但不限于用户上下线审计、定时清理账号等。

7.1.2.5 支持业务随行

园区用户要求随时随地接入网络，并且要求业务策略和网络体验能够保持一致。业务随行是通过技术升级在不依赖特定组网的情况下实现用户的访问控制策略一致性，关键能力定义如下：

a) 支持基于用户组的访问控制策略，包括权限、应用、安全策略；
b) 支持认证点与策略点不分离情况下的业务随行功能；
c) 支持认证点与策略点可分离情况下的业务随行功能，并可兼容第三方组网。

7.1.2.6 智能 QoS 保障策略

智慧园区提供大量丰富的应用，用户之间、用户的应用之间的需求多样性，需要更精细化的网络资源控制，最大化满足不同用户的诉求。智能QoS保障策略是通过精细化的策略控制保障用户端到端的业务体验诉求，关键能力定义如下：

a) 支持有线网络基于用户和应用双因素的HQoS策略部署，支持每应用每用户4级队列缓存和整形；
b) 支持无线网络基于用户和业务优先级的调度策略，支持空口切片技术应用。

7.1.2.7 智能安全策略

智慧园区用户需要访问互联网、SaaS、企业私有应用等，需要更精细化的安全权限管控和一站式安全策略发放。智能安全策略是通过一站式安全策略发放来保障用户端到端的业务权限，关键能力定义如下：

a) 支持用户到应用、网段到网段的一站式安全策略发放；
b) 支持智能推荐用户访问应用需经过的网络和安全设备；
c) 支持智能检查安全策略是否符合企业合规性要求；
d) 支持智能诊断用户到应用、网段到网段之间的策略路径及策略命中规则。

7.1.3 虚拟网络自动化

在多业务园区场景中，一套物理网络需要承载多种业务，通过逻辑隔离可以节省成本。虚拟网络的规划和部署及用户认证自动化，应支持分钟级完成网络调整来提升效率。虚拟网络自动化指通过自动化能力完成虚拟网络的规划、部署及用户认证，关键能力定义如下：

a) 支持虚拟网络自动化规划部署，包括但不限于VPN、VXLAN方式虚拟网络类型；
b) 支持虚拟网络间隔离策略自动化部署；
c) 支持虚拟网络内不同用户网络权限通过用户组进行划分。

7.2 运维排障

7.2.1 数据采集

智慧园区网络实现智能运维的基础是对网络实时、准确、全面的数据感知与认知，关键能力定义如下：

a) 支持秒级的海量数据汇集，包括但不限于Telemetry数据采集；
b) 支持网络基础数据、状态数据、质量数据采集，包括但不限于存量、拓扑、配置、协议状态、告警、日志、光模块、流量统计等；
c) 支持网络资源数据采集，包括但不限于IP、ACL、VRF、VLAN/BD等；
d) 支持网络流量数据采集，包括但不限于网络流量报文采集；
e) 支持应用基础数据采集，包括但不限于服务器、网络接口卡、应用、IP等。

7.2.2 智能告警

智慧园区中存在大量无效告警，告警屏蔽规则配置繁琐且缺乏历史告警分析能力。智能告警指基于大模型开展告警智能分析，关键能力定义如下：

a) 支持告警分析报表，综合分析当前告警和历史告警，分析告警趋势，自动生成屏蔽规则；
b) 支持按照告警严重程度、业务影响程度等维度进行告警规则的分级管理；
c) 支持基于大模型辅助消除无效告警。

7.2.3 多维可视

多维可视构建“以体验为中心”的多维立体数字空间，基于数字孪生进行网络多维可视化，关键能力定义如下：

a) 支持GIS地图展示能力；
b) 支持网络状态可视，包括但不限于设备状态、链路状态、拓扑等；
c) 支持终端状态可视，包括但不限于终端类型、状态、拓扑位置等；
d) 支持用户体验可视，包括但不限于用户体验评分、接入指标参数、用户故障原因分析等；
e) 支持应用体验可视，包括但不限于时延、流量、抖动、异常流、故障的拓扑位置和原因分析等；
f) 支持异常流量可视，包括但不限于实时检测网络异常流量并解决异常流造成的高优先级应用丢包，如站点、链路拥塞可视；支持针对站点、链路的异常流检测，支持获取异常流及应用信息；支持基于异常流的处置策略自动部署。

7.2.4 AI 定界定位

智慧园区中，网络无线化加剧，用户需求多样，漫游、潮汐、双栈等现象复杂多变，掉线问题频出。传统运维方式业务恢复时间长，导致投诉增多。基于AI大模型的Copilot和Agent可用于网络故障快速定界、

故障根因精准定位和故障问题自动化修复的运维快速闭环，关键能力定义如下：

1) 支持基于自然语言的交互方式进行问题定位；
2) 支持给出合理化修复建议，根据用户需求生成图表及分析总结，如运营汇报、成果展示等；
3) 支持提供日常运维查询和辅助排障；
4) 支持无线网络故障定界定位，基于AI故障推理，精确匹配故障场景，包括但不限于接入类（如认证失败、认证超时、用户集体下线、DHCP失败、用户网关不可达等）、漫游类（如乒乓漫游、漫游异常等）、空口性能类（如覆盖弱、信道利用率高、高干扰、非5G优先、终端容量、空口拥塞等）等场景；
5) 支持有线网络故障定界定位，A基于AI故障推理，精确匹配故障场景，包括但不限于物理器件状态异常、设备资源数量/容量异常、网络协议异常、数据传输异常、吞吐异常、网络接口状态异常等场景；
6) 支持精准根因分析，基于AI推理和故障知识库，精准识别故障根因；
7) 支持基于根因自动生成解决方案并实施闭环操作。

7.2.5 智能报表

智慧园区网络运维通常有不同的关注项，智能报表是在网络大模型技术支持下，基于人工交互方式，按需定制报表，关键能力定义如下：

a) 支持自然语言交互式报表定制；
b) 支持报表覆盖网络、WIFI、用户不同等级关键指标；
c) 支持多样呈现方式，多维统计的报表能力；
d) 支持对定制的报表进行实时预览和生成；
e) 支持报表周期性生成和发送。

7.2.6 智能校验

传统园区网络变更主要依赖人工检查和流量监控这两类传统运维手段，具有随机性和不确定性。智能校验是提供网络变更的智能化对比和验证，关键能力定义如下：

a) 支持快照对比，可以发现如设备、配置文件、接口链路状态、IP路由等的差异；
b) 支持子网互访验证，覆盖全网所有业务子网之间的连通性；
c) 支持终端接入验证，实时精准模拟和校验终端接入权限是否精准；
d) 支持多场景覆盖，包括但不限于新建、终端/人员扩容、组织搬迁/切换、专线切换等场景。

7.3 体验保障

7.3.1 用户级体验

用户级体验指呈现和保障每用户每时刻的网络体验，关键能力定义如下：

a) 支持基于用户的体验可视，包括但不限于接入网络的时间和位置、用户认证结果、用户漫游、用户质量等信息；
b) 支持用户旅程的历史回放，基于时间和空间维度回放历史数据；
c) 支持用户保障，支持用户体验劣化告警通知和分析处理，生成保障策略（包含WIFI等）自动下发；

7.3.2 应用级体验

应用级体验指呈现和保障每用户每应用每时刻的网络体验，关键能力定义如下：

a) 支持基于AI的应用自动识别，包括但不限于微信、支付宝等常见应用；
b) 支持应用流量可视，包括但不限于时延、丢包、抖动等应用质量信息；
c) 支持应用质量劣化的自动故障分析，支持应用级故障定界定位(如iFIT技术等)；
d) 支持应用保障，支持应用体验劣化告警通知和分析处理，生成保障策略自动下发；
e) 支持应用质量可回放，基于时间和空间维度回放历史数据；
f) 支持全网应用智能选路，支持推荐最优全网选路策略；

7.3.3 可视化巡检

园区网络日益庞大复杂，设备和终端数量急剧增长。网络例行维护变工作量增加。可视化巡检是基于数字孪生进行网络智能巡检，关键能力定义如下：

a) 支持云端设备巡检，实现对网络的全面检查，对整网进行在线深度健康监测，实时保障网络健康运行，包括但不限于全网故障分布可视，链路拥塞可视，站点、设备、应用、用户、链路状态可视等；
b) 支持云端设备巡检报告分析，包括但不限于以下功能：
    1) 支持无线网络健康评估，包括但不限于接入成功率、接入耗时等；
    2) 支持有线网络健康度评估：包括但不限于网络性能、网络状态等；
    3) 支持网络典型故障根因分析：包括但不限于认证失败、高干扰、二层环路、端口闪断等；
    4) 支持无线网络智能调优，包括但不限于容量、干扰、漫游、覆盖等调优；
c) 支持提供云端设备巡检问题处置方法与闭环手段。

7.4 安全运营

7.4.1 安全策略高效布防

园区网络和业务日益复杂，例如远程办公、分支本地出局等场景，使得企业的安全布防难度日益增加。安全策略高效布防是指有效地安全管控，关键能力定义如下：

a) 支持零信任（ZTNA），具备对内网接入或远端接入的资产进行持续的零信任评估，一旦发现不符合安全基线或安全风险，自动对资产的访问权限进行降级甚至拒绝接入，有效保障客户网络安全；
b) 支持上网行为管理（SWG），具备对客户的安全上网进行权限管控，如WEB过滤、应用管控等；
c) 支持云访问安全代理（CASB），具备对企业用户访问SaaS应用进行安全管控的能力；
d) 支持安全资源池（SSE），具备对跨地域、跨境企业提供安全资源池能力，安全资源池不仅提供高速访问的能力，还提供入侵检测系统（IDS）、入侵防护系统（IPS）、防病毒（AntiVirus）、WEB过滤等安全能力。

7.4.2 威胁高精度检测

园区网络日益庞大复杂，设备和终端数量急剧增长，用户接入复杂多样，面临更多的安全威胁。威胁高精度检测指威胁多维、实时监测和检测，实时监控园区内各个设备和系统的运行状态，及时发现异常行为和安全事件，关键能力定义如下：

a) 支持网络威胁检测 (NDR) , 具备对网络流量进行威胁检测能力, 包括但不限于入侵检测系统 (IDS) 、入侵防护系统（IPS）、防病毒（AntiVirus）等；
b) 支持终端威胁检测（EDR），具备通过EDR代理对终端行为进行威胁检测能力，包括但不限于主机入侵检测（HIPS）、杀毒（EPP）等；
c) 支持沙箱检测，具备对未知威胁进行威胁检测能力，如通过观察文件异常行为及组合来确定威胁等。

7.4.3 威胁快速响应

园区威胁事件响应处置难度日益增加，需要频繁地进行事件研判和处置。威胁快速响应是基于XDR关联分析、网安融合数字地图、安全自动化编排与响应（SOAR）、AI运营助手等进行威胁事件研判处置，关键能力定义如下：

a) 支持XDR关联分析，自动关联分析网边端事件，高聚合、高清还原威胁事件攻击链；
b) 支持网安融合数字地图，如自动评估站点和资产的安全风险评分、风险分布和风险扩散详情等，结合网络拓扑高精溯源；
c) 支持安全自动化编排与响应（SOAR），支持网安协同action和playbook，自动化响应处置威胁事件，近源阻断安全威胁；
d) 支持基于AI大模型实现威胁事件的辅助研判和辅助处置。

7.5 绿色节能

绿色节能是指可视化网络节能状态，并通过大数据智能识别用网场景来推荐最优节能策略，以便合理调整能源供应和使用，从而实现节能和优化能源利用的目标。绿色节能关键能力定义如下：

a) 支持网络能耗可视，支持呈现园区网络内各个站点及站点下各个设备的能耗数据，包括但不限于碳排放量可视、能耗电费可视、节省能耗可视等；
b) 支持网络动态节能，根据网络负载、时段等参数自动调整设备功率、设备开关等实现节能，包括但不限于：
    1) 支持智能识别用网场景，并推荐最优节能策略；
    2) 支持哨兵选择，工作时段轻载哨兵识别、加班时段动态哨兵识别；
    3) 支持智能唤醒，与LSW、AC、AP侧协同完成快速唤醒，保障用网体验与网络能耗平衡。

7.6 开放生态

智慧园区网络智能运维系统支持开放能力，可与外部系统进行交互和集成，以实现整体运维运营的自动化和智能化。开放生态的关键能力定义如下：

a) 支持能力API开放，包括但不限于网络自动化API、网络运维API、认证授权API、数据分析API等；
b) 支持数据API开放，包括但不限于网络、用户、应用、终端等数据的API；
c) 支持准入API开放，支持与外部IAM认证系统集成。