

iNet 智能运维平台 白皮书

深圳天元云科技有限公司

二〇二五年三月

深圳天元云科技有限公司（以下简称“深圳天元云”）及其许可者版权所有，保留一切权利。未经深圳天元云书面许可，本文档不得整体或部分地复印、复制、翻译或缩减成任何电子介质或计算机可以阅读的格式。

免责声明：

由于产品版本升级或其他原因，本手册内容有可能变更。深圳天元云保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。深圳天元云尽全力在本手册中提供准确的信息，但是深圳天元云并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

联系信息：

地址：深圳市福田区车公庙天安数码城创新科技广场一期 A 座 601C

电话：400-8120-996 0755-88600490

目录

- 1 前言 - 5 -
- 2 平台概述 - 6 -
 - 2.1 设计理念 - 6 -
 - 2.2 产品定位 - 6 -
 - 2.3 产品优势 - 6 -
 - 2.4 产品体系架构..... - 8 -
 - 2.5 软硬件环境要求..... - 8 -
- 3 iNet 智能运维系统..... - 9 -
 - 3.1 产品功能 - 9 -
 - 3.1.1 全面设备管理 - 9 -
 - 3.1.2 网络可视化 - 9 -
 - 3.1.3 流程自动化 - 9 -
 - 3.1.4 新增策略分析 - 10 -
 - 3.1.5 优化、合规检查 - 10 -
 - 3.1.5.1 对象分析 - 10 -
 - 3.1.5.2 策略收敛 - 10 -
 - 3.1.5.3 策略分析 - 11 -
 - 3.1.5.4 策略闭环 - 11 -
 - 3.1.5.5 策略合规 - 11 -
 - 3.1.5.6 域间合规 - 11 -
- 4 应用场景 - 11 -

- 4.1 系统适用场景..... - 11 -
- 4.2 用户使用场景..... - 12 -
 - 4.2.1 基础运维流程化 - 12 -
 - 4.2.2 防御网络攻击-迅速封堵攻击 IP - 12 -
 - 4.2.3 加强网络合规性建设..... - 12 -
 - 4.2.4 日常运营保障 - 12 -
 - 4.2.5 实现等保要求 - 12 -
- 5 联系我们..... - 12 -
- 6 关于天元云 - 13 -

1 前言

随着国家信息安全等级保护政策文件的出台，各企业已基本完成自身合规性信息安全保障体系的建设，具备了控制风险的能力。但在新时期、新形势下，随着业务应用与 IT 技术的日趋紧密，虚拟化、云计算、物联网、大数据、移动互联网等新技术的发展，现在所有的设备都变成智能化、网络接入点增多、安全边界逐步消失、各种互联网新型威胁日益猖獗的情况下，可以被攻破的入口越来越多，业务系统比以往任何时候都更加容易遭受到新型、高级、可持续的安全威胁。

企业网络的生态体系规模逐渐复杂；随着业务不断创新与扩充，设备的数量也呈几何级增长。日渐复杂的网络场景、迅速增长的设备数量以及历史遗留的配置问题给管理者带来了巨大的挑战，导致企业网络无法实现精细化、统一化、智能化运维管理。容易出现：

1、服务的交付能力不足：流程脱节、纯人工配置交付使基础架构服务的交付能力不足。

2、安全隐患多：由于安全策略配置不标准，不规范，历史配置不合理，导致基础架构内部的安全防护出现漏洞。

3、可用性低：人工配置不标准、不规范，人为变更错误常常引起严重企业 IT 的可用性事件。

4、运维成本高：由于品牌型号多，设备运维、人员成本、管理成本、审计成本均高。

5、基础架构团队战斗力受制：重复性劳动，导致运维人员积极性、技术能力停滞得不到成长，影响 IT 运维能力的提升。

这一系列问题需要必须用蕴含新模式、新技术的新型系统来应对。iNet 智能运维平台正是为了解决上述问题而研发的一款产品。iNet 智能运维平台以网络自动化垂直领域的空白市场切入助力企业完成网络自动化、智能化运维转型逐步扩展到 IT 监管控一体化全覆盖，采用智能算法实现基于自动化的网络 AIOps。

iNet 智能运维平台于 2017 年公司成立开始筹备，以让网络运维简单快乐为

使命；致力于网络自动化建设；2018 年进入密集研发阶段，并推出第一版 NAP 防火墙自动化产品，2021 年 6 月，对产品进行更新迭代，正式推出第一版 iNet 智能运维平台产品。

截止目前，iNet 智能运维平台，已在金融、制造、能源行业实施建设多个标杆项目，积累了丰富的实施建设经验，为用户带来了巨大价值，也得到用户的普遍认可。

2 平台概述

天元云推出创新的 iNet 智能运维平台，致力于帮助企业实现周期性、重复性、规律性的工作自动化。平台的面世，实现了 IT 运维全生命周期管理和支撑，并协助企业完成运维自动化的全面升级。

2.1 设计理念

iNet 智能运维管理平台致力于解决日渐繁杂的网络运维问题，通过对网络设备形成统一配置模型，完善配置管理接口、实现多场景部署、安全合规分析、智能运维管理等一系列复杂功能，打通了 IT 服务流程和网络设备的需求通路，提升运维效率和安全合规性。通过获取需求、合规检查、路径分析、策略分析、审核确定、下发执行、搜索管理这一整套流程支持策略智能运维自动化。

2.2 产品定位

iNet 智能运维管理平台主要定位在编排层，从上游模块获取网络开通需求，将需求通过智能分析与逻辑计算，形成精确的脚本编排，自动下发至相应的网络设备模块。iNet 将运维团队繁琐重复的工作自动化、标准化，提高运维团队的整体效率。

2.3 产品优势

安全策略可视化

- 将整网的设备及其访问控制规则、网络路由配置策略、地址转换策略、访问控制策略的分析与计算映射为网络拓扑展现。

- 实现策略安全基线的设定与动态监控，实现网络暴露风险的可视化分析，帮助客户收敛网络暴露面，降低网络风险。

策略管理集中化

- 支持网络设备的复杂异构对象资产管理。
- 屏蔽不同品牌访问控制策略差异，实现统一流程策略管理。
- 提供全局视角和单设备视角查看设备资产情况。

策略管理最优化

- 垃圾策略与风险策略检查，实现策略规则最小化与精细化的平衡。通过标准化的策略数据计算，检查策略规则之间的相互关系，发现隐藏策略、冗余策略、可合并策略、空策略、过期策略，分析策略命中情况并提供处置建议，优化策略规则。以降低防火墙策略的复杂性，提高网络性能。
- 合规性检查，根据企业和行业安全配置指导标准和规范进行安全配置检查，对不符合规范的策略和配置自动生成报告。

策略管理自动化

- 支持自动执行下发策略任务任务，提升 IT 管理的效率。
- 避免人为错误、收回错误的支持导致的高昂操作投入。

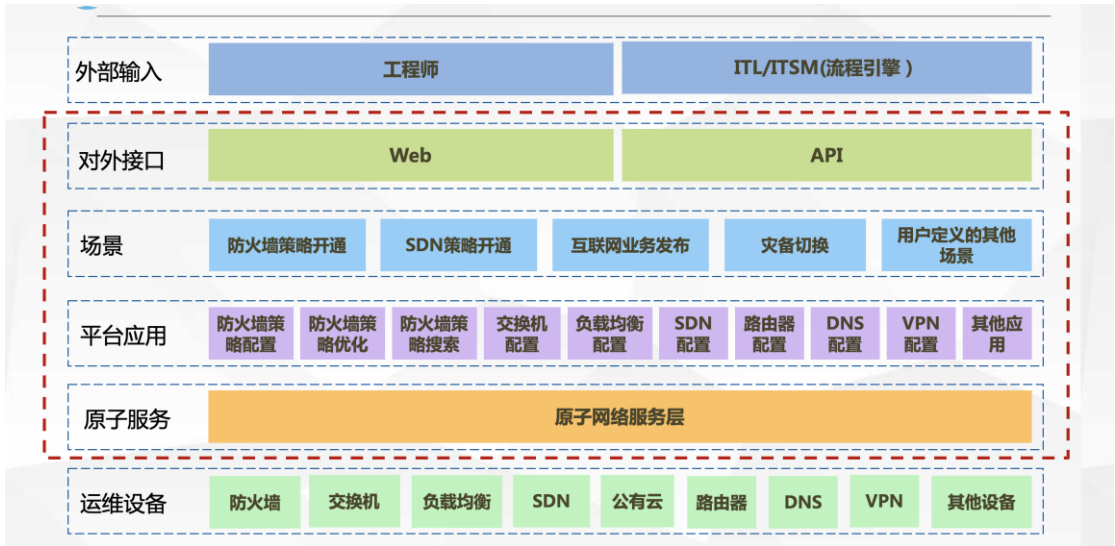
降低运维成本提高运维能力

- 实现敏捷交付：自由组合场景下的配置自动完成，将大大提升基础架构服务的交付效率和能力。
- 高安全防护能力：从设备自身配置着手，减少安全漏洞，由内到外的提升基础架构的安全能力。
- 高架构可用性：标准化、规范化的自动配置将大大降低因不规范的人为变更错误而引起的不可用性事件。
- 将运维人员的工作重心由重复性劳动转变为更有价值的工作，提升眼界

和能力，带动企业 IT 运维水平的进一步提升。

2.4 产品体系架构

系统总体架构如下图所示：



系统总体架构图

2.5 软硬件环境要求

运行环境支持的操作系统

- 客户端操作系统：
 - CentOS 7.4-7.9 64 位
 - RedHat Enterprise Linux 7 64 位
 - 信创：麒麟系统 V10SP1\2\3(支持信创中间件)

运行环境支持的服务器资源：

- CPU：32 vCPU(支持 64 位操作系统)
- 内存：64GB 或以上

- 硬盘：500GB 或以上

运行环境支持的网络环境：

- 网卡：至少一块网卡，分配 IP 地址
- 服务：可访问所管理设备(防火墙)的 SSH，Telnet 或 API 的 443 端口
- 开通端口： iNET 所使用 IP 的 80、8801、8089、5601、9092、8989、13000 端口可被 PC 端访问

3 iNet 智能运维系统

3.1 产品功能

3.1.1 全面设备管理

iNet 智能运维管理平台作为企业级设备一体化管理平台，可提供标准的 API 接口以及协议，适配国内外主流品牌防火墙、负载均衡、交换机等网络设备，系统通过自带的管理体系对相关设备进行分析管理，满足企业管理员对设备管理权限的掌控需求。

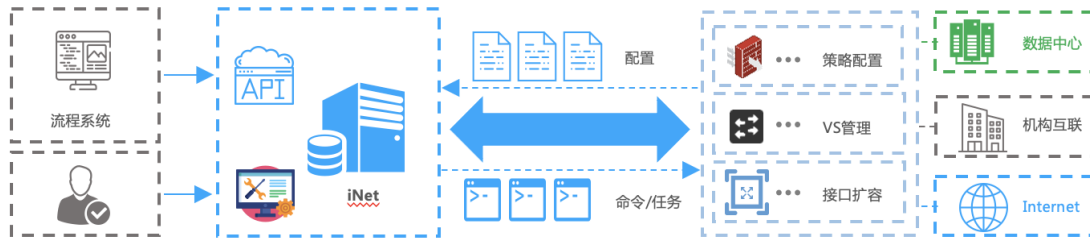
多维度检索数据：

3.1.2 网络可视化

拓扑绘制工具可以帮助客户将关键设备以及连接关系整合到一个视图中。除了及时发现设备故障，还可以简化日常的 IT 管理工作，当需要去数据中心现场排查故障时，可以准确定位设备所在的位置。

3.1.3 流程自动化

iNet 智能运维管理平台与内部运维流程平台集成，实现了全场景的自动化。平台目前已支持防火墙、负载均衡、交换机的功能模块。



3.1.4 新增策略分析

平台可预先对策略库数据进行分析处理,实现对新增策略配置信息进行有效性、冗余、冲突、可合并等策略检测分析,帮助管理员安全合理化的配置相关策略规则,提升企业策略下发的合理性。

3.1.5 优化、合规检查

通常防火墙策略由于频繁变更、日积月累会造成很多垃圾无用策略,一方面影响防火墙运行效率,另一方面也会存在一定安全隐患。平台策略优化检查可定期针对防火墙对象(包括地址对象、时间对象)和策略(包括安全策略、ACL 策略、NAT 策略、路由策略)进行 优化检查分析,梳理出各类空对象、未被应用对象、冗余策略、隐藏策略、过期策略、可合并策略、空策略等,支持防火墙策略优化分析及策略安全合规检测,从设备日志分析的维度,支持对指定策略的命中数统计和收敛功能。管理员可根据分析结果再对策略进行精简和优化调整。

3.1.5.1 对象分析

支持 IPV4 和 IPV6 的空对象、过期对象、未被引用对象等对象分析,并生成分析报告及优化建议、支持生成工单关联下发,实现闭环操作,支持审计。

3.1.5.2 策略收敛

分析具体策略涉及的源目地址及端口,分析是否存在可收紧策略,并生成分析报告及优化建议。

3.1.5.3 策略分析

支持 IPV4 和 IPV6 的冗余策略、冲突策略、可合并策略、未命中策略等策略分析，并生成分析报告及优化建议。

3.1.5.4 策略闭环

支持根据平台分析结果做策略闭环，支持对无效策略的删除/批量删除及对策略 disable 操作。

3.1.5.5 策略合规

通过策略梳理，对策略的合规性进行全面检查，支持对预定义和自定义高危策略或者端口给出合规的优化建议。

3.1.5.6 域间合规

基于网段访问关系矩阵对墙上已有策略的合规性进行全面检查，并给出合规的优化建议。

4 应用场景

4.1 系统适用场景

应用于企业网络建设、网路维护及网络自动化系统替代；

- 金融、证券、智能制造、能源等行业领域
- 应用程序交付领域
- 网络规划领域

4.2 用户使用场景

4.2.1 基础运维流程化

提供标准接口，可对接工单系统工单需求，快速定位工单参数，放通状态校验。

4.2.2 防御网络攻击-迅速封堵攻击 IP

实时查询访问、放通关系，策略关系，及时进行策略优化，通过安全策略收敛避免策略开放过于宽泛造成暴露面风险，通过一键阻断一旦发现渗透攻击，立即收回网络访问权限，通过安全策略自动下发在攻防演练中预验证策略提高容错处理能力。

4.2.3 加强网络合规性建设

策略检查冗余、无效策略，支持防火墙策略网络合规审计。

4.2.4 日常运营保障

确保入网设备的全面纳管和全生命周期管理，确保设备的业务与安全状态可监可控。

4.2.5 实现等保要求

基于等保要求，调优改善防火墙现存配置，保证网络的安全性和稳定性。

5 联系我们

了解关于系统相关的更多内容，请致电免费电话：400-8120-996。

深圳天元云科技有限公司

地址：深圳市福田区车公庙天安数码城创新科技广场一期 A 座 601C

邮箱： sales@sky-cloud.net

Tel: 400-160-1670

6 关于天元云

天元云 2017 年成立，总部位于深圳，在北京和上海设有分支机构。公司专注于基础架构自动化运维，帮助客户 IT 基础架构完成标准化、自动化、智能化转型。团队主要核心人员来自 Openstack、Mirantis、Juniper 、Arista 等厂商，拥有强大的 IT 基础架构规划能力，同时深刻了解基础架构运维痛点，在运维开发、云计算架构设计、实施等方面具备丰富的经验。

深圳天元云科技有限公司