runxun 润迅

Refract 洞流

洞流 Refract 系统 V1.0

产品手册

◆ **阅读说明** 本手册所有界面截图均来自洞流 Refract 真实后台（脱敏展示），所有 IP、协议、会话数、置信度等均为系统实拍数据。平台采用纯被动旁路检测，只“看”不“拦”，不解密流量、不产生阻断。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

官网：www.runxun.com

关于本手册

本手册为洞流 Refract 加密流量检测平台的使用说明，所有界面截图均来自真实后台（已脱敏），所有 IP、协议、会话数、置信度等均为系统实拍数据。平台采用纯被动旁路检测，只“看”不“拦”，不解密流量、不产生阻断。

文档修改记录

文档版本	产品版本	发布时间	修改内容	作者
V1.0	V1.2.0	2026-08-27	登录后台逐模块讲解 + 真实抓取的 IP / 隧道 / 跨境证据	产品部

术语与缩略语

术语 / 缩略语	说明
VPN	Virtual Private Network，虚拟专用网络；本文档指用于建立加密通信隧道的技术，含商业 VPN 与自建隧道。
跨境 VPN	指境内主机通过技术手段连接境外 VPN / 代理出口的行为。
代理节点	被识别为隧道 / 代理对端的 IP 节点，按对端聚合，含协议、端口、伪装域名、国外出口与命中数。
五维证据	洞流对单条加密会话的被动刻画框架：IP 情报、端口协议、协议握手、流量时序、全加密熵，五维交叉印证。
被动旁路	仅镜像 / 分光观测流量，不解密、不阻断，对业务零干扰。
判定分级	Confirmed（确认铁证）/ likely（疑似） 两级；低置信归入观察池（suspect），不打扰运维。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

官网：www.runxun.com

术语 / 缩略语	说明
工单	将检测结果转为可闭环处置的任务，含类型、严重度、置信度、状态（待处理 / 处理中 / 已处置 / 误报加白）。
名单与情报	白名单（误报加可信）、抑制名单与情报源，依据以上结论，减少重复研判。
监控范围	仅对这些 CIDR 网段内的源 IP 做重点检测，范围外流量不进入检测 / 开单。
PCAP	握手数据包捕获文件，可供对证据链逐包复核。
关系拓扑	内网客户端 → 中转节点 → 境外出口 的连接关系图。

手册概述

感谢您选择深圳润迅数据通信有限公司的洞流 Refract 加密流量检测平台。本手册详细说明洞流 Refract 的基本功能，帮助您快速掌握如何用本系统检测、取证并处置加密流量中的违规 VPN、自建隧道、混淆代理与跨境中转。

手册所提供的内容仅具备一般性指导意义，并不确保涵盖所有部署形态的使用场景。因版本升级、部署形态、配置文件不同等原因，手册中所提供的内容与用户使用的实际界面数据可能不一致，请以用户界面的实际数据信息为准。

手册中针对功能的介绍及示例的需要，可能会使用 IP 地址、网址和域名等信息，如无特殊说明上述信息均为示意（且已脱敏），不代表任何实际意义。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

预期读者

本手册主要适用于使用洞流 Refract 产品的读者，包括系统管理员、安全运营（SOC）分析师、合规审核员等。本手册假设读者对以下领域知识有一定了解：

- 传统 VPN 技术与隧道协议的基础概念
- 网络基础知识，包括计算机网络、TCP/IP 协议及常用网络术语
- 基本的网络交换机、分光 / 镜像接入知识
- 基本的 Linux / Windows 运维知识

格式与操作约定

内容	说明
【 】	系统 Web 界面上的按钮。例如：“点击【VPN 检测】进入检测页面”。
粗体字	系统 Web 界面窗口名、菜单名、数据表和字段名等。
>	介绍系统 Web 界面操作步骤时，用于隔离对象（菜单项、子菜单和按钮以及链接等），例如：“在导航栏依次选择【发现】>【VPN 检测】”。
单击	快速按下并释放鼠标的一个按钮。
双击	连续两次快速按下并释放鼠标的一个按钮。

提示框约定

框体	含义
阅读说明（蓝绿框）	操作小窍门、背景补充，方便用户理解平台能力。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

官网：www.runxun.com

框体	含义
诚实口径 / 边界声明（橙框）	说明平台能力边界（如“未解析 ≠ 漏检”、不解密不阻断），提醒正确解读判定。

公司信息：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503　邮编：518057

官网：https://maxrefract.com/　客服电话：400-854-5566

目 录

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

官网：www.runxun.com

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

官网：www.runxun.com

第 1 章　平台概述与登录

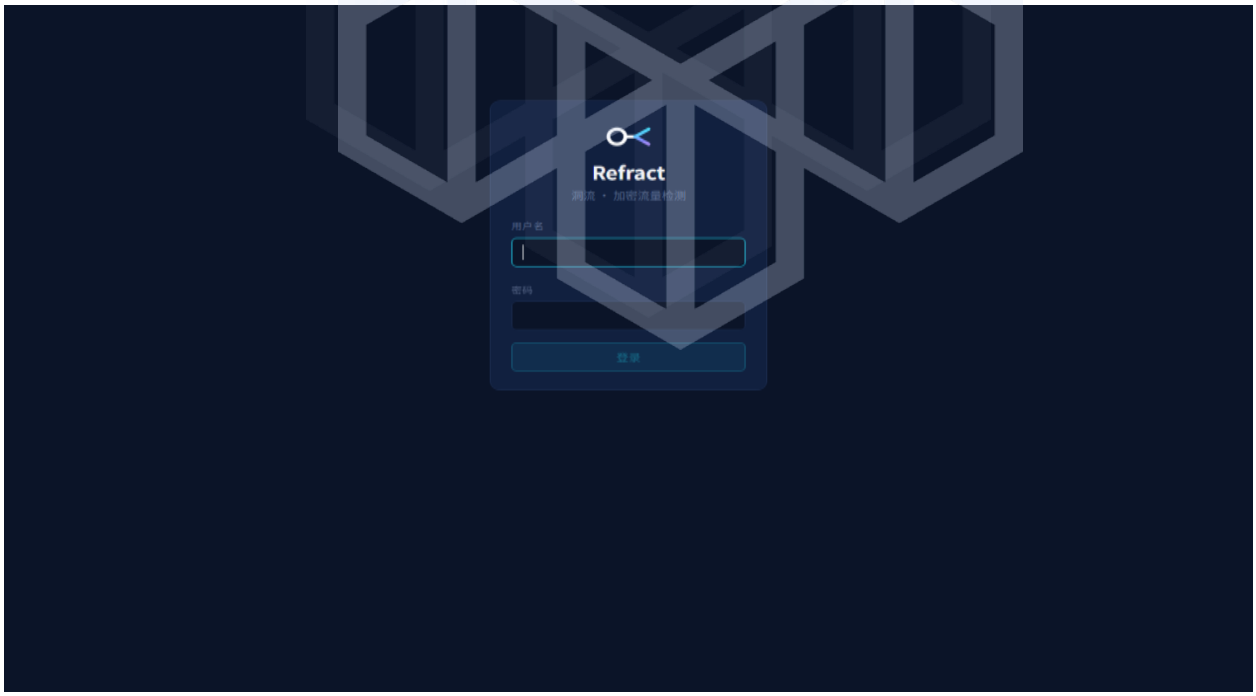
1.1 产品定位

Refract 洞流是面向服务运维、安全与合规团队的加密流量被动旁路观测与取证平台。

这款产品部署于交换机镜像口或光分路器之后。它以只读、不解密、不阻断、不进业务链路的方式，从加密流量中识别 VPN/代理/隧道与算力滥用行为，为每个来源生成带证据、可复核、可导出的判定报告，处置决策与执行权留给客户自身。

1.2 登录后台

访问后台地址，输入管理员账号与密码即可进入。单击【登录】后默认进入“态势总览”，左侧为模块导航，顶部为实时状态与当前账号。



图：登录界面（账号 / 密码，纯旁路只读监测）

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

1.3 模块地图

左侧导航将能力分为四大区，逐章讲解：

- 发现：总览 · 代理节点 · VPN 检测 · 跨境 VPN · 挖矿检测
- 调查：检索 · 关系拓扑
- 处置：工单 · 名单与情报 · 监控范围
- 系统：系统健康 · 系统设置 · 服务设置 · 系统授权 · 指挥大屏

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

官网：www.runxun.com

第 2 章　发现模块

2.1 态势总览

态势总览在一屏内汇总当前监测域的体量、分布与判定分级。以下为本次登录实拍的关键数字：

指标	数值	含义
加密中转节点	698	被识别到的隧道代理节点 IP
内网涉事主机	1,436	经各类 VPN 隧道外联的节点
命中境外国家/地区	33	跨境中转后落点地理区域的分布范围
命中会话	6492.9 万	系统识别到的非正常判定的累计流量
聚合代理节点	634	按对端归并后的隧道代理节点 IP
确认隧道主机	219	系统判定 L3 铁证级搭建 VPN 隧道的 IP 终端（包含境内境外 VPN 隧道）

功能：聚合全局指标。重点看三个指标——体量（中转节点/内网主机/会话）、分布（境外属地 Top：美国 185、加拿大 64、德国 43、中国香港 30、英国 22、新加坡 22、法国 12…）、判定分级（确认 219 / 高度疑似 213 / 疑似 844；境外出口已解析 107、被动边界未解析 527）。

数据证据：协议分类占比（非正常判定 1,436 个）——其它 612(43%)、确定性隧道 533(37%)、疑似 179(12%)、封装/全加密代理 38(3%)、传统 VPN 57(4%)、QUIC/其它代理 11(1%)。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

官网：www.runxun.com

图：态势总览（KPI 卡片 + 跨境流向 ）

图：态势总览（ 协议占比 + 判定分级）

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

官网：www.runxun.com

> ◆ **诚实口径** “未解析”不是漏检：流量经过多层中转或封装时，被动旁路看不到最终落地点，所以如实留空，不会瞎猜。

2.2 代理节点

功能：按“对端”聚合的疑似中转/代理节点清单，一个节点一行，卷起协议、端口、伪装域名、国外出口与命中数。默认按严重度排序——确凿、多协议、出口可见的节点优先。

图：代理节点（618 个节点，按严重度排序，可导出 CSV）

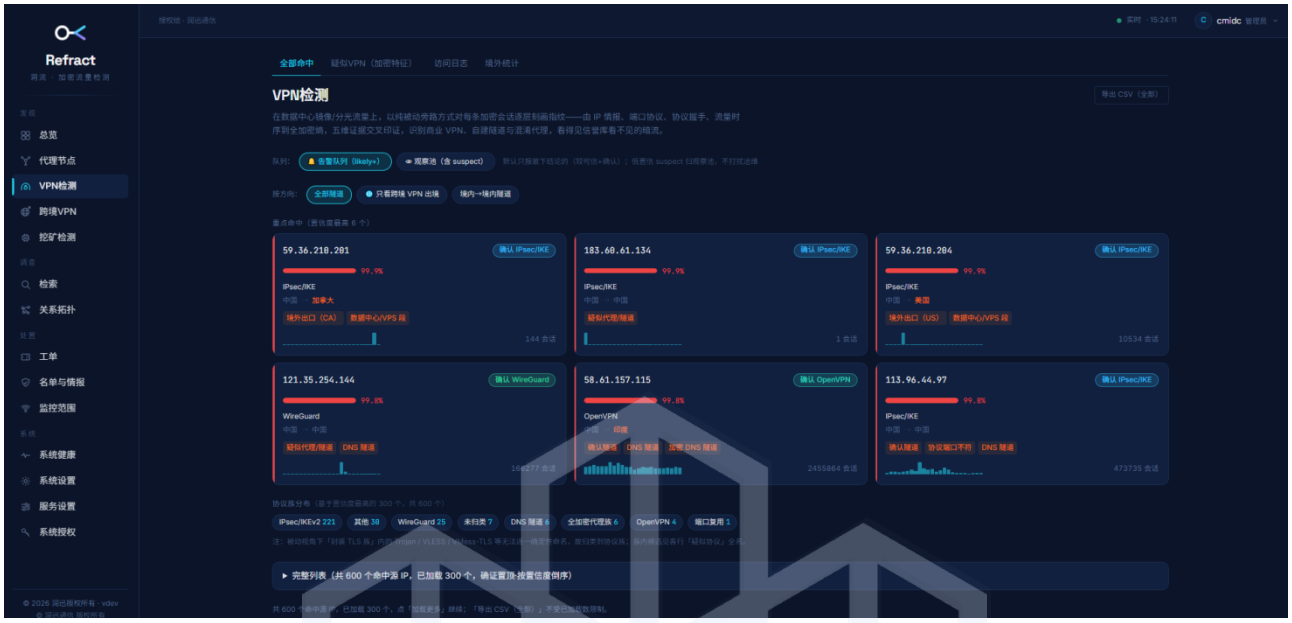
地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

数据证据：以下为实拍列表中的高严重度代理节点样例（节选）：

2.3 VPN 检测

功能：在镜像/分光流量上以纯被动旁路方式，对每条加密会话逐层刻画指纹——由 IP 情报、端口指纹、协议握手、流量时序到全加密熵，五维证据交叉印证，识别商业 VPN、自建隧道与混淆代理。默认只报“敢下结论的”（likely 较可信+confirmed 确认），低置信 suspect 归观察池不打扰运维。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com



图：VPN 检测（五维证据方法论 + 告警队列 + Top 高置信命中）

数据证据：当前共 600 个命中源 IP。协议族分布（置信度最高 300 个）——IPsec/IKEv2 221、WireGuard 25、全加密代理族 6、DNS 隧道 6、OpenVPN 4。重点命中（Top 6）：

源 IP	判定	置信	协议	境内→境外	会话
59.36.210.201	确认 IPsec/IKE	99.9%	IPsec/IKE	中国→加拿大	144
183.60.61.134	确认 IPsec/IKE	99.9%	IPsec/IKE	中国→中国	1
59.36.210.204	确认 IPsec/IKE	99.9%	IPsec/IKE	中国→美国	10534
121.35.254.144	确认 WireGuard	99.8%	WireGuard	中国→中国	166277
58.61.157.115	确认 OpenVPN	99.8%	OpenVPN	中国→印度	2455864
113.96.44.97	确认 IPsec/IKE	99.8%	IPsec/IKE	中国→中国	473735

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

VPN 检测 · 关键操作

【疑似 VPN（加密特征）】— 概率性命中视图

操作路径：**VPN 检测页** > 单击【疑似 VPN（加密特征）】标签。

作用：切换到"概率性命中"视图——基于加密 / 混淆特征(全加密代理、封装 TLS、ShadowTLS、QUIC·DTLS 代理、端口复用）识别。被动视角无法确定性命名具体协议，故只给"疑似"，须人工复核；确定性握手 VPN 见「全部命中」页签。

图：VPN 检测 · 疑似 VPN（加密特征）视图

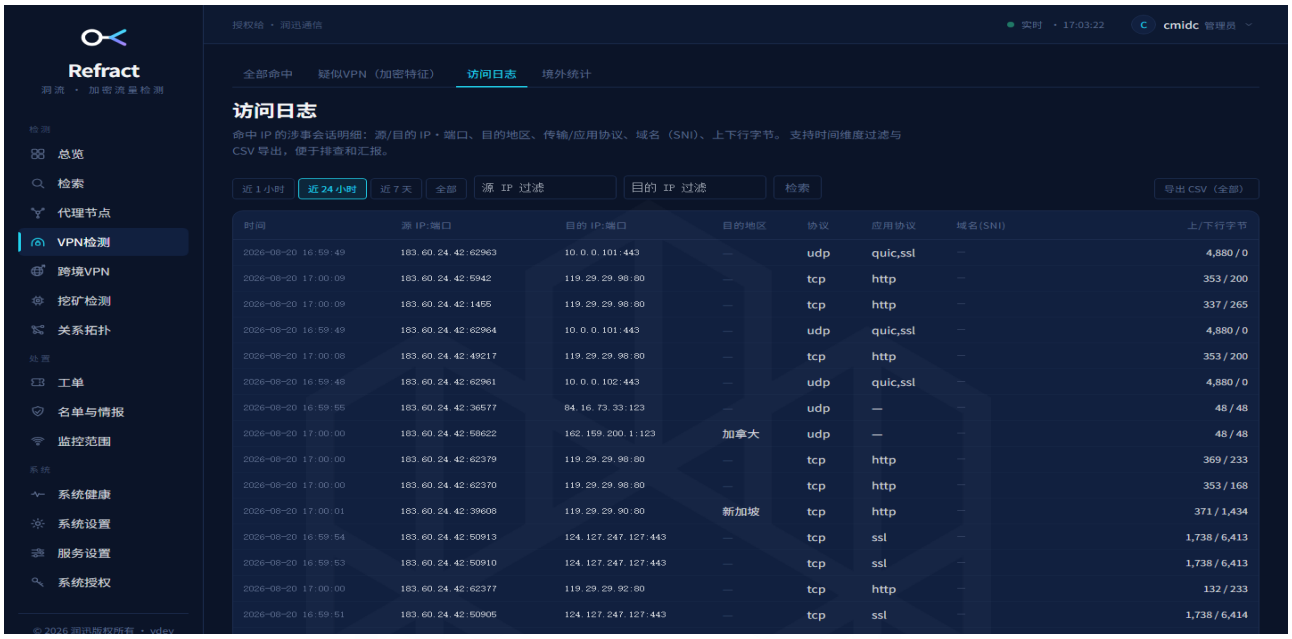
界面要点：命中表含 源 IP / 疑似协议 / 置信度 / VPN 端口 / 外部 IP / 位置 / 首见 / 末见，支持「导出 CSV（全部）」。

【访问日志】— 会话明细排查

操作路径：**VPN 检测页** >单击【访问日志】标签。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

作用：打开命中 IP 的涉事会话明细界面，含 源/目的 IP·端口、目的地区、传输/应用协议、域名（SNI）、上下行字节；支持时间维度过滤（近 1 小时/24 小时/7 天/全部）与 CSV 导出，便于排查与汇报。



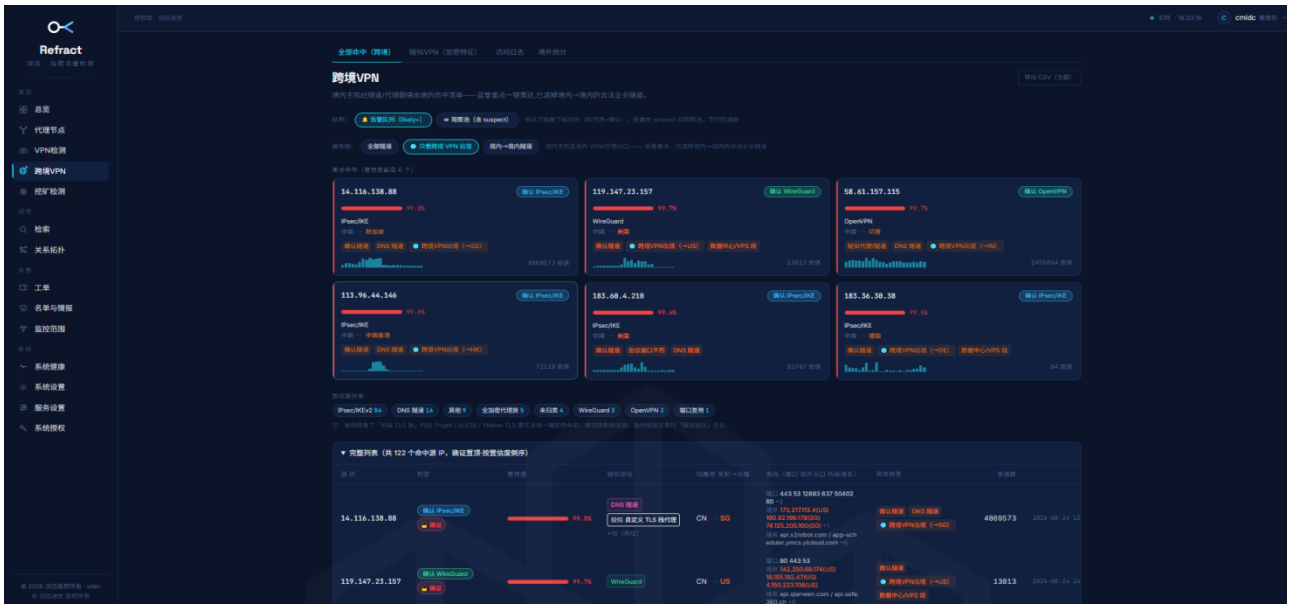
图：VPN 检测 · 访问日志（会话明细）

界面要点:时间过滤条 + 会话表(时间 / 源IP:端口 / 目的IP:端口 / 目的地区 / 协议 / 应用协议 / 域名(SNI) / 上·下行字节）。

2.4 跨境 VPN

功能：聚焦“境内主机连境外 VPN/代理出口”这一监管重点，已滤掉境内→境内的合法企业隧道。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com



图：跨境 VPN（139 个命中，定向境内→境外出境）

数据证据：共 139 个命中源 IP（已全部加载）。重点命中（Top，均为中国→美国出境）：

源 IP	判定	置信	协议	境内→境外	会话
14.116.138.88	确认 IPsec/IKE	99.8%	IPsec/IKE	中国→美国	4869573
119.147.23.157	确认 WireGuard	99.7%	WireGuard	中国→美国	13813
58.61.157.115	确认 WireGuard	99.7%	WireGuard	中国→美国	2455864
113.96.44.146	确认 IPsec/IKE	99.6%	IPsec/IKE	中国→美国	72119
183.60.4.210	确认 IPsec/IKE	99.6%	IPsec/IKE	中国→美国	83797

2.5 挖矿检测

功能：识别内网主机连向矿池、呈现挖矿心跳/算力特征的行为。当前监测域实拍结果为“未发现挖矿迹象”——未见连接矿池或挖矿心跳特征的主机。该模块在出现挖矿行为时会以相同五维证据框架给出确认/疑似判定。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

图：挖矿检测（当前未发现挖矿迹象）

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

官网：www.runxun.com

第 3 章　调查模块

3.1 检索

功能：输入 IP、网段、协议或关键字，快速检索历史判定与证据。是日常“拿到一个 IP，先查它是什么”的入口，也是从工单/拓扑反查单条证据链的起点。

图：检索（按 IP / 协议 / 关键字反查判定与证据）

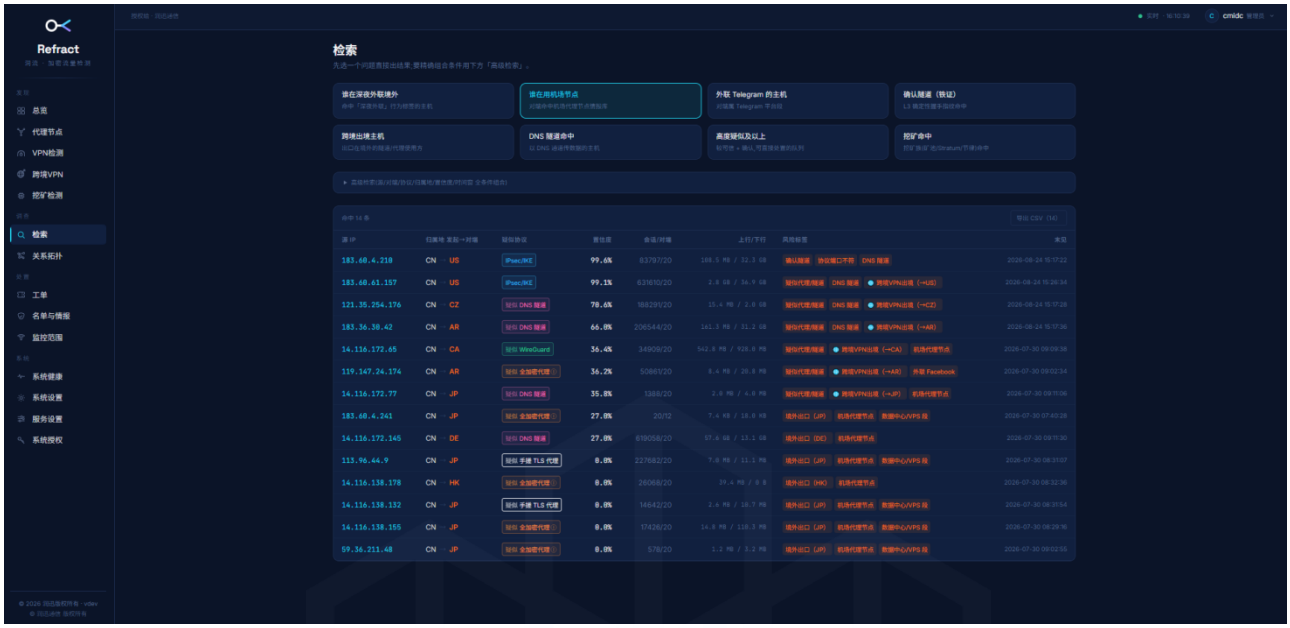
检索 • 关键操作

【谁在用机场节点】— 按类型一键筛选

操作路径：**检索页** > 单击**【谁在用机场节点】**按钮。

作用：IP 类型快捷筛选，只看机场代理类节点；同组按钮还包括：谁在深夜外联/外联 Telegram 的主机/确认隧道（铁证）/跨境出境主机/DNS 隧道命中/高度疑似及以上/挖矿命中，可按应用一键透视某类外联。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com



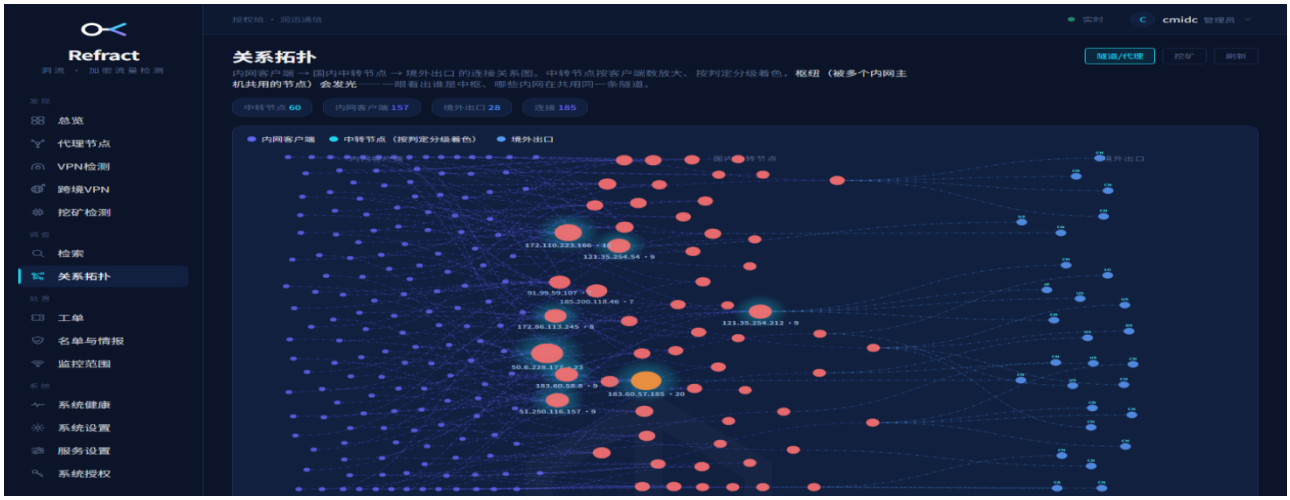
图：检索 · 机场代理节点筛选

界面要点：检索条件区（源 IP/对端/协议/归属地/置信度区间/末见时间） + IP 类型按钮组 + 归属地筛选 + 会话检索入口。

3.2 关系拓扑

功能：把“内网客户端 → 国内中转节点 → 境外出口”的连接关系画成图。中转节点按客户端数放大、按判定分级着色，被多个内网主机共用的“中枢节点”会高亮显示，方便快速识别谁是中枢、哪些内网在共用同一条隧道。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com



图：关系拓扑（内网客户端 157 · 中转节点 60 · 境外出口 28 · 连接 185）

数据证据：中枢节点 Top（客户端最多 = 最值得查）：

中转节点	归属	客户端数
50.6.228.177	美国	23
183.60.57.185	中国	20
172.110.223.166	中国	15
121.35.254.212	中国	9
121.35.254.54	中国	9

◆ **诚实口径** 出口未解析的中转节点不连出口边（被动旁路看不到其加密转发）；图为按严重度取的 top 子集，完整列表见“代理节点”。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

第 4 章　处置模块

4.1 工单

功能：把检测结果转成可闭环的工单。每条工单含类型（隧道/挖矿）、严重度、置信度、时间、状态（待处理/处理中/已处置/误报/误报·加可信）。支持改状态或“误报·加白”闭环。

图：工单（实拍 100+ 条，含真实工单号与关联 IP）

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

数据证据：实拍工单样例（节选，均为本次登录实时数据）：

工单号	类型	严重度	置信	时间	状态	关联 IP / 命中协议
VPN-3C830F62	隧道	高	95%	08-24 10:52	待处理	183.60.57.153 · 疑似 VPN 隧道使用
VPN-BE051002	隧道	高	98.6%	08-24 10:34	待处理	183.60.57.159 · 确认 IPsec/IKE
VPN-358BF8CD	隧道	中	62.3%	08-24 09:02	待处理	95.214.55.186 · 疑似 VPN 隧道使用
VPN-9EF788C4	隧道	高	95%	08-24 08:50	待处理	59.36.210.71 · 疑似 VPN 隧道使用
VPN-1617861F	隧道	中	72.6%	08-24 08:17	待处理	131.186.43.158 · 较可信 HTTP 正向代理（CONNETCT 隧道）

说明：命中协议覆盖 Opera VPN、MTProto（Telegram MTProxy Fake-TLS）、Shadowsocks/V2Ray 类全加密代理、DNS 隧道（DoH/DoT、iodine/dnscat2）、ProtonVPN、自定义 TLS 栈代理（AnyTLS/Go-TLS）等，置信度区间约 60%–100%。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

官网：www.runxun.com

4.2 名单与情报

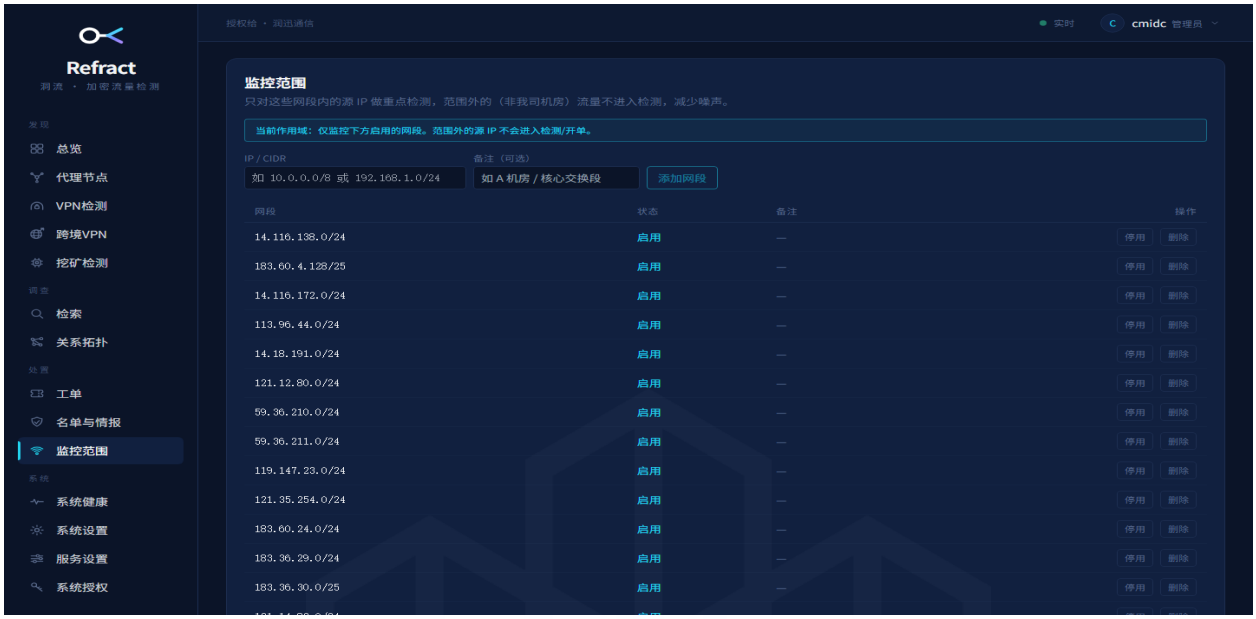
功能：维护白名单（误报加可信）、抑制名单与情报源。把“已确证为正常/已复核为误报”的 IP 记下来，减少重复研判——这正是洞流“越用越准”的反馈机制。

图：名单与情报（白名单 / 抑制 / 情报三类）

4.3 监控范围

功能：只对这些网段内的源 IP 做重点检测，范围外的流量不进入检测/开单，从而减少噪声。可随时增删网段并启停。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com



图：监控范围（当前启用 25 个 CIDR 网段）

监控范围 · 关键操作

【添加网段】— 配置检测作用域

操作路径：**监控范围页** > 单击【添加网段】。

作用：向监控作用域新增一个 IP/CIDR 网段，启用后该网段内源 IP 进入重点检测；范围外不进检测/开单。

这就是产品“可控作用域”的思路：只监控你指定的网段，不做全网监听。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

官网：www.runxun.com

图：监控范围 · 添加网段

界面要点：输入框（IP/CIDR + 备注）+ 添加按钮 + 当前启用网段表（25 段，如 14.116.138.0/24、183.60.4.128/25、183.60.58.0/24… 状态均为启用）。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

官网：www.runxun.com

第 5 章　系统模块

5.1 系统健康

功能：呈现采集管道与各服务的运行态、资源占用与采集质量，是运维自检入口。

图：系统健康（分光/CPU/内存/磁盘/采集质量/服务状态）

系统数据采集：分光 13.5 Gbps、216 万 pps；CPU 30 / 48 线程；系统内存 22G/31G；磁盘 31%（401G/915G）；采集层卸流 85%（有意只留握手）；本地丢包 2.1%。服务占用：流量解析 7.8G/20G、39%、CPU 1505%；实时判定 3.6G/6G、60%、CPU 398%。采集质量含“镜像/分光完整度”与“异常单向 5.37%”。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

5.2 系统设置 / 服务设置 / 系统授权

功能：系统设置用于账号/角色与基础参数；服务设置管理各检测服务的开关与阈值；系统授权查看授权客户、容量（接口/传感器/吞吐）、离线气隙与有效期。当前授权客户为“润迅通信”，支持离线气隙部署。

图：系统设置

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

图：系统授权（授权客户 / 容量 / 离线气隙 / 有效期）

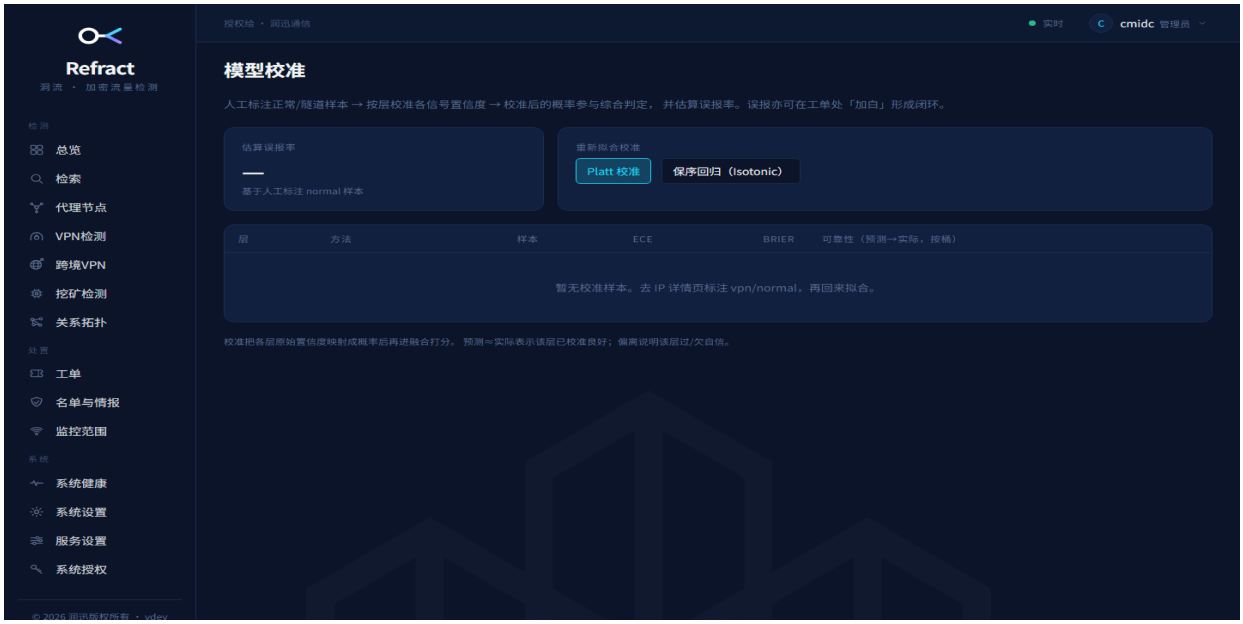
服务设置 · 关键操作

【打开校准】— 模型校准

操作路径：**服务设置页** > 单击【打开校准】> 跳转模型校准页。

作用：跳转到模型校准页面——人工标注 normal/vpn 样本 → 按层校准各信号置信度 → 校准后的概率参与综合判定并估算误报率。这是洞流“越用越准”的实现方式。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com



图：服务设置 · 【打开校准】（→ 模型校准页）

界面要点：校准方法（Platt 校准 / 保序回归 Isotonic）+ 重新拟合按钮 + 可靠性表（层/方法/样本/ECE/BRIER/可靠性）+ 标注提示。

系统授权 · 关键操作

【复制申请码 / 上传授权】— 离线气隙激活

操作路径：**系统授权页** > 【复制申请码】→ 邮件发厂商 → 收到令牌 → 【上传授权】粘贴激活。

作用：离线气隙（air-gapped）部署场景的激活流程。复制本机指纹申请码发给厂商，厂商返回授权令牌后粘贴上传即完成激活——全程无需联网。授权失效即停服务，但授权页/健康/登录仍可达，便于当场续期。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

图：系统授权 · 复制申请码 · 上传授权

界面要点：授权信息（客户 润迅通信 / 授权编号 RFL-RUNXUN-GZ01 / 签发 2026-08-20→2027-12-31 / 容量 采集口 8·吞吐 20G·传感器 1 / 本机指纹 eca65107…）+ 离线激活步骤 + 复制申请码/上传授权/在线更新/强制授权(硬停)按钮。

5.3 指挥大屏

功能：面向指挥/汇报场景的全屏可视化大屏，把态势总览、跨境流向、协议占比与判定分级投射到大屏，适合值守与汇报。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

图：指挥大屏（全屏可视化，适合值守/汇报）

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503

电话：400-854-5566

官网：www.runxun.com

第 6 章　IP 数据证据详解（核心）

洞流 Refract 的核心能力之一，是“登录平台后把每条证据讲清楚”：任意一条命中都能下钻到单 IP 详情页，看到五维证据、置信度、判定依据与“为什么这么判”的证据链，且可一键导出报告 PDF / 证据 JSON / 握手 PCAP 逐包复核。下面用两条真实命中做完整示范。

6.1 一条 IP 的证据链怎么读

以 59.36.210.201 为例，如下图：

图：IP 详情：59.36.210.201（综合判定 99.9%）

基础画像：源 IP 59.36.210.201，发起方归属地中国；对端 192.99.37.179（加拿大，AS16276）。同时观测到 IPsec/IKE、疑似 HTTP 正向代理、现代加密代理。会话数 144，对端样本 9。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com

五维证据

维度	数值	说明
协议特征	99.9%	协议层指纹命中强度
IP 风险	0%	情报/归属地风险
综合	99.9%	多层交叉后封顶判定

“为什么这么判”——逐条证据链

1) 命中确定性指纹「协议握手指纹 · IPsec」(IPsec/IKE) —— 这是铁证级判定,可导出握手 PCAP 逐包复核。

2) 作为 IPSec/IKE 响应方完成 SA 协商 2 次（responder_spi≠0，窗内≥2，确定性 · 反扫描旁路 · engine batch)

3) 服务器级持续确证:5 个自然日(2026-08-18~2026-08-23)持续呈现「非标端口 4443 多客户端无 SNI 已建立 TLS」服务端签名(单日峰值 58 个不同客户端)——瞬态误报不会跨日同端口复现,结构签名+时间持续性共同确证为现代加密代理服务器(Trojan/VLESS/SS-over-TLS 类)

> ◆ **边界声明** 证据链由已入库信号现场重算、逐条可核对；加密流量的被动研判到“协议命名”为止——不解密、不阻断。

6.2 跨境 VPN 出境证据

以 14.116.138.88 为例，如下图:

地址: 广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话: 400-854-5566
官网: www.runxun.com

图：IP 详情：14.116.138.88（中国 → 美国 T-Mobile，综合 99.9%）

基础画像：源 IP 14.116.138.88，发起方中国；对端 190.92.199.178（新加坡，AS136907）。标记 🌐 跨境 VPN 出境（→SG）。会话数 4869573，对端样本 20。五维证据：协议特征 20.0%、IP 风险 95.0%、综合 99.8%。

“为什么这么判”——逐条证据链

1) 命中确定性指纹「协议握手指纹 · WireGuard」与「协议握手指纹 · IPsec/IKE」——铁证级，可导出 PCAP 逐包复核；

2) 确定性握手确认为 handshake:ipsec，记忆保留期内维持判级（确定性握手为铁证，按服务器持久保留）。

地址：广东省深圳市南山区粤海街道深南大道 9668 号华润置地大厦 C 座 1503
电话：400-854-5566
官网：www.runxun.com