SDWAN组网上云

租户管理员指南

租户管理员指南

|  |
| --- |
| [NSE的安装与初始化](https://nsc.nova.net.cn/docs/tenant/nse-installation) |

|  |
| --- |
| [监控-站点&站点间](https://nsc.nova.net.cn/docs/tenant/monitor-site) |

|  |
| --- |
| [监控-安全服务](https://nsc.nova.net.cn/docs/tenant/monitor-security) |

|  |
| --- |
| [配置-站点](https://nsc.nova.net.cn/docs/tenant/config-site) |

|  |
| --- |
| [配置-VRF](https://nsc.nova.net.cn/docs/tenant/VRF) |

|  |
| --- |
| [配置-网络服务-Nova网关](https://nsc.nova.net.cn/docs/tenant/VRF-vpe-connecting) |

|  |
| --- |
| [配置-网络服务-应用加速](https://nsc.nova.net.cn/docs/tenant/VRF-management) |

|  |
| --- |
| [配置-安全服务-云安全实例](https://nsc.nova.net.cn/docs/tenant/config-security-cloud-safety-instance) |

|  |
| --- |
| [配置-租户参数](https://nsc.nova.net.cn/docs/tenant/config-tenant) |

|  |
| --- |
| [系统-告警管理](https://nsc.nova.net.cn/docs/tenant/system-warning) |

|  |
| --- |
| [系统-许可管理](https://nsc.nova.net.cn/docs/tenant/system-permit) |

|  |
| --- |
| [前言](https://nsc.nova.net.cn/docs/tenant/foreword) |

|  |
| --- |
| [监控-概览](https://nsc.nova.net.cn/docs/tenant/monitor-overview) |

|  |
| --- |
| [监控-网络服务](https://nsc.nova.net.cn/docs/tenant/monitor-network) |

[监控-告警](https://nsc.nova.net.cn/docs/tenant/monitor-alarm)

[监控-日志](https://nsc.nova.net.cn/docs/tenant/monitor-log)

|  |
| --- |
| [监控-报表](https://nsc.nova.net.cn/docs/tenant/monitor-report) |

|  |
| --- |
| [配置-模板](https://nsc.nova.net.cn/docs/tenant/config-profile) |

|  |
| --- |
| [配置-网络服务-拓扑](https://nsc.nova.net.cn/docs/tenant/VRF-topo) |

|  |
| --- |
| [配置-网络服务-远程办公](https://nsc.nova.net.cn/docs/tenant/VRF-remote-vpn) |

[配置-网络服务-网络对象](https://nsc.nova.net.cn/docs/tenant/VRF-internet-object)

[配置-网络服务-高速通道](https://nsc.nova.net.cn/docs/tenant/VRF-high-speed-tunnel)

|  |
| --- |
| [配置-安全服务-安全模板](https://nsc.nova.net.cn/docs/tenant/config-security-template) |

|  |
| --- |
| [配置-安全服务-安全对象](https://nsc.nova.net.cn/docs/tenant/config-security-safety-object) |

|  |
| --- |
| [系统-用户](https://nsc.nova.net.cn/docs/tenant/system) |

|  |
| --- |
| [系统-升级管理](https://nsc.nova.net.cn/docs/tenant/system-upgrade) |

[系统-诊断](https://nsc.nova.net.cn/docs/tenant/system-diagnose)

前言

手册内容

无内容

本书约定

图形界面格式约定

|  |  |  |
| --- | --- | --- |
| 文章描述 | 代替符号 | 举例 |
| 按钮 | 边框+阴影 +底纹 | |  | | --- | | 确定 |   “确定”按钮可简化为 |
| 菜单项 | 『』 | 菜单项“系统设置”可简化为『系统设置』 |
| 连续选择菜单项及子 菜单项 | → | 选择『系统设置』 →『接口配置』 |
| 下拉框 、单选项 、复 选框选项 | [] | 复选框选项“启用用户”可简化为[启用用户] |
| 窗口名 | 【】 | 如点击弹出 【新增用户】 窗口 |
| 提示信息 | “” | 如提示框中显示“保存配置成功， 配置已修改,需要重 启服务才能生效， 是否立即重启该服务?” |

标志约定

 小心 、注意：提醒操作中应注意的事项，不当的操作可能会导致设置无法生效 、数据丢失或者设备损 坏。

 说明 、提示 、窍门：对操作内容的描述进行必要的补充和说明。

NSE的安装与初始化

激活NSE是将NSE的SN与控制器站点进行绑定的过程， 配置方法如下：

URL激活

配置步骤如下：

1K 创建站点，填写设备名称， 无需填写序列号；

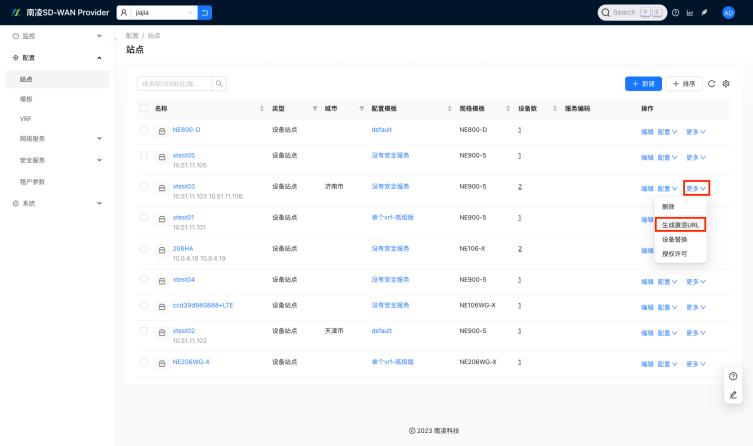
2K 选中该站点， 点击『更多』创建[生成激活URL]；

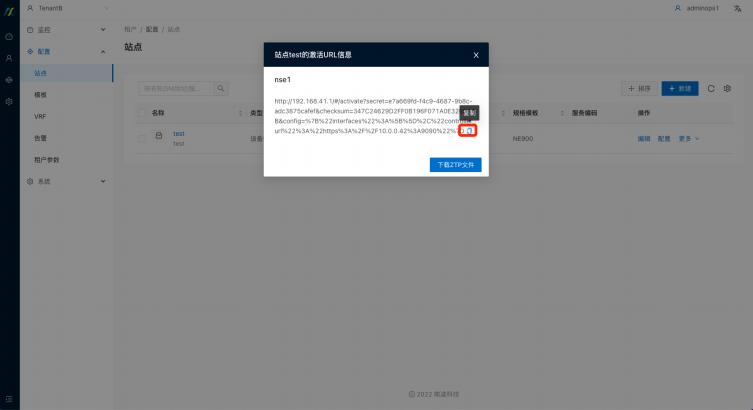
3K 笔记本电脑用网线连接NSE的MGMT口；

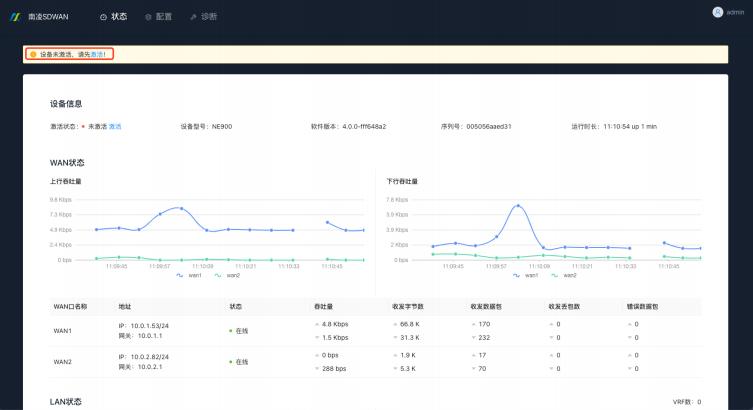
4K NSE的MGMT口IP是固定的<192.168.41.1>/24，所以笔记本电脑网卡要配置一个与其同网段的IP， 并ping 测确保其连通性；

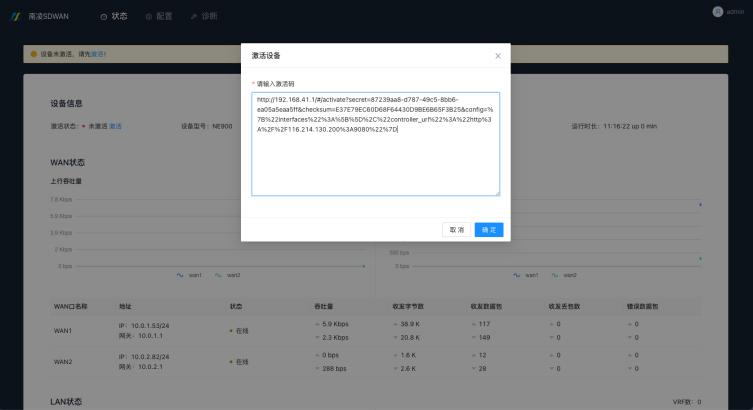
5K 将激活码复制到笔记本电脑浏览器中激活NSE， 或者在浏览器中输入NSE的MGMT口IP， 进入到Device Manager进行激活 。（默认账号密码：admin/admin）

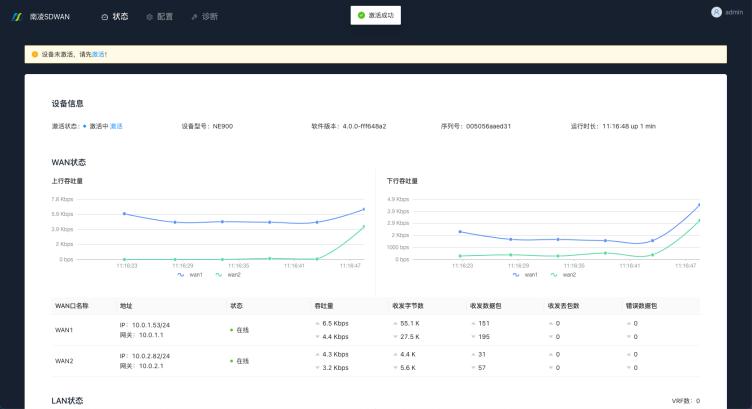












手动激活

配置步骤如下：

1K 创建站点，填写设备名称和序列号；

2K 用笔记本电脑打开NSE的Device Manager；

3K 检查控制器地址是否正确：『配置』 →『系统』 →『控制器地址』（ [https://nsc.nova.net.cn:9090](https://nsc.nova.net.cn:9090/) ）

4K 完成绑定。





监控-概览

概览

『租户』 →『监控』 →『概览』

· 站点/链路数

· 安全实例/统计数

。 每日新增威胁

○ 每日新增失陷主机

 告警数

 一个月内的告警总量

 一个月内每日的增长量

 流量统计

○ 全局流量

○ 加速流量

 总字节排行

○ 应用

 主机地址

○ 目的地址

○ 业务分类

○ 站点

○ 站点间

 VRF

○ 远程用户

○ 传输网络

 安全统计

。 威胁总次数

○ 威胁阻止次数

○ URL总次数

○ URL阻止次数

 文件内容总次数

○ 文件内容阻止次数

○ 应用

○ 主机地址

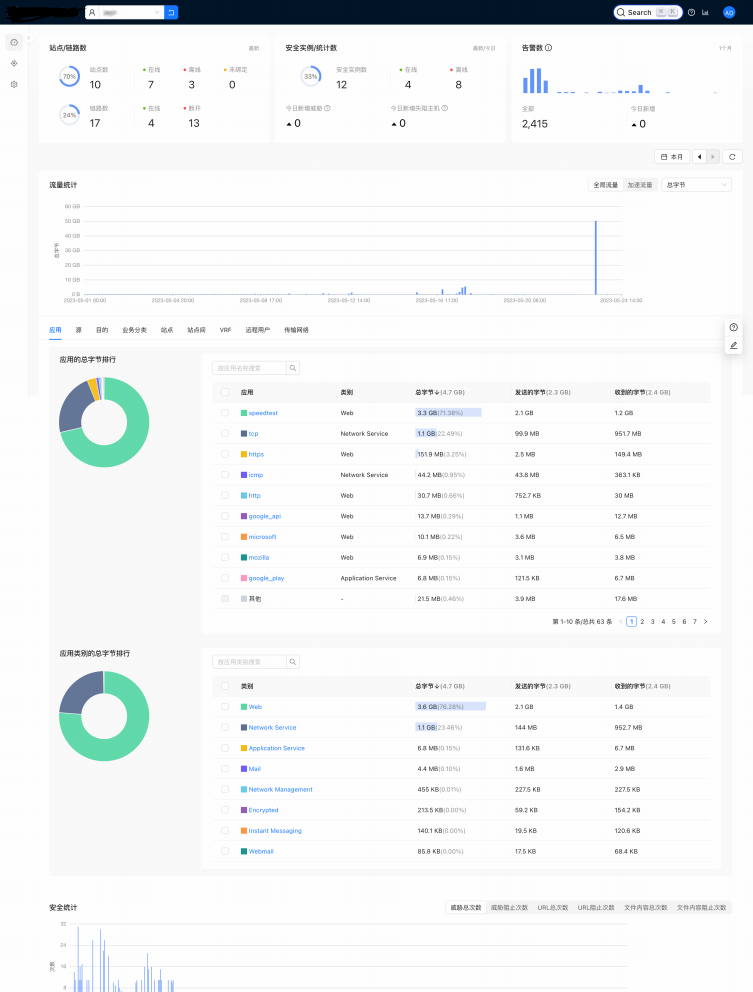
○ 目的地址

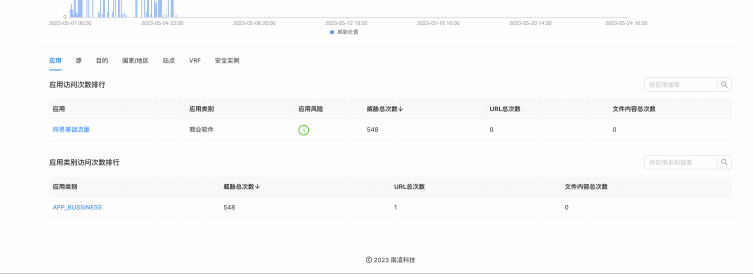
 国家/地区

 站点

 VRF

。 安全实例





监控系统数据查询说明

历史数据默认时间粒度

查询时间范围和返回数据时间间隔的关系如下：

|  |  |
| --- | --- |
| 时间范围 | 间隔 |
| J0, 1h] | 60s |
| J1h, 3h] | 300s |
| J24, 7d] | 3600s |
| J7d, 31d] | 10800s |
| J31d, ~) | 86400s |

s表示秒， h表示小时， d表示天

最新数据说明

页面列表展示的当前值， 如设备 CPU 使用率 、端口吞吐量 、链路丢包率等等， 计算的是从查询当前时刻起 最近 5 分钟内最新的一条数据 。如果 5 分钟内没有数据，则显示为空。

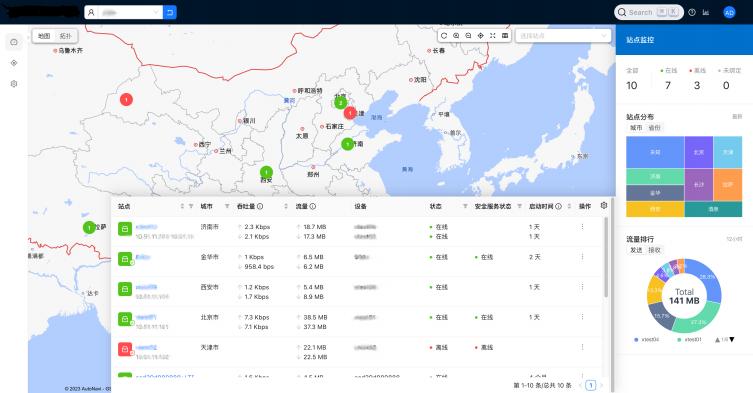
监控-站点&站点间

站点

站点信息

『租户』 →『监控』 →『站点』

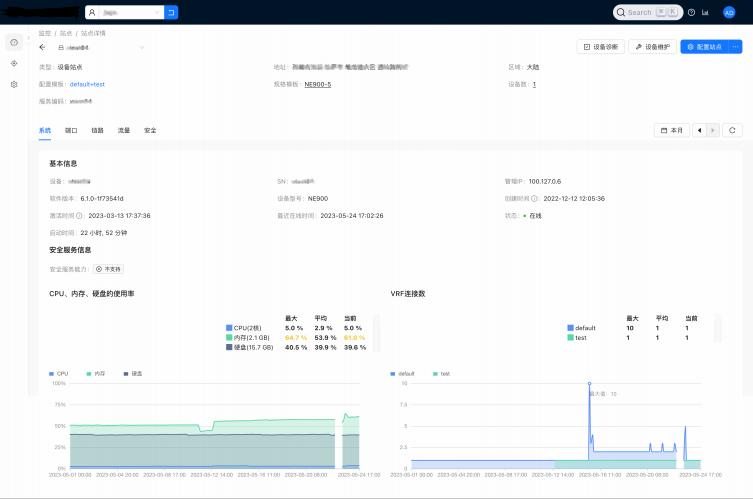
 显示站点 、城市 、吞吐量 、流量 、设备在线状态和设备启动时间



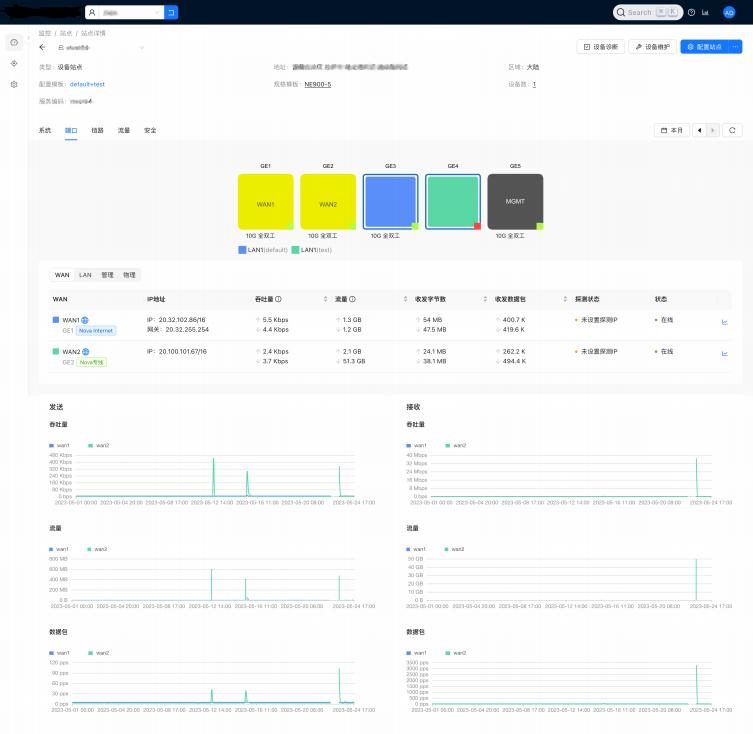
站点详情

○ 点击站点名称可查看NSE系统 、端口 、链路 、流量 、安全等信息

监控站点系统



监控站点端口

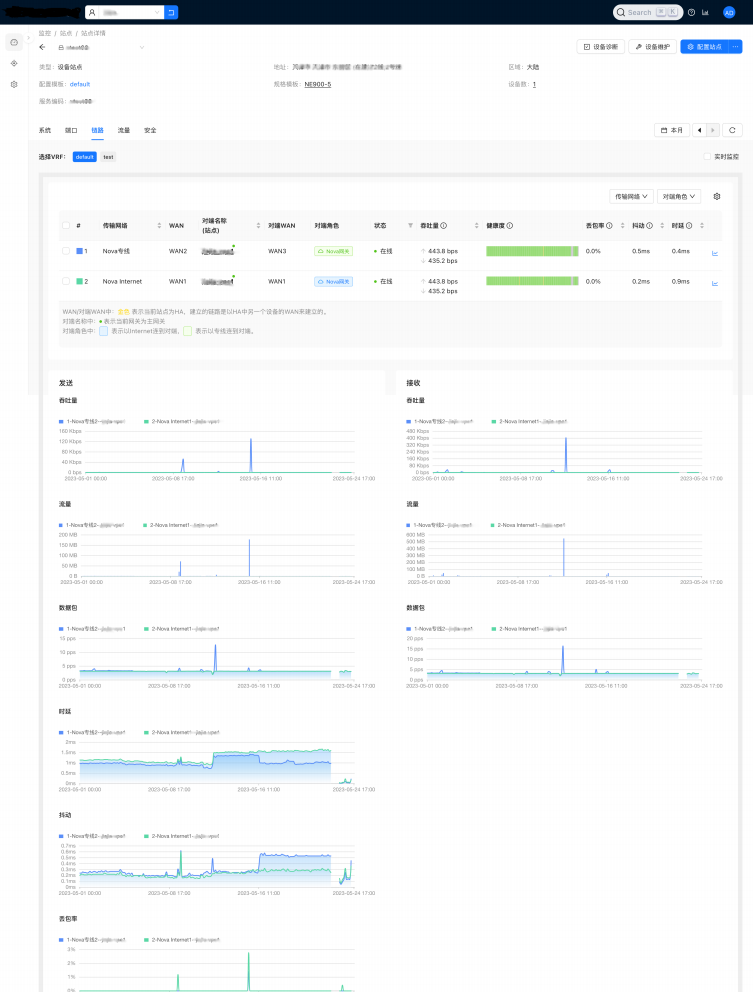


监控站点链路

 深色加粗字体的网关表示主网关

 绿色粗线条表示网络健康度，质量变差会变成黄色甚至红色

 可查看指定时间

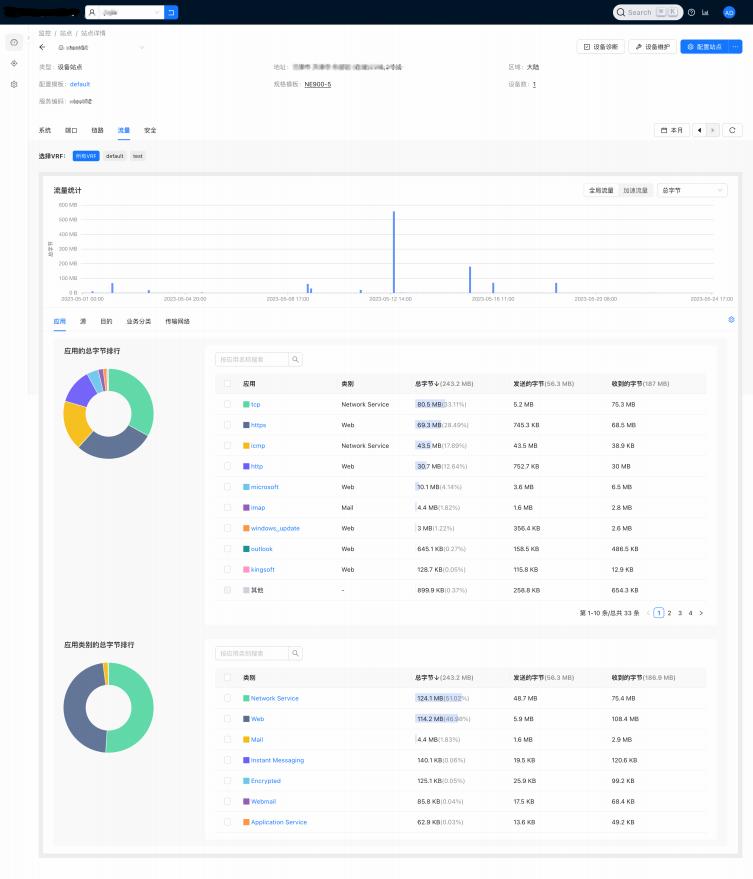




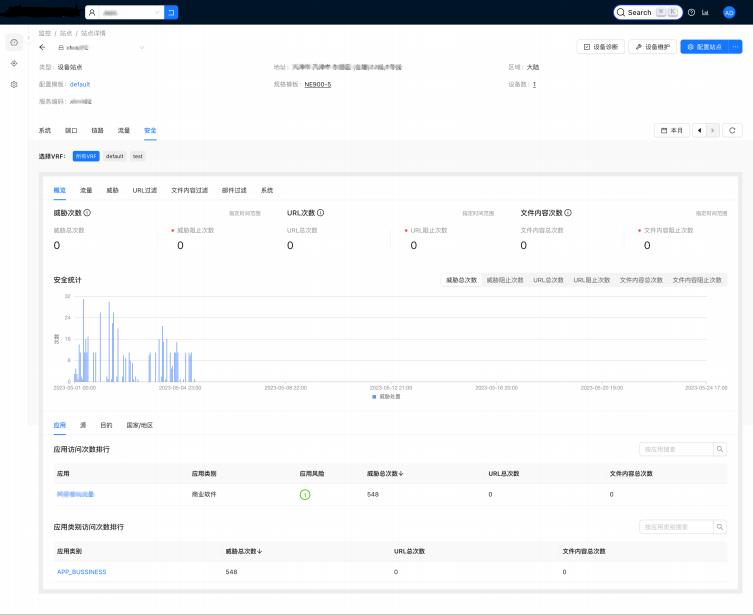
监控站点流量

应用 源 目的 业务分类 传输网络





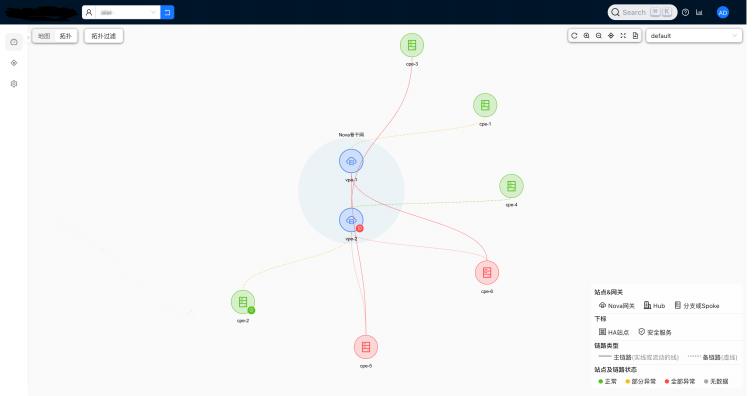
监控站点安全



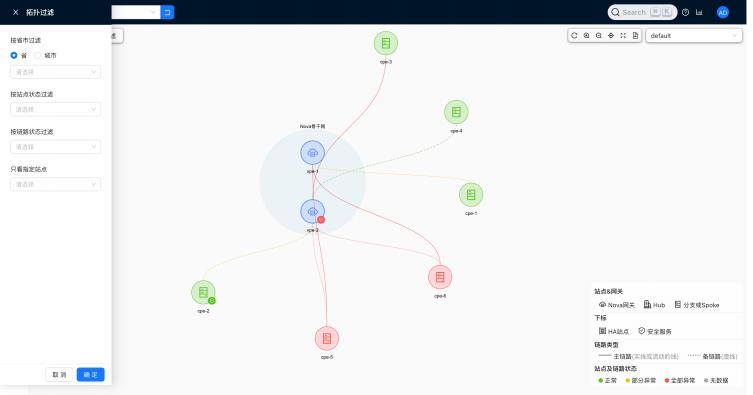
站点拓扑

『租户』 →『监控』 →『站点』 →『拓扑』

拓扑查看



拓扑过滤



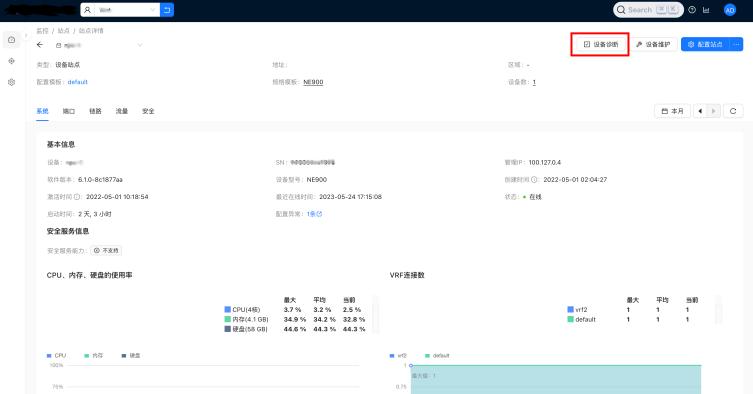
运维工具

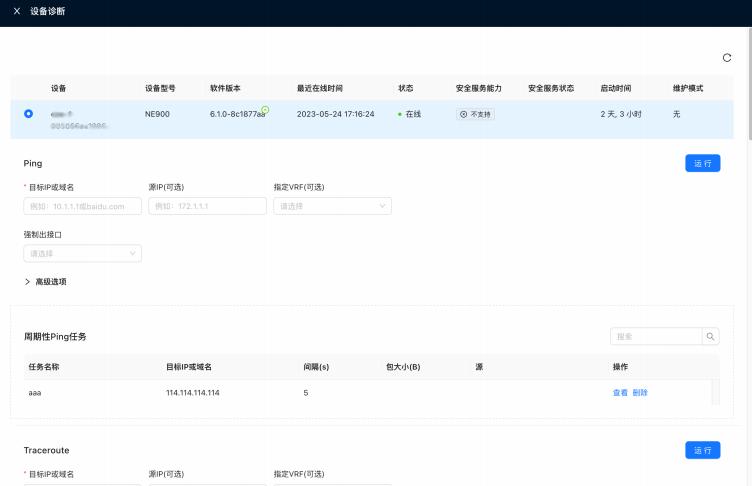
设备诊断

『租户』 →『监控』 →『站点』 →『查看站点详情』 →



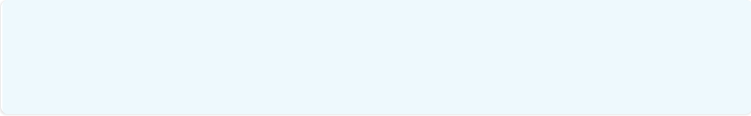
|  |
| --- |
| 设备诊断 |





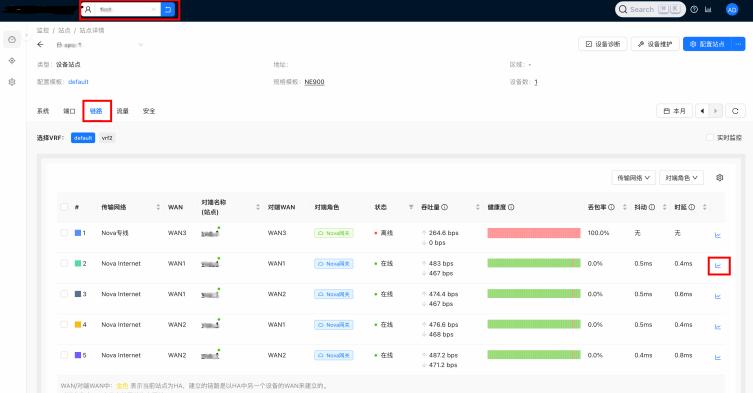
链路诊断

『租户』 →『监控』 →『站点』 →『查看站点详情』 → 查看链路流量详情 → 【流量详情】



 INFO

注:通常是在设备离线的情况, 隧道的断线状态不能被很快感知,可以通过该工具在隧道的对端来探测 隧道是否正常



 INFO

『流量详情』 → 运行『链路诊断』 ,会出现下面的链路诊断结果报告 。其中链路的平均往返时间在 0.67毫秒到0.75毫秒之间说明没有丢包。



设备维护

『租户』 →『监控』 →『站点』 →『设备维护』

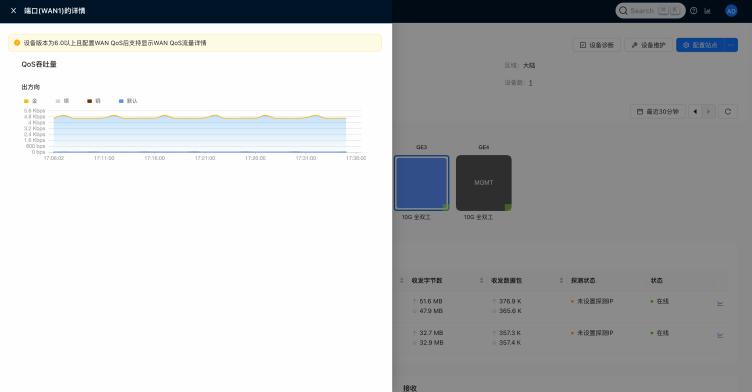
 INFO

控制器会基于学习到的CPE的状态, CPE的硬件条件, 控制器上发布的设备镜像情况决定是否可以开 启安全服务能力

|  |
| --- |
| 无安全服务能力 未开启安全服务 |
|  |
| QOS流量统计 |
| |  | | --- | | INFO  可在端口处查看WAN的QOS出流量，也可在链路处查看QOS吞吐量出方向与如方向的流量 | |
| 端口QOS流量 链路QOS流量 |



 点击后可查看QOS吞吐量出方向



显示指定时间的burst带宽

 INFO

查询时间说明（ 选择粒度过细可能会导致页面性能下降）：

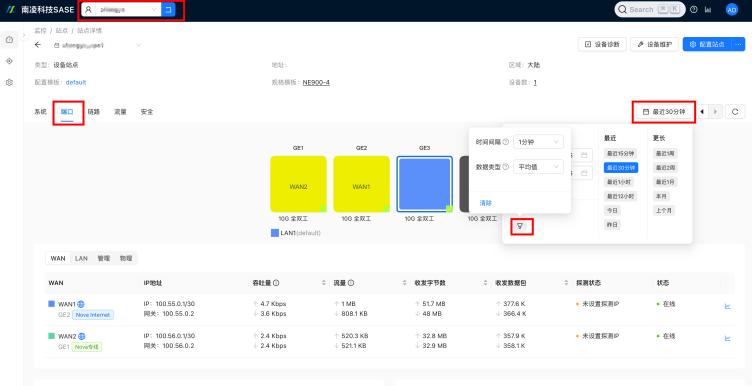
 查询时间范围在7天以内， 可选1分钟数据时间间隔

 查询时间范围在31天以内， 可选1分钟 、5分钟 、1小时数据时间间隔

· 查询时间范围超过31天，不可指定数据时间间隔

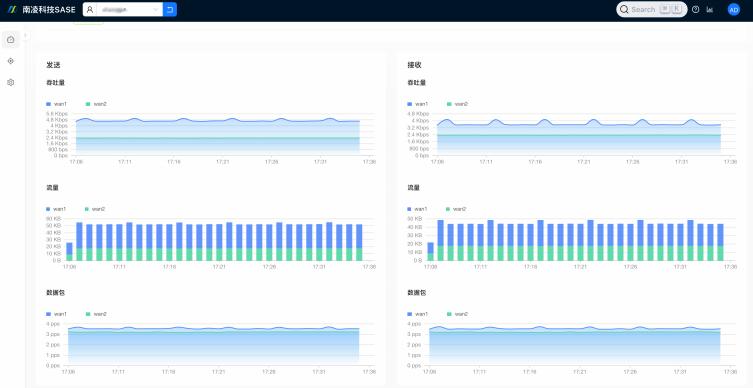
数据类型说明：

 时间间隔内的数据取平均值 、最大值 、最小值或最新值



默认流量图 1分钟平均值流量图 5分钟平均值流量图 1小时平均值流量图

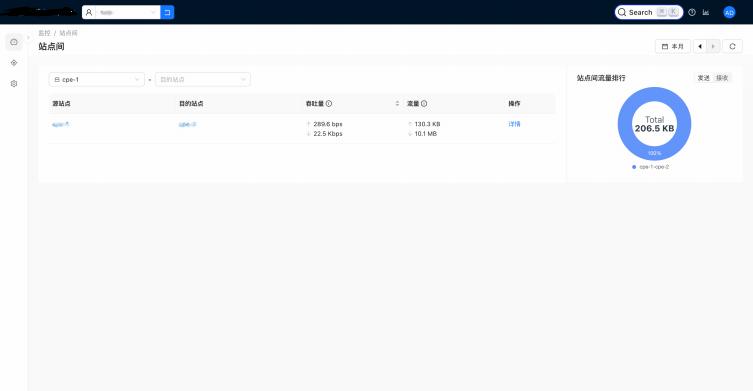


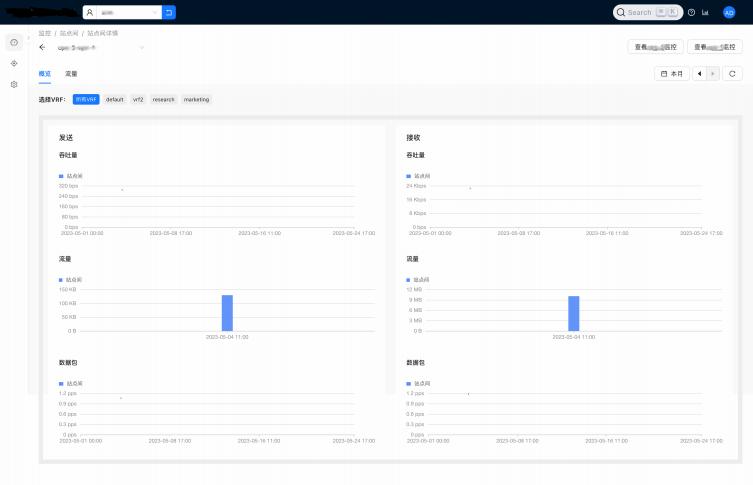


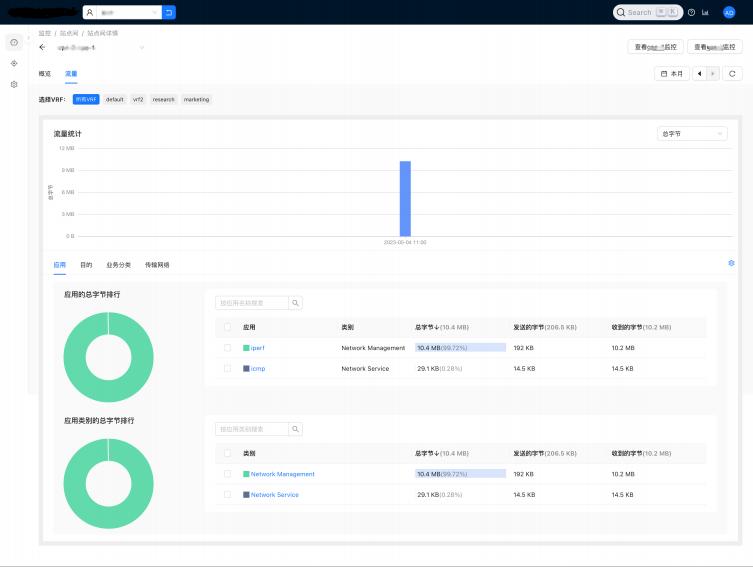
站点间

『租户』 →『监控』 →『站点间』

○ 站点间可以查看站点间吞吐量 、流量和数据包。





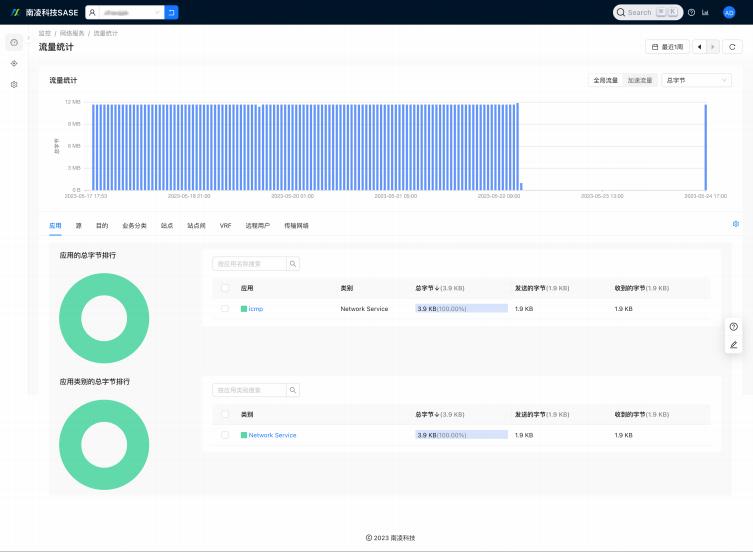


监控-网络服务

『租户』 →『监控』 →『网络服务』

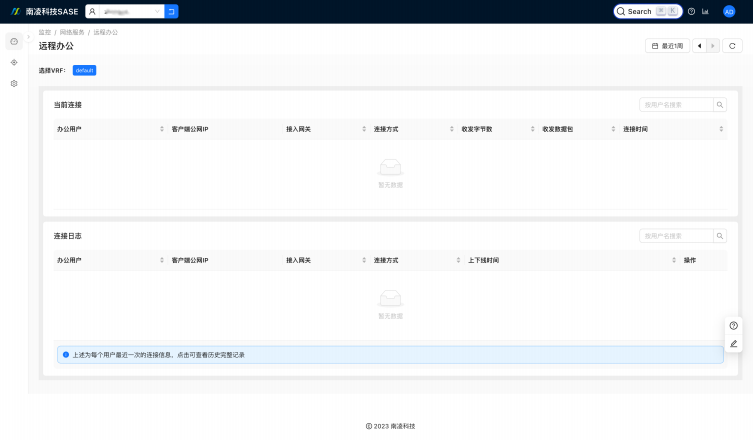
流量统计

 流量统计



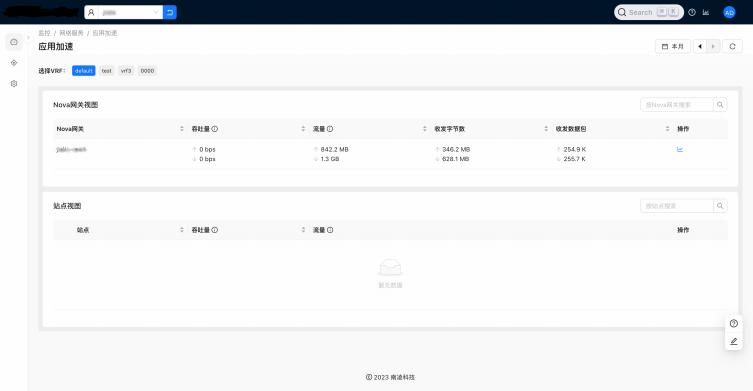
远程办公

 远程办公当前连接， 连接日志

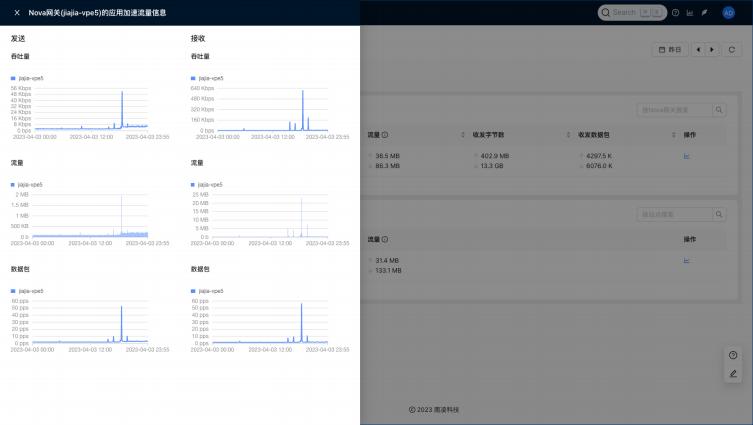


应用加速

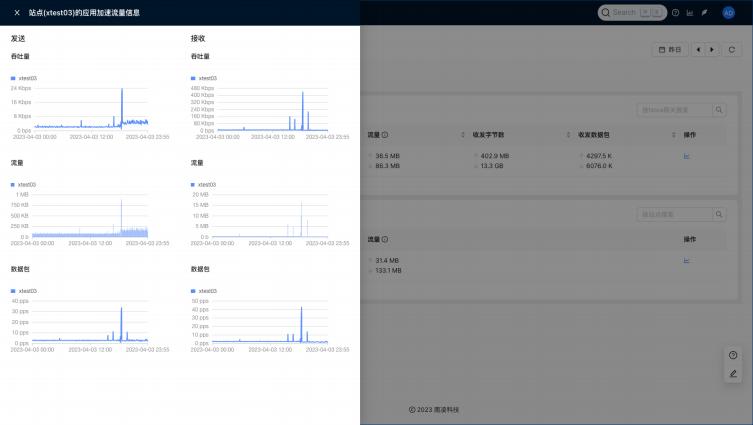
○ 可查看应用加速流量情况



○ Nova网关视角查看历史流量信息

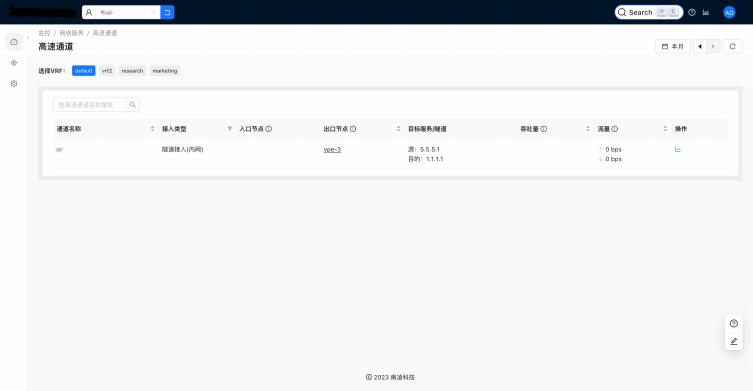


 站点视角查看加速流量信息



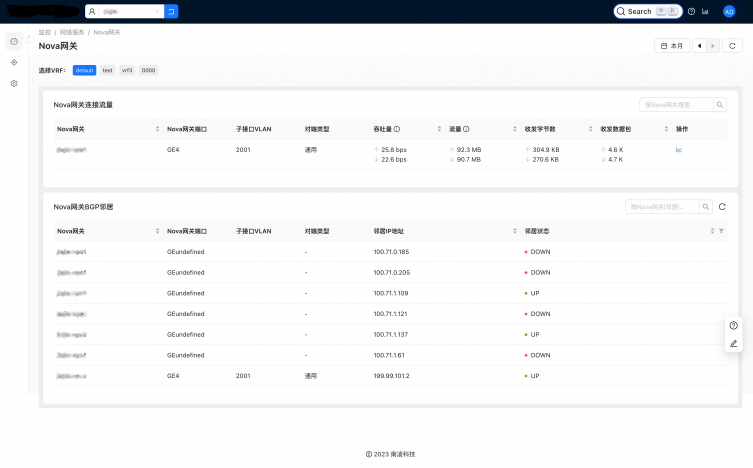
高速通道

○ 高速通道



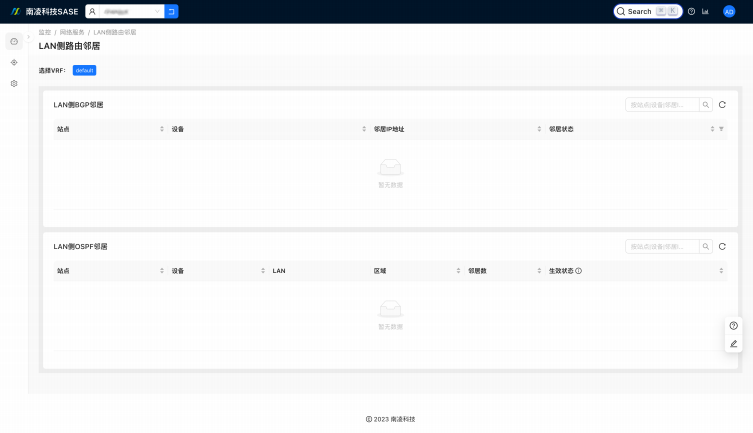
Nova网关

 Nova网关连接流量， Nova网关BGP邻居



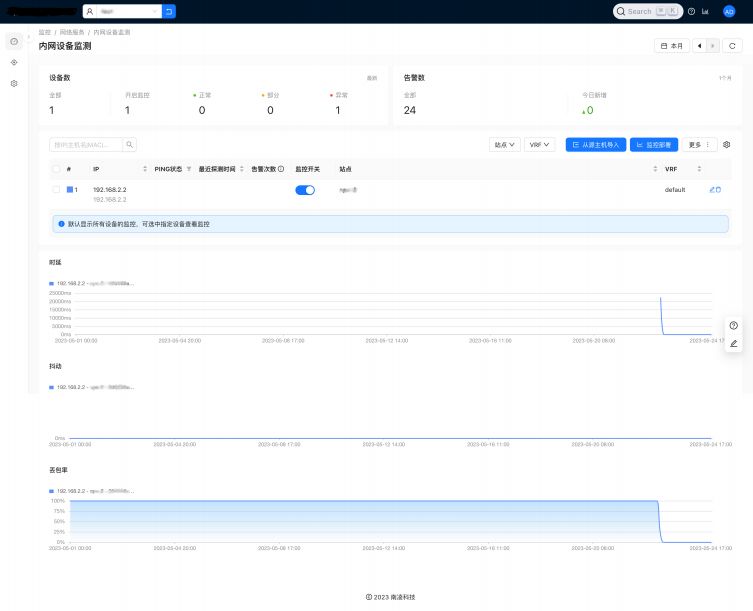
LAN侧路由邻居

○ LAN路由邻居状态



内网设备监测

○ 查看内网设备状态并选择是否开启监控



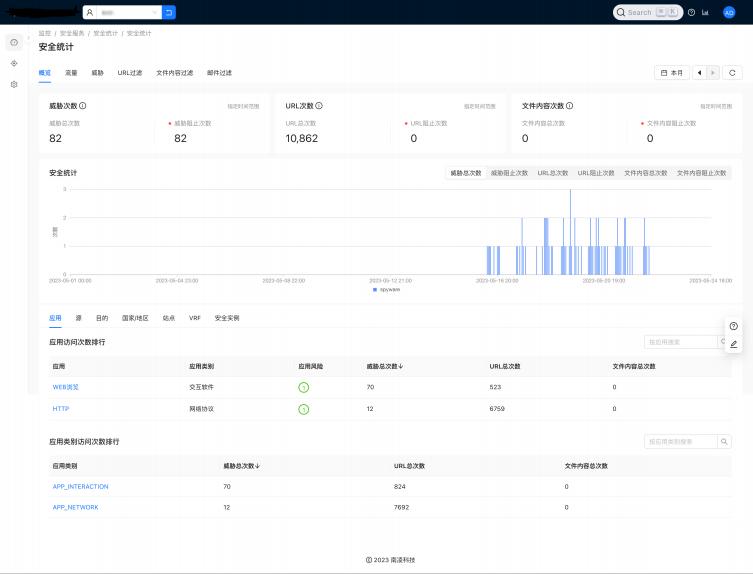
监控-安全服务

安全统计

『租户』 →『监控』 →『安全服务』 →『安全统计』

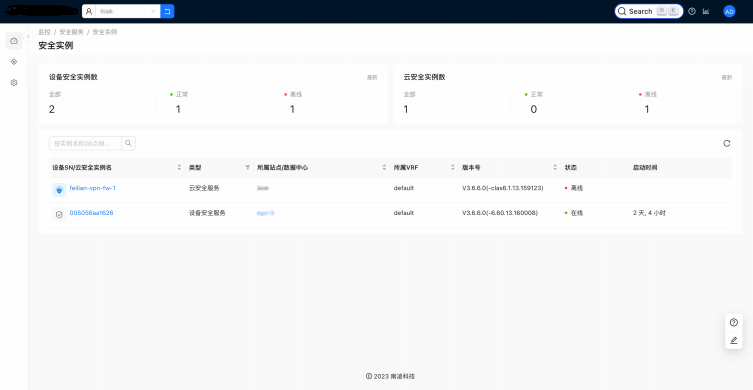
概览 流量 威胁 URL过滤 文件内容过滤 邮件过滤





安全实例

『租户』 →『监控』 →『安全服务』 →『安全实例』



处置中心

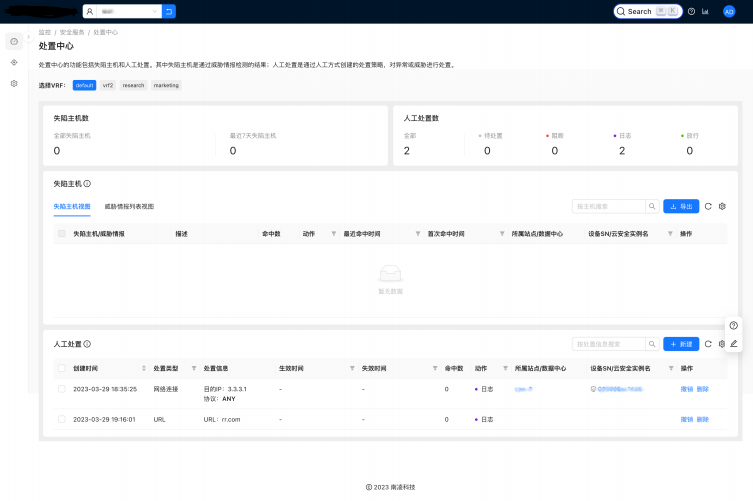
『租户』 →『监控』 →『安全服务』 →『处置中心』

INFO

失陷主机： 当主机访问的地址命中威胁情报库时，会生成—条失陷主机记录

人工处置：对异常或威胁进行处置，人工处置策略的优先级高于威胁情报





失陷主机视图 威胁情报列表视图





监控-告警

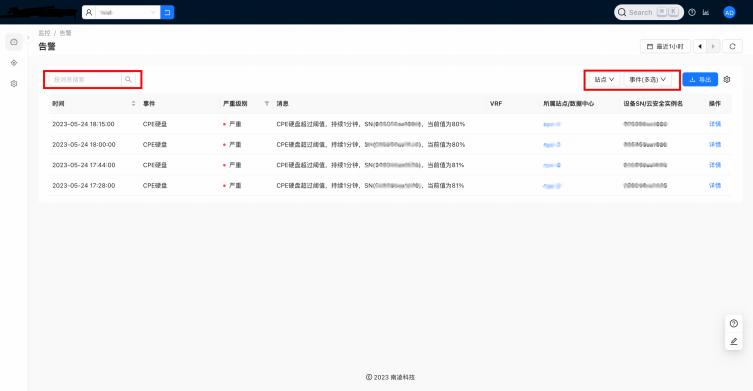
『租户』 →『监控』 →『告警』

· 按消息|VRF|安全实例搜索

 按事件进行筛选（ 多选）

 可自定义时间范围

 可导出告警事件



监控- 日志

『租户』 →『监控』 →『日志』

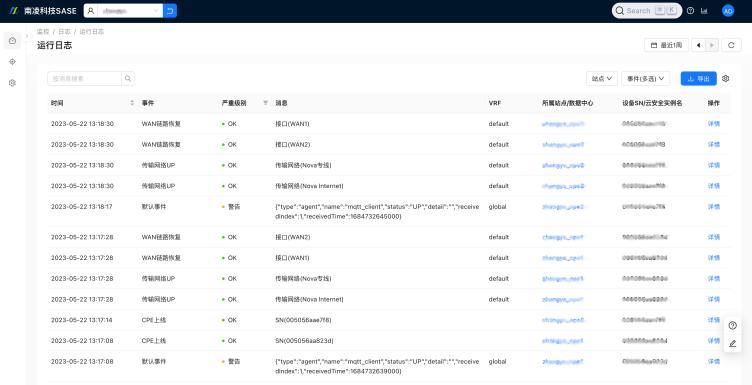
运行日志

 按消息 、SN或站点名进行搜索

 按事件进行筛选（ 多选）

 可自定义时间范围

 可导出日志



运行日志类型

|  |  |
| --- | --- |
| 事件名称 | 事件说明 |
| 端口UP | 端口UP |
| 端口DOWN | 端口DOWN |
| CPE CPU | CPE CPU状态监控 |
| CPE 内存 | CPE 内存状态监控 |

|  |  |
| --- | --- |
| 事件名称 | 事件说明 |
| CPE 硬盘 | CPE 硬盘状态监控 |
| CPE 温度 | CPE 温度状态监控 |
| CPE上线 | CPE和控制器恢复通信 |
| CPE下线 | CPE和控制器断开通信 |
| CPE升级成功 | CPE系统升级成功 |
| CPE升级失败 | CPE系统升级成功 |
| 传输网络UP | 传输网络恢复到有UP的链路 |
| 传输网络DOWN | 传输网络所有链路DOWN |
| CPE链路不可用 | CPE上所有链路DOWN |
| CPE链路恢复 | CPE恢复到有UP的链路 |
| WAN链路不可用 | WAN口所有链路DOWN |
| WAN链路恢复 | WAN口恢复到有UP的链路 |
| 链路UP | 链路UP |
| 链路DOWN | 链路DOWN |
| 链路BGP邻居UP | CPE链路对端BGP邻居UP |
| 链路BGP邻居DOWN | CPE链路对端BGP邻居DOWN |
| 接口探测异常 | 接口探测异常 |
| 接口探测恢复 | 接口探测恢复 |
| LAN侧BGP邻居UP | LAN侧BGP对端邻居UP |

|  |  |
| --- | --- |
| 事件名称 | 事件说明 |
| LAN侧BGP邻居DOWN | LAN侧BGP对端邻居DOWN |
| LAN侧OSPF UP | LAN侧OSPF INSTANCE UP |
| LAN侧OSPF DOWN | LAN侧OSPF INSTANCE UP |
| 链路带宽拥塞 | 链路带宽超过配置的阈值 |
| 链路带宽恢复 | 链路带宽恢复到配置的阈值以下 |
| HA角色切换 | CPE设备的HA角色切换 |
| CPE激活成功 | CPE激活成功 |
| 内网设备探测 | LAN侧配置的PING探测事件 |
| 设备配置失败 | CPE设备配置失败 |
| 设备配置恢复 | CPE设备配置恢复 |
| 设备系统重启 | CPE设备系统重启 |
| VRF连接数 | VRF连接数 |
| 安全服务CPU | 安全服务CPU状态 |
| 安全服务内存 | 安全服务内存状态 |
| 安全服务硬盘 | 安全服务硬盘状态 |
| 安全特征库升级失败 | 安全特征库升级失败 |
| 安全特征库升级成功 | 安全特征库升级成功 |
| Nova网关BGP邻居UP | Nova网关BGP邻居UP |
| Nova网关BGP邻居DOWN | Nova网关BGP邻居DOWN |

|  |  |
| --- | --- |
| 事件名称 | 事件说明 |
| 链路QoS宽带恢复 | 链路QoS宽带恢复 |
| 链路QoS宽带拥塞 | 链路QoS宽带拥塞 |
| CPE Agent UP | CPE Agent UP |
| CPE Agent DOWN | CPE Agent DOWN |
| 配置回滚 | 配置回滚 |
| 病毒事件 | 病毒事件 |
| 攻击事件 | 攻击事件 |
| 异常事件 | 异常事件 |
| 启动事件 | 启动事件 |
| 失陷主机告警 | 失陷主机告警 |
| 默认事件 | 默认事件 |

安全日志

威胁日

志

URL过滤日

志

文件内容过滤

日志

邮件过滤日

志

流量过滤日

志

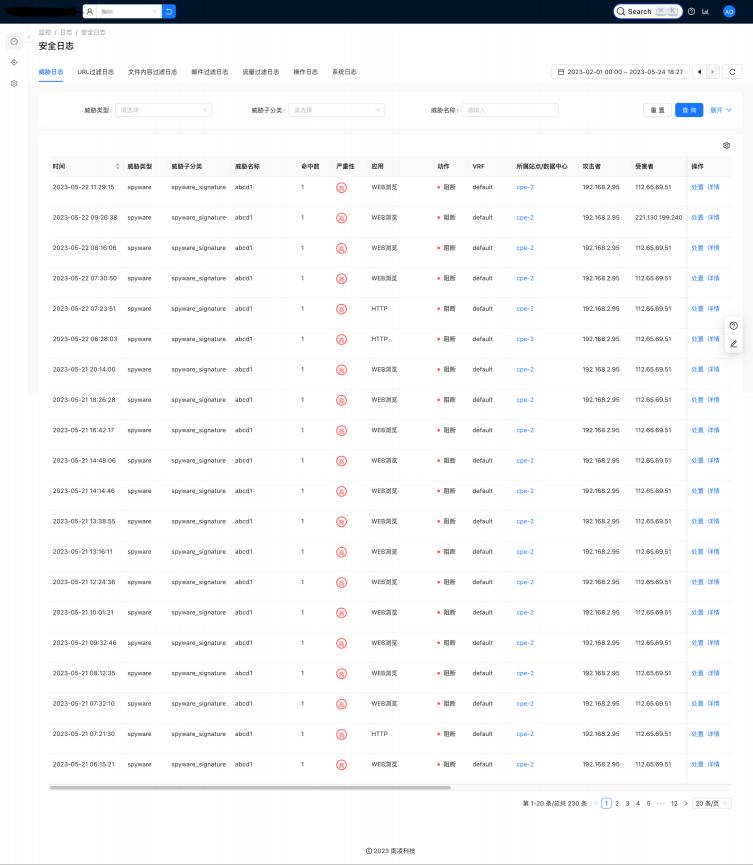
操作日

志

系统日

志

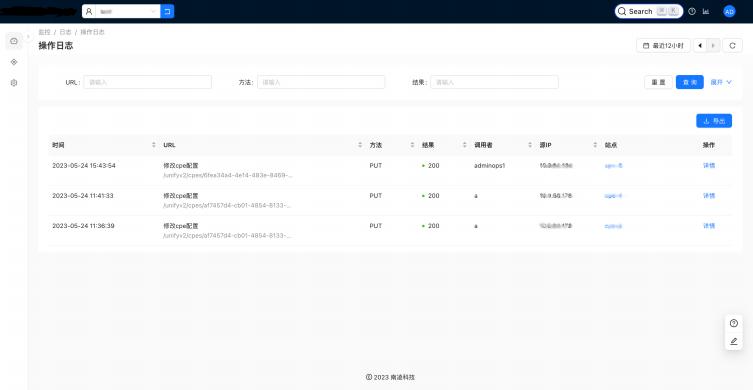




操作日志

 按URL或参数搜索

 可自定义时间范围

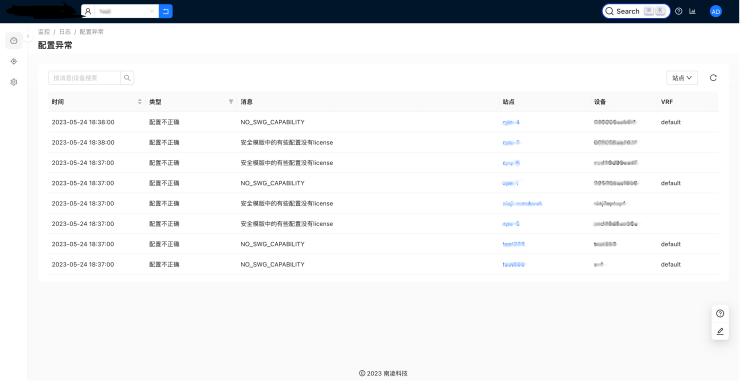


配置异常

控制器对该设备反复下发配置

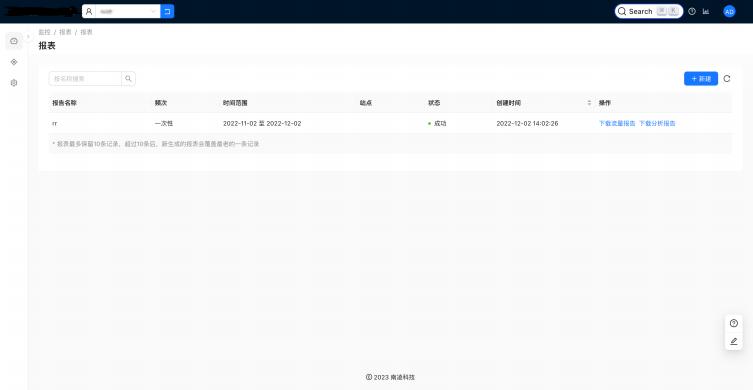
 按消息 、SN或站点名进行搜索

 可自定义时间范围



监控-报表

『租户』 →『监控』 →『报表』



流量报告

 每个VRF的流量占比。

 各个传输网络的流量占比。

 流量使用排名前10的站点。

· 流量使用排名前10的站点间。

 流量使用排名前10的应用。

 流量使用排名前10的业务分类。

 流量使用排名前10的主机。

分析报告

 站点可用性分析

· 站点带宽分析

 站点告警分析

配置-站点

编辑站点

『租户』 →『配置』 →『站点』 →『编辑』

进入站点编辑页面，修改站点基本信息， 配置引用的模板



配置站点

『租户』 →『配置』 →『站点』 →『配置』

进入站点配置页面， 站点的配置还可以通过模板来统—配置和批量下发，所以通用的配置建议通过 模板来完成。

全局配置

『租户』 →『配置』 →『站点』 →『配置』 →『全局配置』

WAN

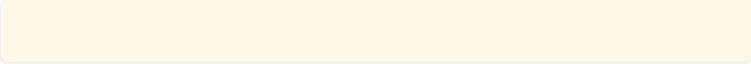
『租户』 →『配置』 →『站点』 →『配置』 →『全局配置』 →『WAN』

配置步骤如下：

· WAN配置：配置传输网络， 配置连接类型， 配置WAN探测；

 传输网络用于与远端建立隧道，根据标签匹配与CPE或Nova网关建立隧道，不填则匹配任意

 [传输网络]决定了该WAN用什么样的链路进行组网 ｜Nova专线 | Nova Internet | Hub-Spoke专线 | Hub-Spoke Internet|

此配置一定要配置，否则无法触发隧道建立

 [优先级]决定了南北向流量从哪个WAN出，数值越低越优先，数值相同则负载分担；  [权重]决定了当优先级相同的情况下WAN的流量分担比，优先级不同时[权重]则无效；

 [禁用Internet能力] 决定了该WAN是否有访问的Internet能力；

 [隧道标签] 拥有相同标签的WAN会建立隧道，不填则匹配任意建立隧道；

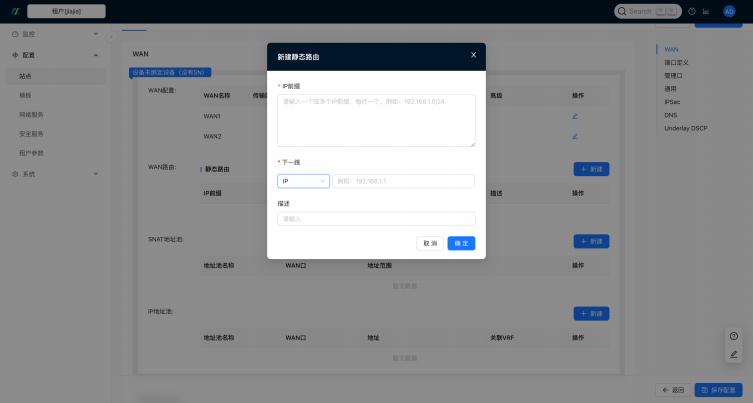
 [公网IP]HUB设备宣告用哪个IP来建立隧道， Hub-Spoke拓扑的Hub必须提前配置公网IP；



· WAN路由：配置静态路由；

 WAN路由不会被发布；

○ 下一跳VRF的路由是WAN到LAN的路由，一般配置了NO-NAT的场景使用；



 SNAT地址池：南北向SNAT的时候可以调用预定义的地址池；

 地址池可以是1个IP， 如果地址池中的IP和wan口IP在同一 网段，必须把地址池中的IP配置到该wan口 的备用IP中。



 IP地址池：



· 传输网络优先级：输入优先级值调整WAN在各个传输网络中的优先级；

 不同WAN配置了相同的[传输网络]， 可输入优先级值，调整WAN在各个传输网络中的优先级， 决定了 东西向流量优先从哪个WAN出，下图为例WAN1比WAN2优先；



端口定义

· 端口定义：配置WAN接口， 支持Vlan子接口；

 创建了子接口的物理接口将不能被使用；



 此类配置推荐使用『模板』统一配置批量下发：『租户』 →『配置』 →『模板』 →『新建』 →『全局

配置』然后与“站点关联”；

管理口

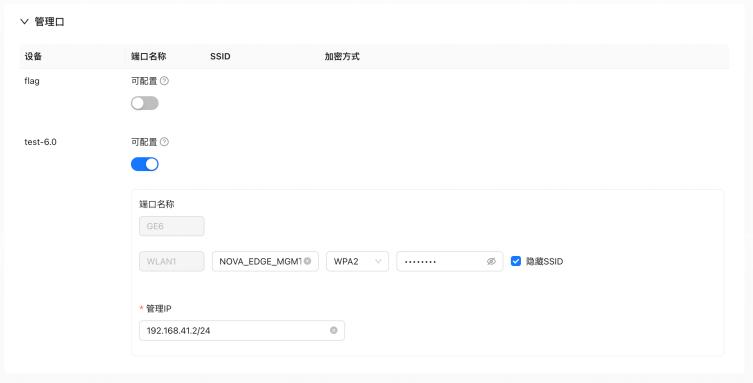


隐藏ssid



 INFO

必须具有WLAN



通用

『租户』 →『配置』 →『站点』 → [通用]

 配置模板：通用配置可以配置到模板中，然后与站点关联， 把配置批量下发到相应的CPE；

 站点配置覆盖模板配置：模板中的配置站点里基本都能配， 如果有勾选覆盖模板配置，则忽略模板配 置， 以站点配置为主；

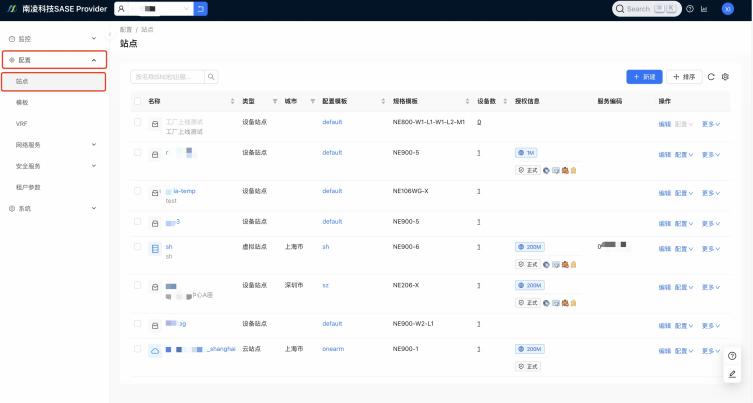
 规格模板：不同硬件有不同的规格模板，该模板定义了接口数量和类型；

此类配置推荐使用『模板』统一配置批量下发：『租户』 →『配置』 →『站点』 → [ ···] → 【编辑】然后配置

模板信息；

1K 设备GUI密码： Device Manager的密码， 默认账号密码为admin/admin；

2K 单臂模式：是否启用单臂模式， 单臂模式启用后不支持MultiVRF；





IPSec

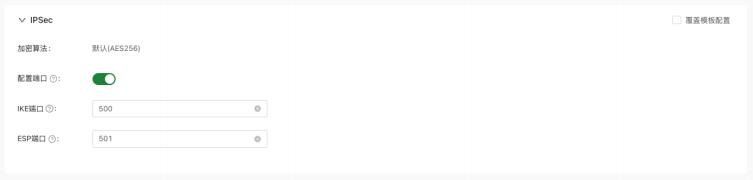
 IPsec配置：加密算法切换， 支持国密。



 配置端口， IKE端口默认1443， ESP端口1444， 可修改为其他端口 。

 IKE端口 可修改为500， 或者大于1024的奇数，不填则为500

 ESP端口 可修改为4500， 或者IKE端口号§1，不填则为4500



DNS

 配置本地域名解析



Underlay DSCP

运营商向用户提供4种服务协约（ SLA）： 金，银，铜， 默认。

 对于这4种服务， 可以指定配置不通的DSCP标签

○ EF 加速转发

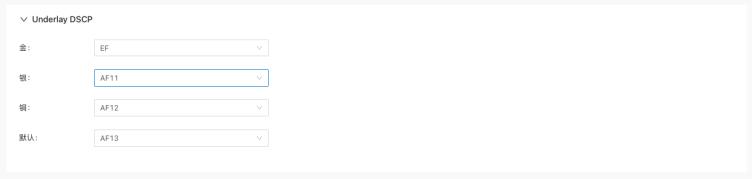
 AF 确保转发

 01 低丢弃优先级

. 10 中丢弃优先级

. 11 高丢弃优先级

○ CS 类别选择



VRF配置

LAN

『租户』 →『配置』 →『站点』 →『配置』 →『VRF网络』

 LAN定义：配置LAN名称， 配置LAN接口， 支持多个LAN， 支持Vlan子接口；

 创建了子接口的物理接口将不能被使用；





· LAN配置：配置LAN IP， 配置DHCP；



只有定义LAN后，才会出现LAN配置项

 Options中文本可自定义填写，但不能加引号；数组可以填写多个IP或者域名， 中间用逗号隔开；



DHCP-BOOT 批量导入静态IP



DHCP-BOOT配置



 LAN路由：配置静态路由， 配置BGP和OSPF；

 静态路由下一跳WAN表示要从本地WAN出去不走东西向隧道；

 静态路由下一跳BLACK HOLE表示Null0路由；

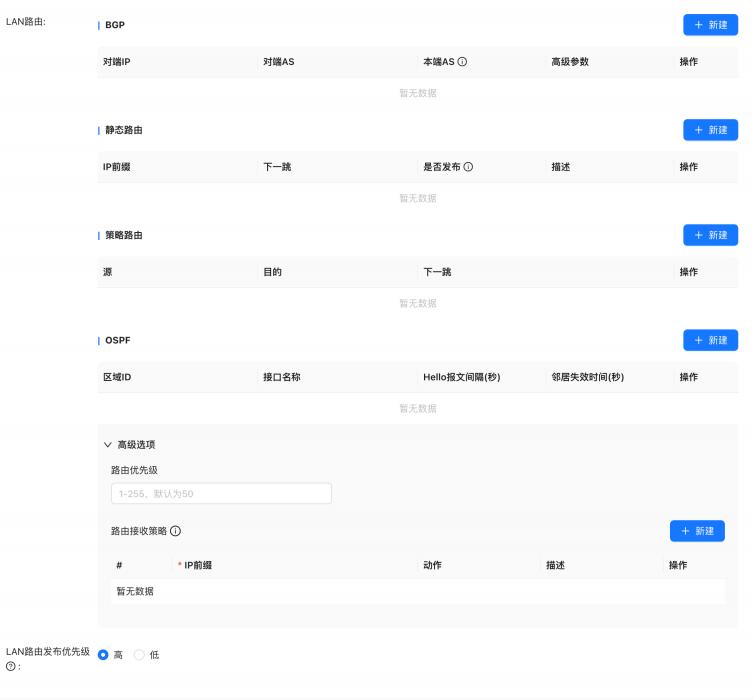
 LAN路由发布优先级，用于发布相同路由条目的站点， 主站点优先级高，备站点优先级低；

 BGPL隐藏ASM可以过滤LAN侧BGP路由中的AS d Path号，但不能过滤路由条目；

 BGPLAS Path Prepend长度]可以向LAN侧发出的路由增加AS d Path跳数；

 BGPL发布策略]和[接收策略]中勾选[严格匹配]则掩码必须精确匹配，不勾选[严格匹配]则掩码为模糊

匹配 。（勾选：ip prefix-list vrf1\_out\_w198.20.0.13 seq 5 permit 199.255.0.0/24；不勾选：ip prefix-list vrf1\_out\_w198.20.0.13 seq 10 permit 199.255.1.0/24 le 32）



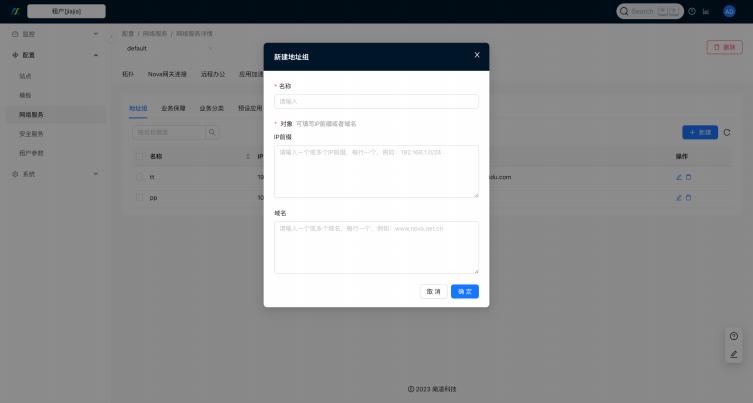
 LAN路由：配置策略路由， 需先配置地址组， 再新建策略路由



|  |
| --- |
| 新建 |

『租户』 →『配置』 →『网络服务』 →『网络对象』 →『地址组』 →

→ 【新建地址组】

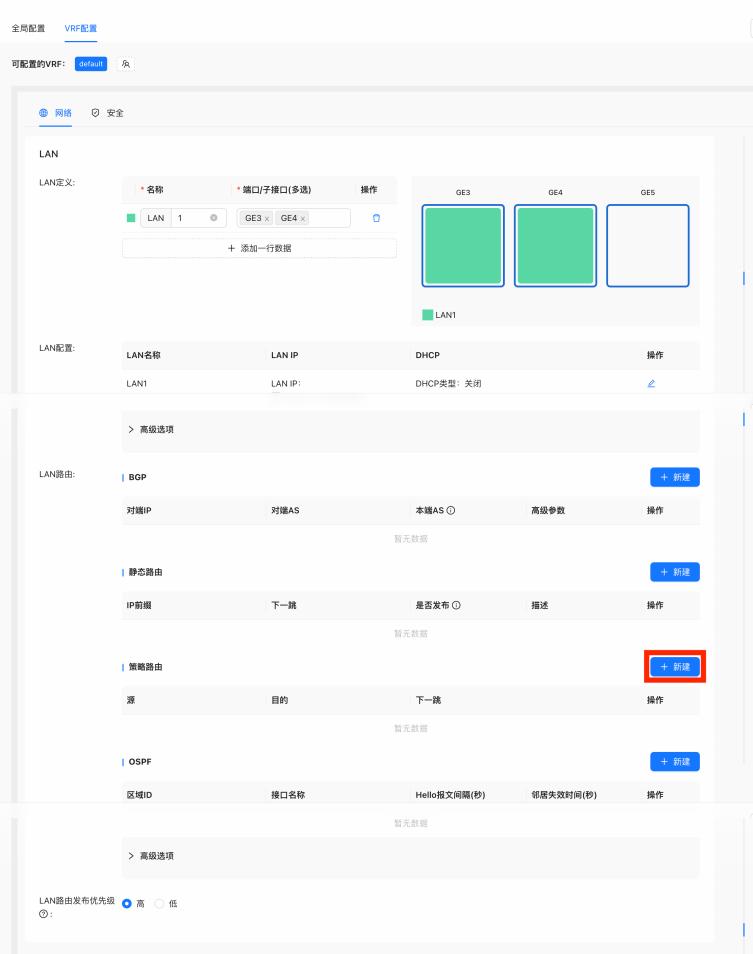


『租户』 →『配置』 →『站点』 → [配置] →



|  |
| --- |
| VRF网络 |

→ 【新建地址组】





WI-FI

『租户』 →『配置』 →『站点』 →『配置』 →『全局配置』， 配置完WI-FI后在LAN定义中调用；

只有具备WI-FI能力NSE才可以打开此配置项。





HA高可用

配置步骤如下：

· 启用HA， 选择VRRP主设备：『租户』 →『配置』 →『站点』 →『配置』 →『全局配置』

· 配置NSE的备用IP：『租户』 →『配置』 →『站点』 →『配置』 →『VRF配置』

 错开DHCP的地址池（ 可选， 如果有必要的话）

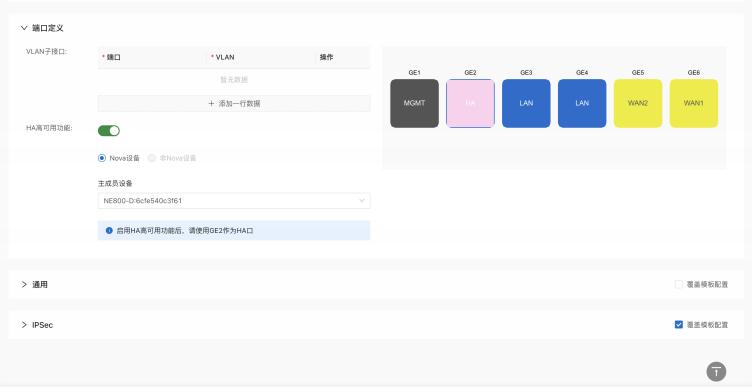
 默认将最后一个LAN口作为HA口连接心跳线， 背靠背连接，不要过交换机；

 Lan配置中填写的LAN IP为VRRP的VIP，备用IP为NSE的实际IP；

 MulitVRF下， 主备NSE保持一致；

 主备NSE通过心跳线可共享WAN，每个Transport除了有通过本地WAN建立的overlay隧道， 还能通 过HA PEER建立一条等价的overlay隧道， 当本地WAN口故障， 可通过心跳线切换至HA PEER的WAN口 出局；

 PFR选路或者故障切换时，会优先考虑HA PEER， HA PEER也不满足则切换到其他Transport的 overlay隧道。





OverLay路由策略

『租户』 →『配置』 →『站点』 →『配置』 →『VRF配置』

 传输网络默认优先级： NOVA\_专线→ NOVA\_INTERNETËHS\_专线→ HS\_INTERNET；

 Per Prefix收发路由设置优先级，优先级可根据需求自定义；

 Per Prefix设置站点路由优先级， 通常由于不同Site但有相同路由的场景；

 收发路由黑白名单，发布只能通过IP前缀过滤，接收可以基于站点 、网关 、IP前缀三种方式来过滤。

 注： 当前加速实现,是在加速网关侧配置IP或者DOMAIN，通过路由协议将该VRF的流量吸到加速网关。

基于策略路由和cpe内部acl：

 可以提供一种新的加速场景

· 可以在站点配置匹配ip和domain的将流量导入隧道上

· 加速网关只发布0.0.0.1和128.0.0.0/1的default路由











防火墙

『租户』 →『配置』 →『站点』/『模板』 →『配置』 →『VRF配置』

防火墙分为普通防火墙和应用防火墙，应用防火墙在普通防火墙的基础上支持应用识别，推荐使用模板配 置， 如有个别站点有特殊配置， 可以用站点配置来覆盖模板配置；

 防火墙所有的匹配条件都是and的关系，必须全部匹配才能匹配上相应流量；

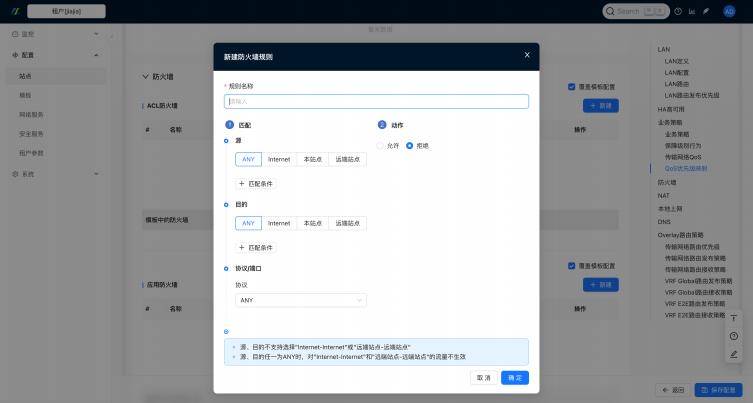
 调用站点区域可以直接匹配站点名称，表示该站点发出的所有流量；

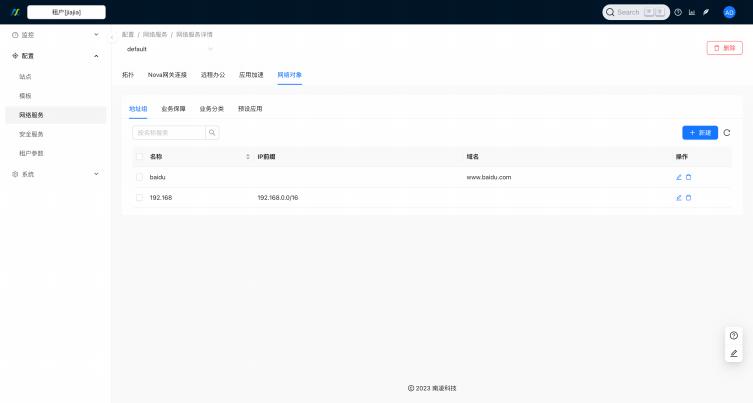
 调用安全组可以定义一段或多个IP网段：『租户』 →『配置』 →『VRF』 →『安全组』；

 防火墙从上往下匹配， 匹配之后则不再匹配；

 普通防火墙优先于应用防火墙；









业务策略

南凌SD-WAN解决方案支持基于IP五元组 、基于应用组 、基于DSCP进行流量分类等， 支持对流量进行队列 优先级调度 、流量整形等QoS策略， 支持通过DSCP重标记等QoS功能 。 为了满足不同的配置场景，提供了 两种QoS配置策略，一种是Overlay网络的QoS，一种是Underlay配置的QoS称 。两种QoS的实现原理相

同， 只是策略应用的范围不同。

当拥塞的情况下有最小的带宽保证



|  |
| --- |
| > 当发生拥塞时如满足所有类保证带宽后 ,还有多余带宽 ，各个类class会按着优先级来占用多余带宽； |

 流量策略分INTERNET流量、站点间流量和应用加速流量，可以设置QOS金银铜、带宽限速和选路策略，推 荐使用模板配置；

业务策略



保障级别行为

针对不同的业务，提供不同的保障模式

 指定传输网路

 质量优先

 故障切换

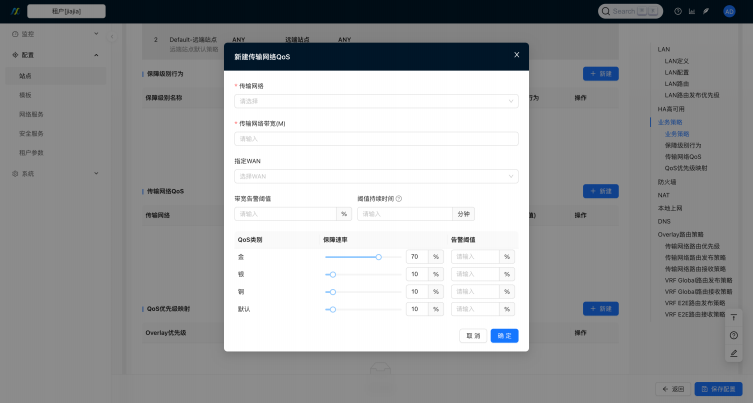


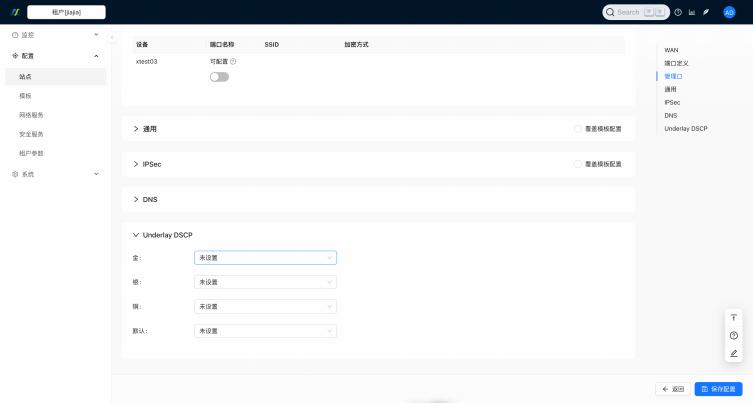
传输网络QoS

 INFO

注:当前qos 带宽的力度是基于transport, 如果同一个transport 有两个不同带宽的wan, 需要可以同 时基于wan来设置

设置每一个传输组的带宽 、带宽告警阈值 、告警持续时间还有速率保障的百分比；





QoS优先级映射



NAT

『租户』 →『配置』 →『站点』 →『配置』 →『VRF配置』

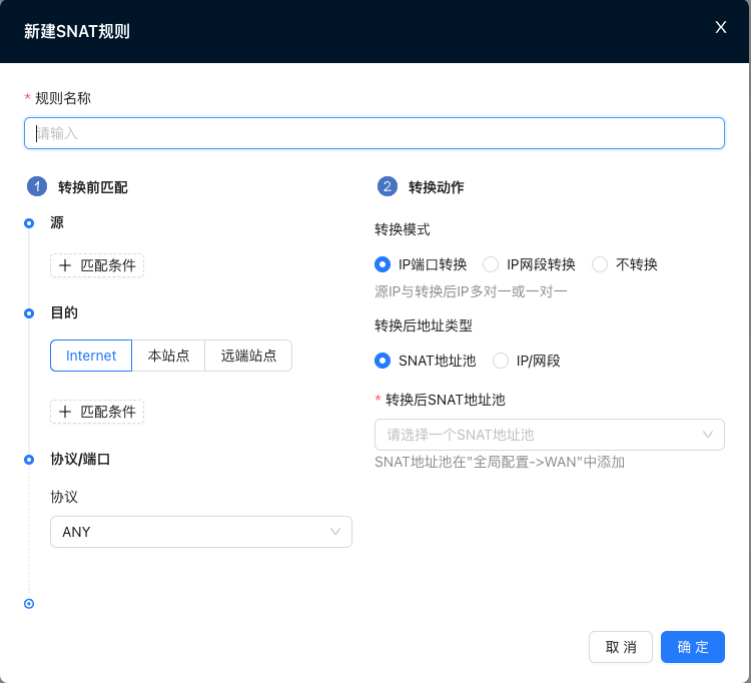
 DNAT的IP映射支持Internet方向；

。 DNAT的IP映射不能被MulitVRF复用；

 SNAT可以关掉Internet方向的NAT，WAN出去不转换源地址。

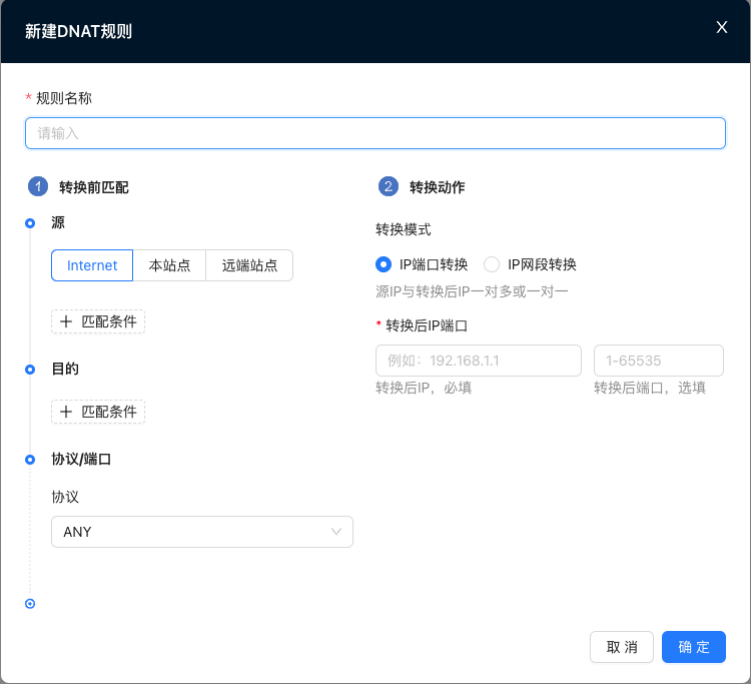
SNAT





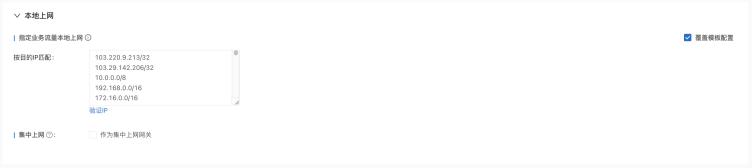
DNAT





本地上网

通过策略路由， 强制流量从本地WAN口出去 。可以选择配置匹配目的IP的方式

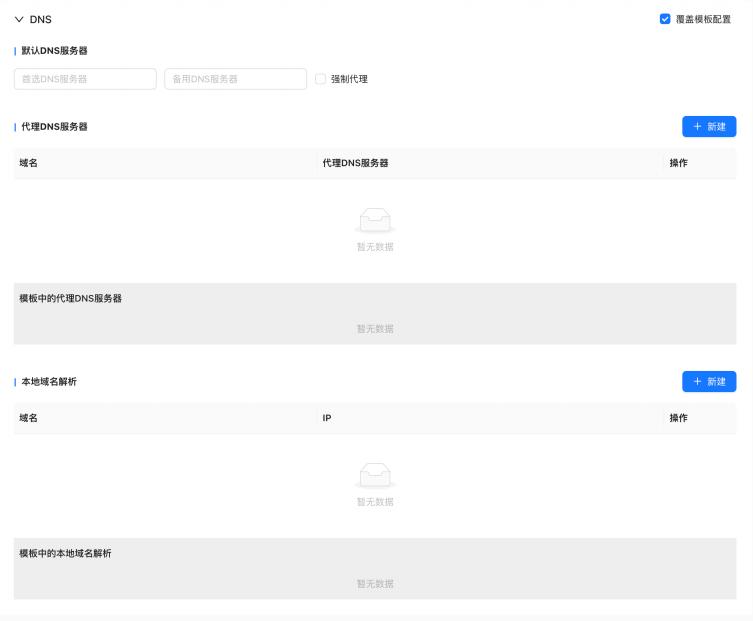


DNS

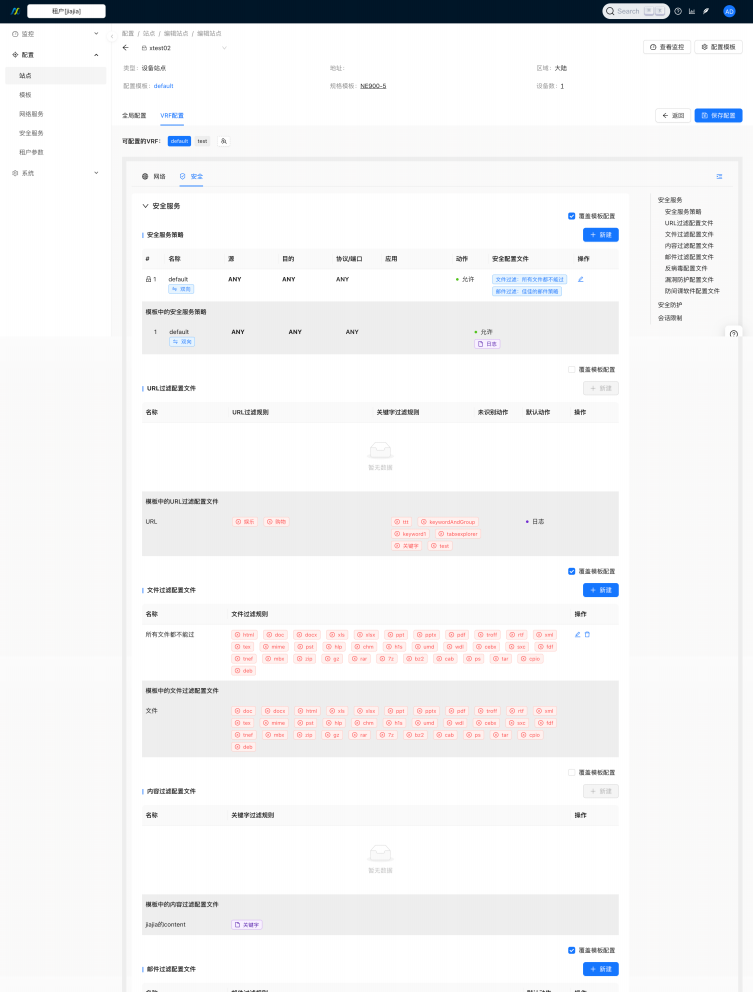
 默认DNS服务器：可以覆盖WAN的DNS配置；

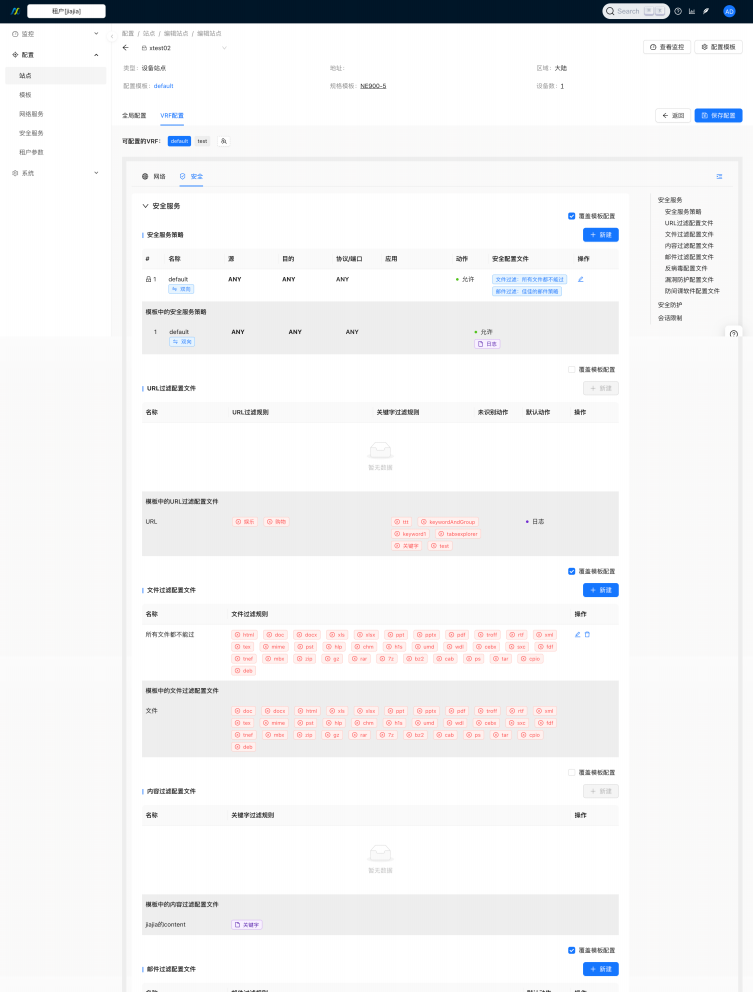
。 代理DNS服务器：指定域名转发到指定DNS解析；

 本地域名解析：配置本地A记录。



VRF安全配置







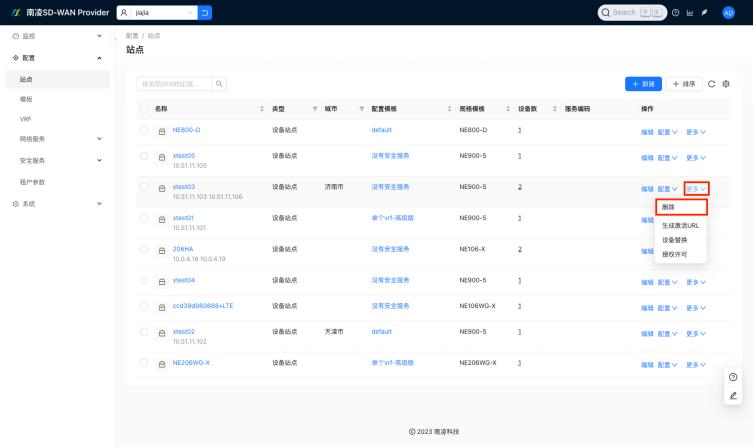
更多操作

删除 生成激活URL 设备替换 授权许可



 INFO

删除站点后无法恢复。



配置-模板

『租户』 →『配置』 →『模板』 → 【新建/编辑】

 配置模板：通用配置可以配置到模板中，然后与站点关联， 把配置批量下发到相应的CPE；

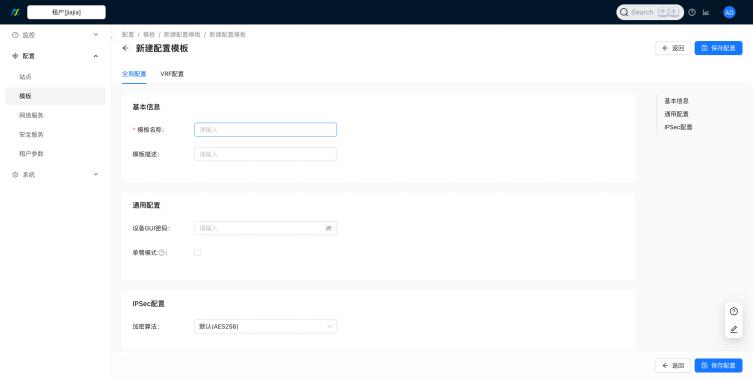
。 站点配置覆盖模板配置：模板中的配置站点里基本都能配， 如果有勾选覆盖模板配置，则忽略模板配 置， 以站点配置为主；

 规格模板：不同硬件有不同的规格模板，该模板定义了接口数量和类型；



全局配置

 模板全局配置：通用配置 、IPsec端口；

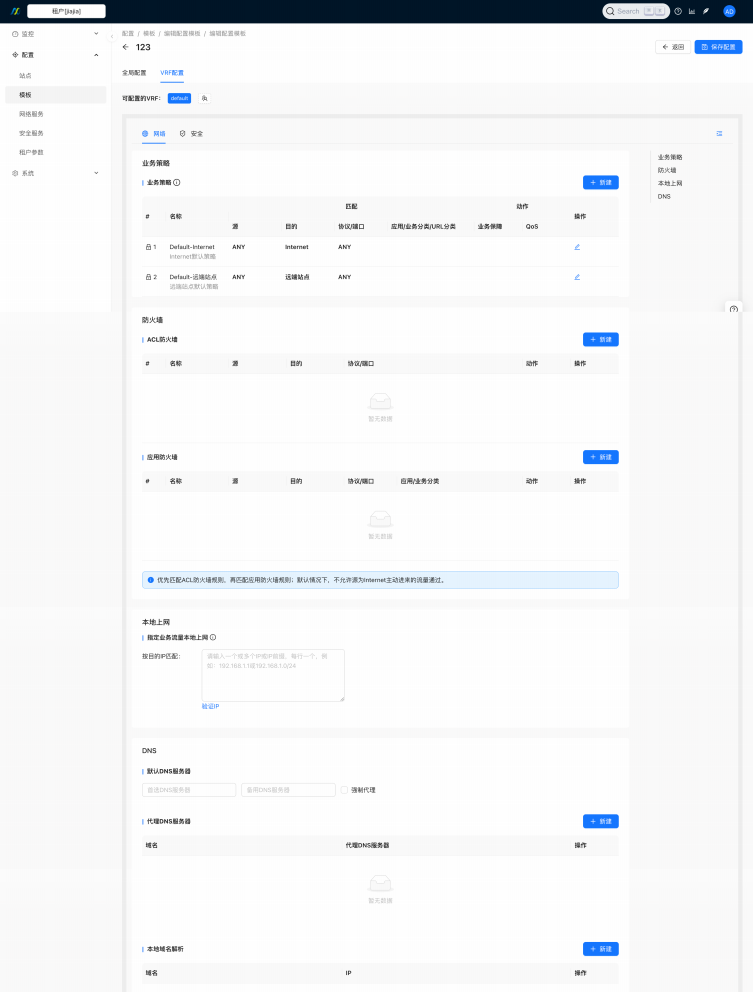


VRF配置

 模板VRF配置：防火墙 、业务策略 、本地上网 、DNS；

网络 安全





配置-VRF

企业内部多个部门业务有隔离要求， 可以通过VRF来构建多个虚拟网络 。保证不同的部门转发独立 ，转发互 相不能访问，从而实现不同部门业务在网络转发层面的安全隔离。

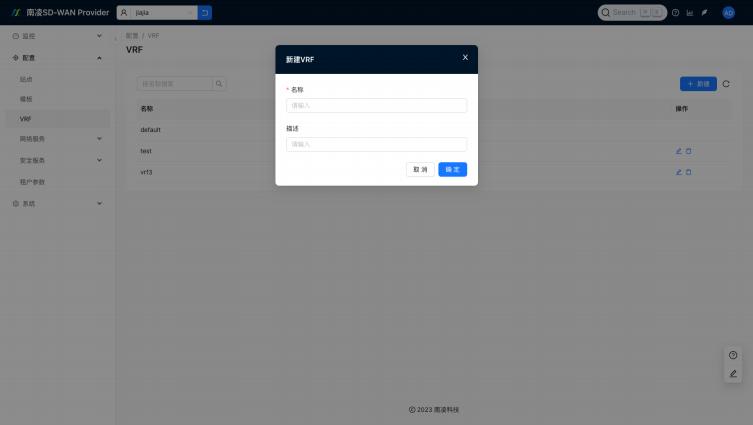
 VRF（VIRTUAL ROUTING AND FORWARDINGK

虚拟路由转发技术通过在一 台三层转发设备上创建多张路由表实现数据或业务的隔离， 常用于

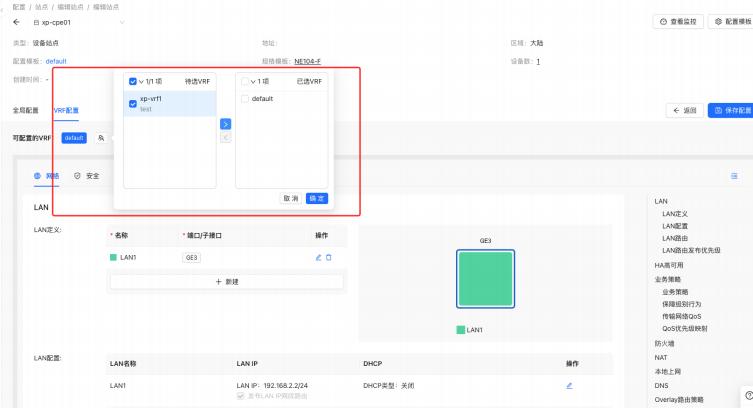
MPLS VPN 、防火墙等一些需要实现隔离的应用场景 。 VRF又称VPN实例（VPN Instance）， 是一 种虚拟化技术，在物理设备上创建多个VPN实例，每个VPN实例拥有独立的接口 ，路由表和路由协 议进程等。

VRF管理

可以在『租户』 →『配置』 →『VRF』 → 【新建】创建多个VRF，每个VRF都可以进行单独的配置并且是完 全独立的。



在『站点』点击任意一个站点名称→『VRF配置』选择自己新建的VRF进行相应的配置



配置-网络服务-拓扑

『租户』 →『配置』 →『网络服务』 →『拓扑』

 VRF不共享拓扑，每个VRF需要单独配置拓扑；

 组网分单层拓扑和分层拓扑：

· 单层拓扑： Nova骨干网 、Hub-Spoke/Full-Mesh 、混合模式（ Nova骨干网 + Hub-Spoke/Full- Mesh）；

 分层拓扑：可建多区域拓扑，一个区域拓扑为一个Hub-Spoke组网， 区域拓扑之间通过Hub可以继续 用Nova骨干网或者Hub-Spoke/Full-Mesh组网；

。 拓扑配置好后还需要在站点中配置NSE的传输组Transport， 否则无法建立隧道组网！

 如果有Full-Mesh组网 ，请确保每个SITE的IPsec端口是相同的 。（IPsec端口默认1443/1444，打

开“配置端口 ”不填任何参数时IPsec端口为500/4500）

单层拓扑

 Nova骨干网 、Hub-Spoke/Full-Mesh 、混合模式配置三选一， 如果选择了混合模式配置会自动继承 到Nova骨干网和Hub-Spoke/Full-Mesh上；

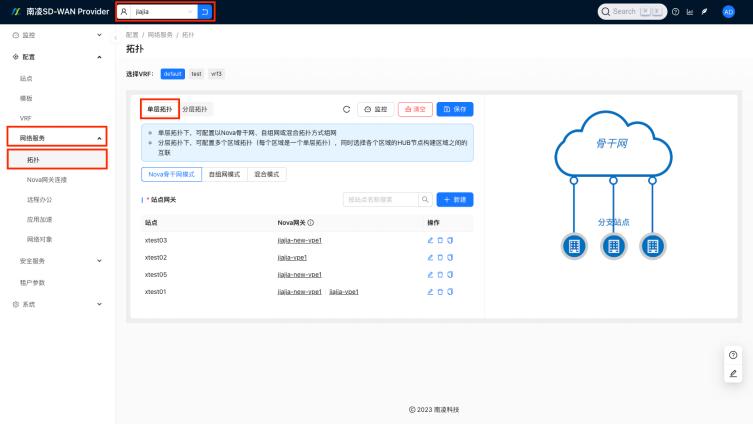
。 Nova骨干网模式站点可以选1个或多个网关，优先级从左到右；

 Hub-Spoke可以选多个Hub， 可自定义优先级， 其余站点的NSE则全部为Spoke；

。 Hub-Spoke的Hub和Full-Mesh的站点需要配置Wan的公网IP， 以确定建立IPsec的IP。

骨干网模式 自组网模式 Nova骨干网模式







|  |
| --- |
| 新建 |

分层拓扑

『租户』 →『配置』 →『网络服务』 →『拓扑』 → [分层拓扑] →



 选择多个网关时， 排在第—个的为主网关， 其余为备网关



 区域拓扑之间通过Hub可以继续用Nova骨干网或者Hub-Spoke/Full-Mesh或者混合组网模式。

Nova骨干网模式 自组网模式 混合模式





配置-网络服务-Nova网关

NOVA网关连接

『租户』 →『配置』 →『网络服务』 →『Nova网关』 →『Nova网关连接』 → 【新建】



Nova网关端口需要选择Nova网关后才可选择， 并且选择的Nova网关需要有NNI端口

INFO



对端类型：通用主要为站点 、数据中心等， 星连为南凌科技的零信任接入网关



BGP路由

【新建Nova网关连接配置】 → 【新建】



 本端AS不填则使用默认值4290000006

 路由发布策略： LAN侧网络与其他站点使用BGP交换路由时，控制本站点发布的路由信息。

 路由接收策略： LAN侧网络与其他站点使用BGP交换路由时，控制本站点接收的路由信息。

路由发布/接收策略

路由发布策略表单与路由接收策略表单基本一致，此处示意图以新建路由发布策略为例





严格匹配勾选后，将严格匹配IP前缀的网段

Nova网关流量引导

 配置规则，将流量引导到云安全服务

新建流量引导配置



 INFO

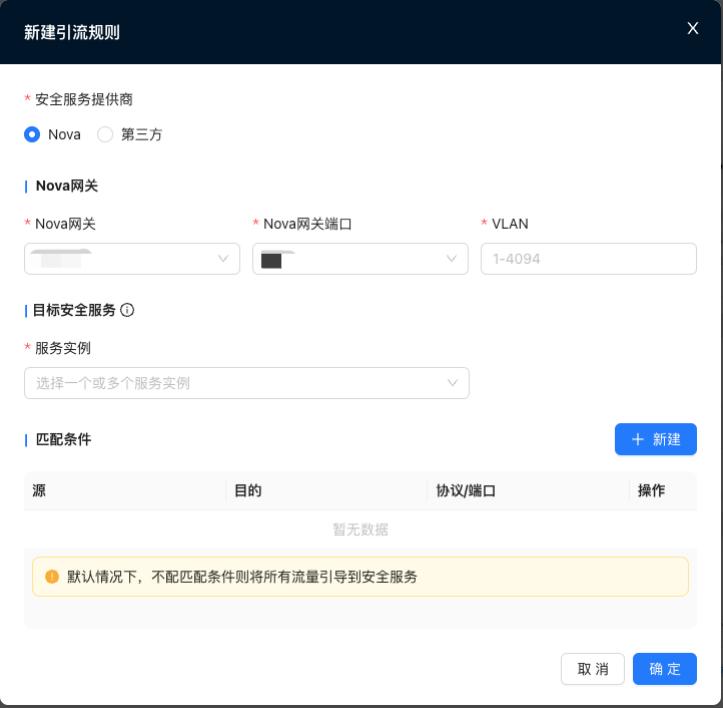
需设置好数据中心并选择数据中心后才可配置引流规则

新建引流规则

 INFO

选择的Nova网关需要含有引流的端口

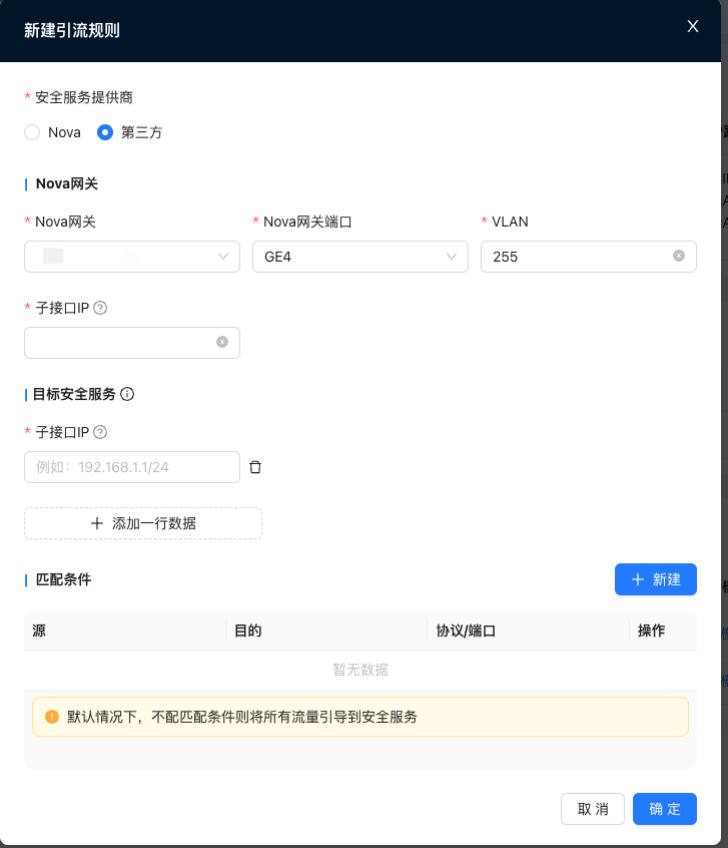
目标安全服务：选择多个服务实例时， 排在第—个安全实例的为主， 其余为备



引流规则的安全服务提供商选择第三方时需要提供以下子接口IP：

 Nova网关与安全服务对接的子接口IP

 安全实例与网关对接的子接口IP（若填写多个， 则第安全实例一个为主， 其余为备）

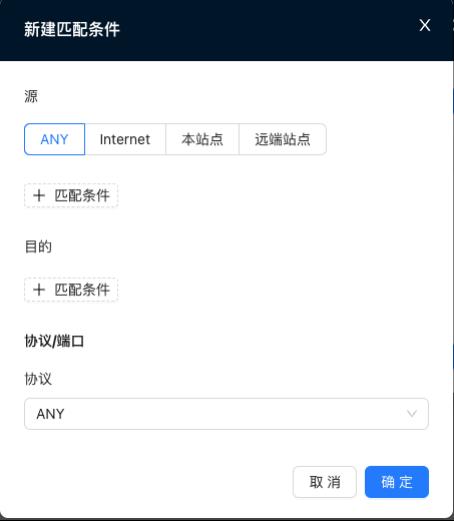


 INFO

若不设置匹配条件则将所有流量引导到安全服务， 建立匹配条件后，则将满足条件的流量引导至安 全服务

新建匹配条件

选择TCP或UDP协议时需要设置源端口以及目的端口， 可不填



Nova网关高级配置

 INFO

配置更多路由 、业务策略 、防火墙 、NAT 、DNS等

Nova网关高级配置流程如下：

1. 点击新建

2. 选择一个Nova网关， 点击确定，创建空的网关配置， 如图1

3. 对该空网关配置进行编辑， 如图2

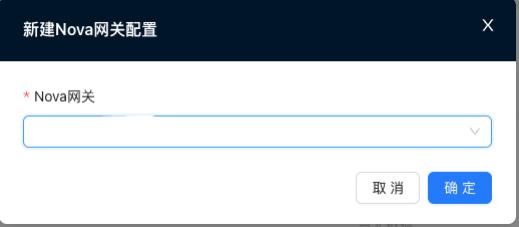
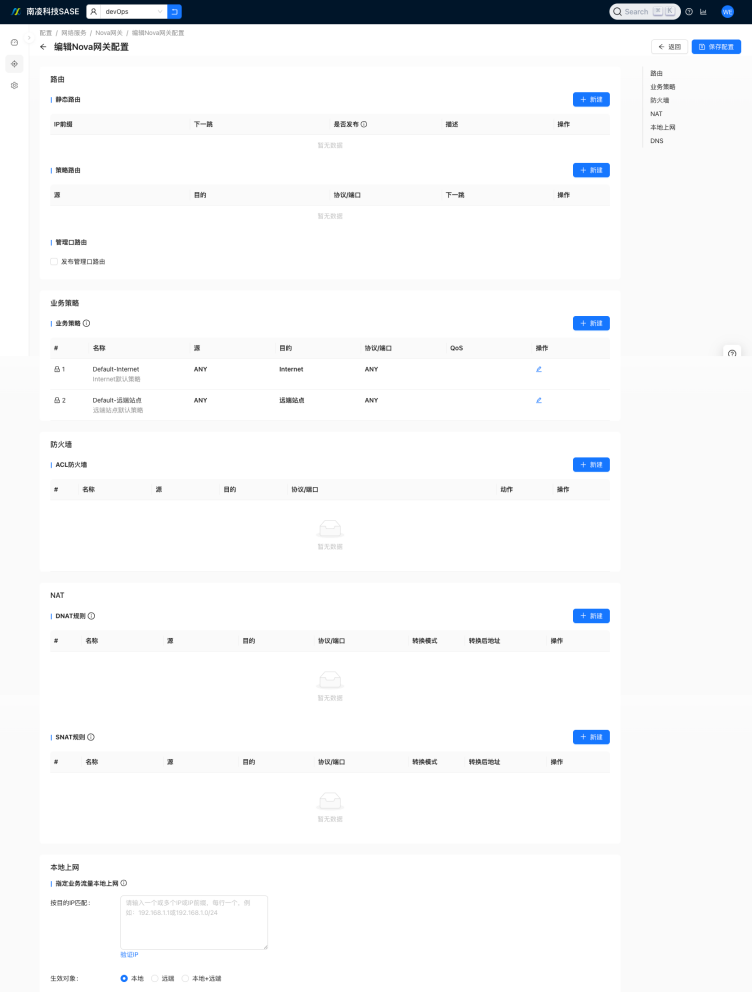


图1 新建Nova网关配置图



图2 Nova网关高级编辑图

Nova网关配置详情页面如图3



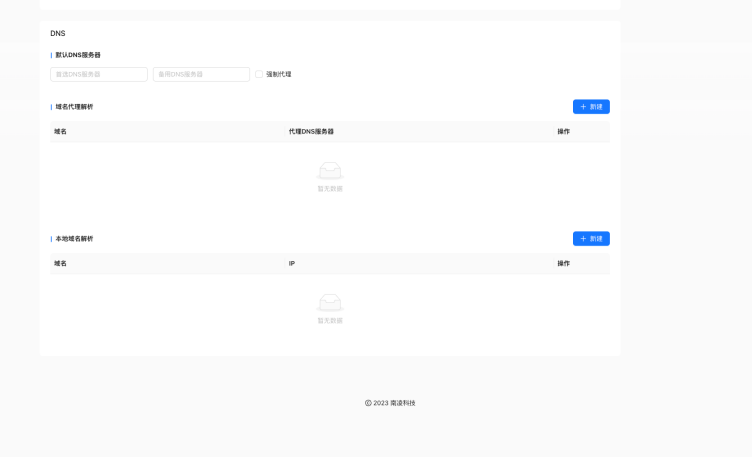


图3 Nova网关高级编辑详情图

下面将从上到下依次介绍各功能

路由

可选择配置静态路由与策略路由， 同时还可发布管理口路由。

静态路由

新建静态路由界面如图4



图4 新建静态路由图

下—跳可选择以下选项：

 IP， 需填入下—跳IP

 其他VRF， 需创建VRF

 WAN

 远端站点

· Black Hole 勾选是否发布后可以将该静态路由发布到其他站点

策略路由

新建策略路由界面如图5



图5 新建策略路由图

可设置编辑匹配条件，新建匹配条件如图6。

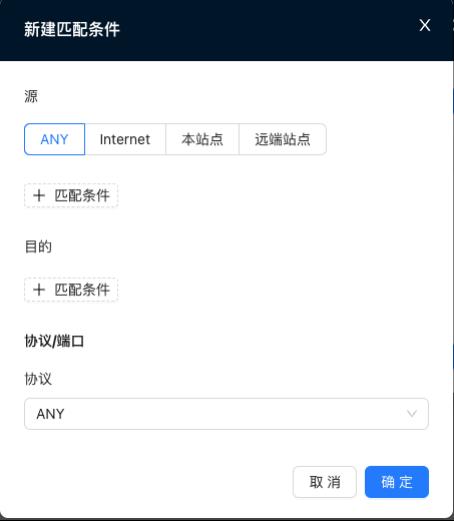


图6 新建匹配条件图

可选匹配源的类型。

点击匹配条件后可直接匹配IP，也可设置地址组。

地址组位于『租户』 →『配置』 →『网络服务』 →『N网络对象』 →『地址组』 此处可对地址组进行新建或 者编辑。

协议若选择TCP或UDP可选择填写端口 。

业务策略

 INFO

新建业务策略时需注意以下问题：

· 源 、 目的不支持选择"Internet-Internet"或"远端站点-远端站点"

· 源 、 目的任一为ANY时，对"Internet-Internet"和"远端站点-远端站点"的流量不生效

 源为本站点时支持配置源主机限速



 目的为本站点时支持配置目的主机限速



新建业务策略

新建业务策略表如图7



图7 新建业务策略表

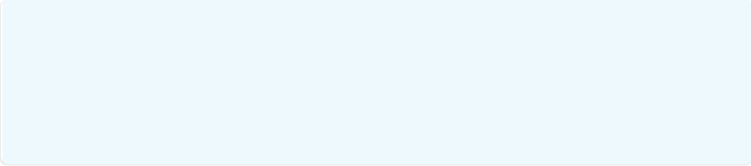
 打开优先级，优先级的可选择默认 、金 、银 、铜

· 打开策略限速， 可选择对带宽进行限速， 最大为1000000Mbps

· 源为主机本站点时支持配置源主机限速

 目的主机为本站点时支持配置目的主机限速

防火墙



 INFO

新建防火墙规则时需注意以下问题：

· 源 、 目的不支持选择"Internet-Internet"或"远端站点-远端站点"

· 源 、 目的任一为ANY时，对"Internet-Internet"和"远端站点-远端站点"的流量不生效

新建防火墙规则

新建防火墙规则表单如图8



图8 新建防火墙规则表单图

NAT

此项可配置DNAT与SNAT。

DNAT：用于配置DNAT功能，可将 [ 转换前IP/网段，协议，端口 ] 映射成 [ 转换后IP/网段，协议，端口 ]，外部网络可以通过映射后地址访问内部网络，从而使内部网络可对外提供服务。

SNAT：用于配置SNAT功能，可将 [ 转换前IP/网段 ] 映射成 [ 转换后IP/网段 ]， 内部网络可以通过映射后 地址访问外部网络，但外部网络不能通过映射后地址主动发起对内部网络的访问

新建DNAT规则

新建DNAT规则表单如图9

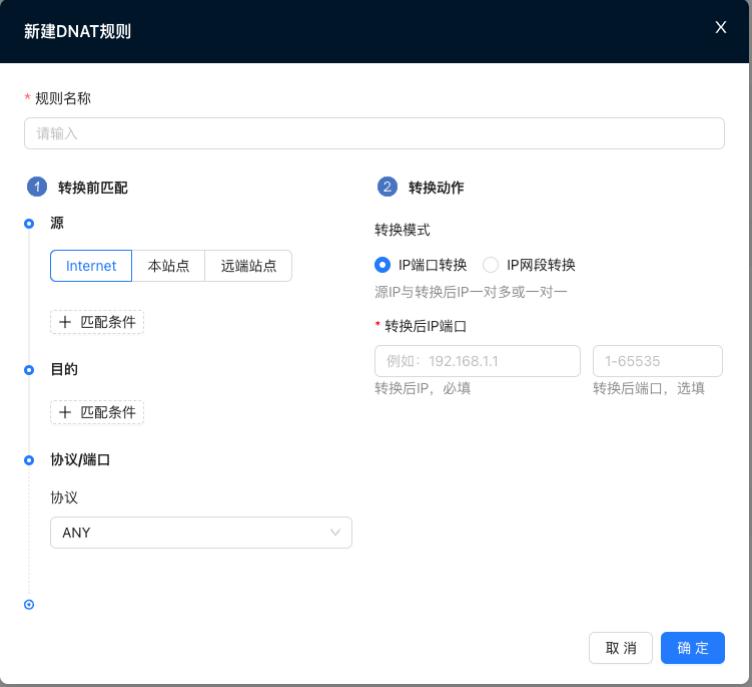


图9 新建DNAT规则表单图

 INFO

若进行IP端口转换， 源IP与转换后IP—对多或—对—。

若进行IP网段转换， 源IP网段与转换后IP网段—对— 。若固定不变 。不转换端口

新建SNAT规则

新建SNAT规则表单如图10

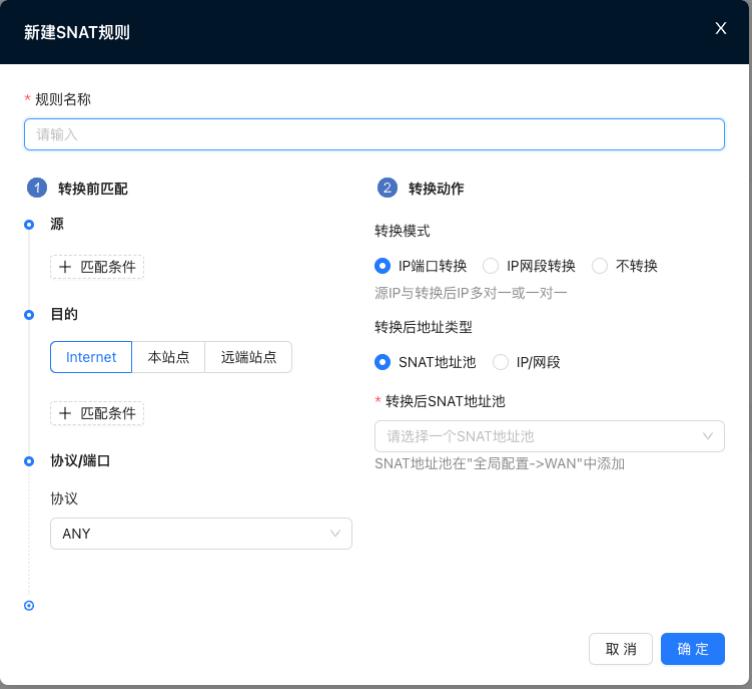


图10 新建SNAT规则表单



INFO

若进行IP端口转换， 源IP与转换后IP一对多或一对一。

若进行IP网段转换， 源IP网段与转换后IP网段一对一 。若固定不变 。不转换端口

若不转换，则不对源IP转换 SNAT地址池在『租户』 →『配置』 →『站点』 →『配置』 →『全 局』 →『WAN』 中的SNAT地址池添加



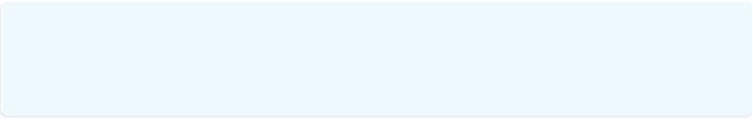
本地上网

本地上网如图11



图11 本地上网图

由于目的IP较多，不清楚新IP是否已在目的IP中 。故可点击验证IP，验证新添加的IP是否已在目的IP表中。



 INFO

通过策略路由， 强制流量从本地WAN口出去 。此处可以选择配置匹配目的IP的方式将流量从本地 WAN口出去

DNS

DNS配置如图12， 可选择强制代理

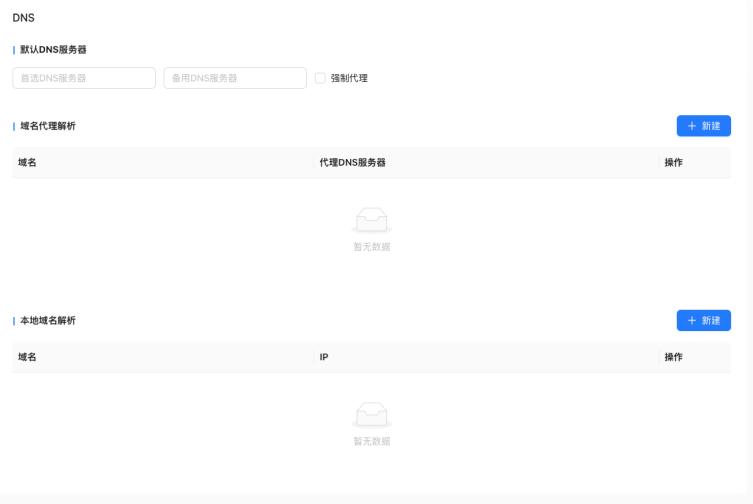


图12 DNS配置图

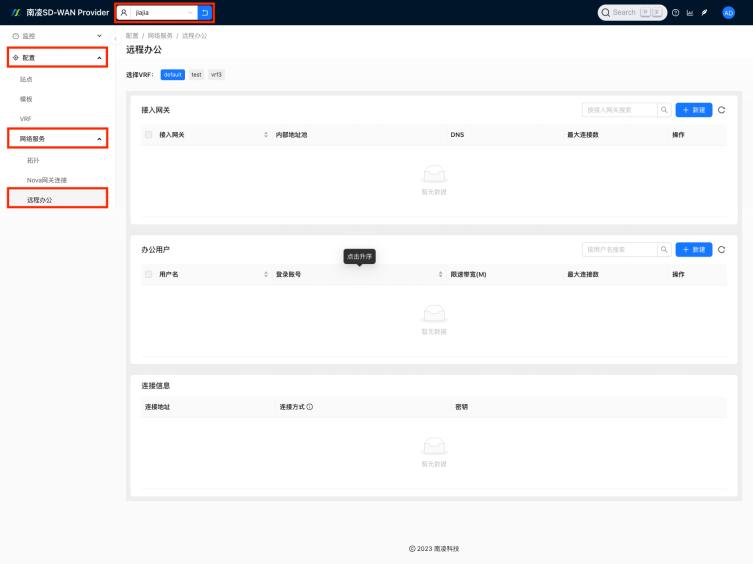
配置-网络服务-远程办公

『租户』 →『配置』 →『网络服务』 →『远程办公』

配置接入网关和办公用户；

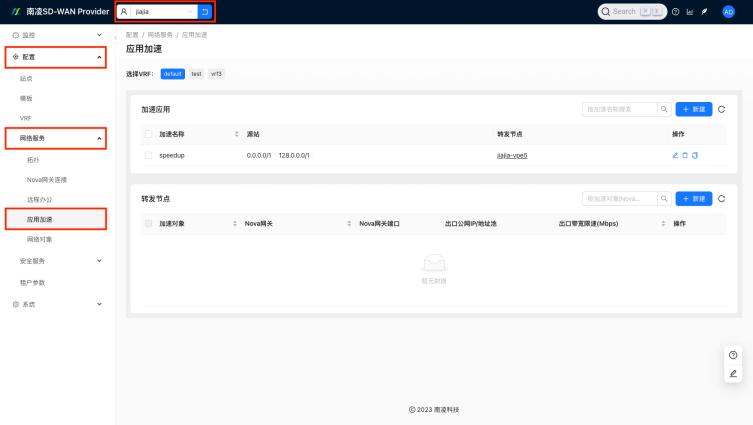
移动端ipsec/l2tp vpn拨号接入， 操作系统自带客户端；

IPsec不需要组账户；



配置-网络服务-应用加速

『租户』 →『配置』 →『网络服务』 →『应用加速』



把需要加速的目标IP/网段或者域名通过加速网关转发；

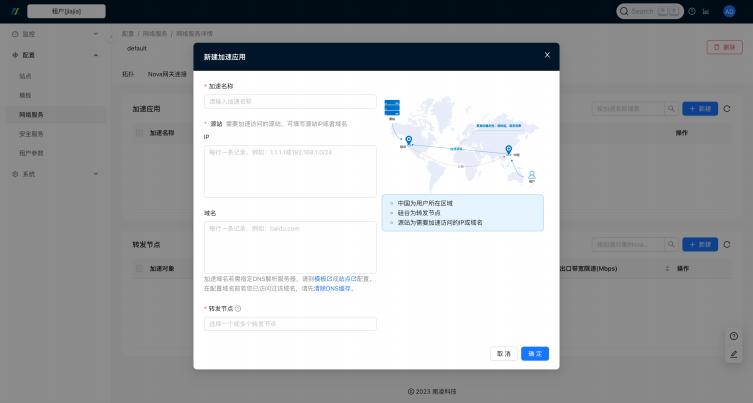
应用加速网关只能选择类型为[应用加速]的网关， 其他网关不可使用；

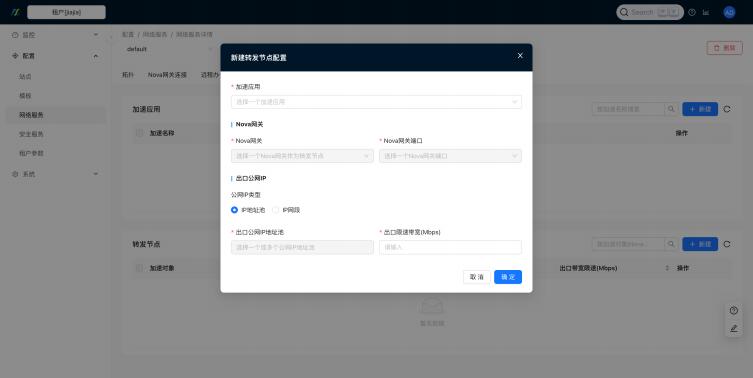
支持域名填写， 支持SNAT；

DNS必须通过加速网关出局， 让网关获取域名解析回来的IP地址；

先创建[加速名称]，后创建[加速对象]，加速对象调用之前创建的[加速名称]；

路由不能重叠， 如有重叠需要分开两条策略 。（比如：0.0.0.0/1 、128.0.0.0/1 、210.75.24.195， 其 中默认路由已经包含<210.75.24.195>，所以这种情况要分开写两条策略）

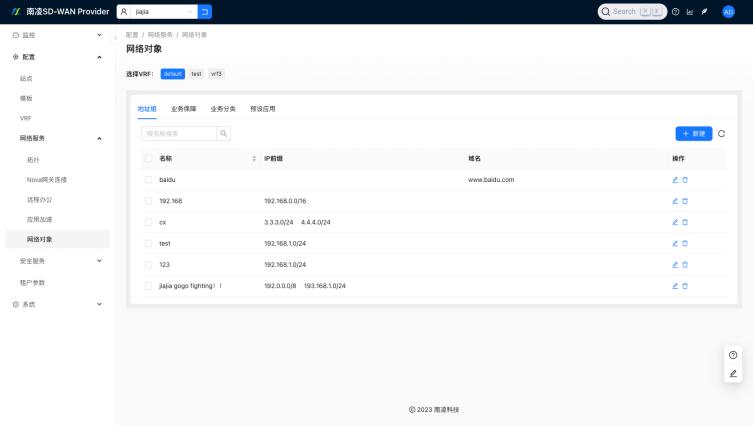


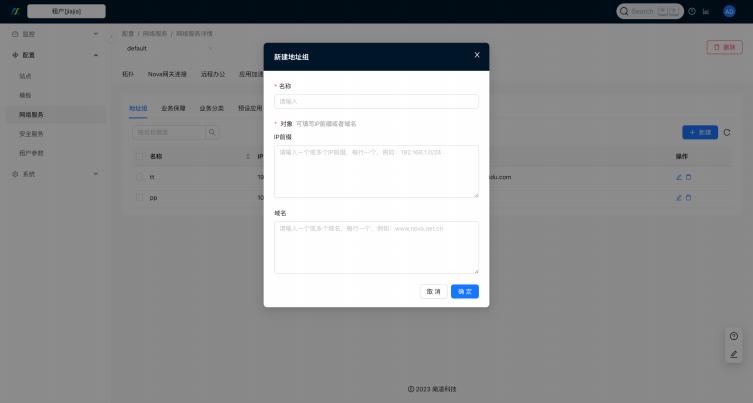


配置-网络服务-网络对象

地址组

『租户』 →『配置』 →『网络服务』 →『网络对象』 →『地址组』 →『新建』 → 【新建地址组】

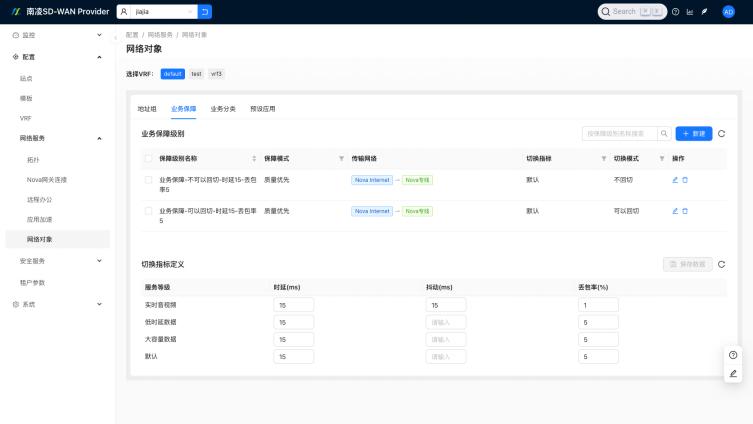




业务保障

创建业务保障

『租户』 →『配置』 →『网络服务』 →『网络对象』 →『业务保障』 →『新建』 → 【新建业务保障级别】





 指定传输网络：只选一条路径，任何情况下不切换路径

 质量优先：可以选择多条路径，根据优先级选择路径转发，根据切换指标动态切换路径 切换指标：切换指标有预定义， 通常不建议修改

 故障切换：可以选择多条路径，根据优先级选择路径转发， 可选择是否回切

创建业务策略

『租户』 →『配置』 →『模版』 →『编辑』 →『VRF网络』 →『新建』 → 【新建业务策略】

在业务策略中开启业务保障， 选择业务保障级别



覆盖保障级别行为

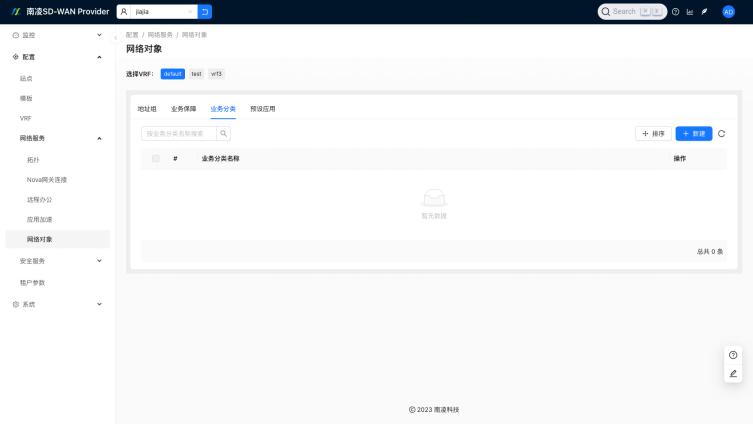
网络对象中配置“业务保障”是不能指定WAN口的，但在站点配置中调整“业务保障”可精确到WAN口 ，用来 满足同传输网络不同WAN之间的应用选路。

『租户』 →『配置』 →『站点』 →『配置』 →『VRF网络』 →『网络』 →『业务策略』 →『保障级别行为』

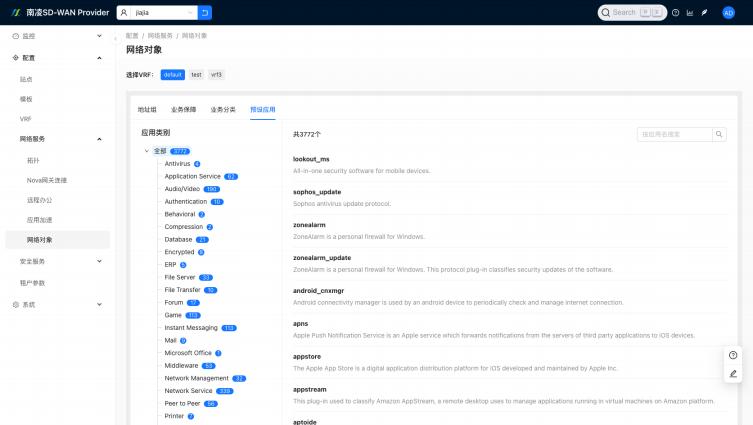


业务分类

『租户』 →『配置』 →『网络服务』 →『网络对象』 →『业务分类』 →『新建』 → 【新建业务分类】



预设应用



配置-网络服务-高速通道

高速通道可通过『租户』 →『配置』 →『网络服务』 →『高速通道』进行新建 、编辑 、设置， 如图1所示。

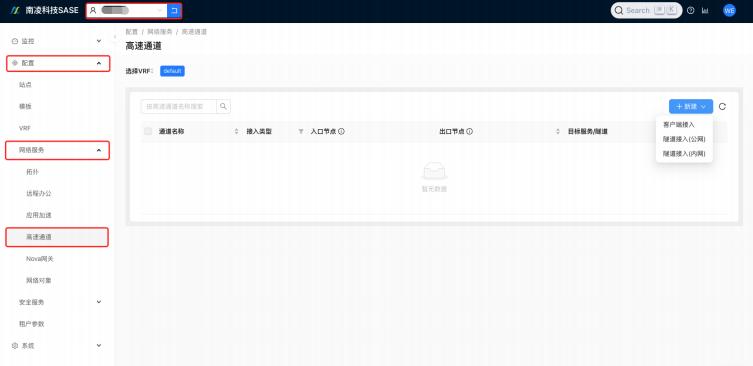


图1 高速通道示意图

 INFO

接入高速通道须知：

 入口节点需选择客户端所在区域或者就近区域的节点。

 出口节点负责将数据通过公网转发给目标服务器， 出口节点—般与目标服务器所在地距离较 近。

 入口节点端口与出口节点端口都是wan口

客户端方式接入

客户端方式接入高速通道的新建表单如图2所示



图2 客户端方式接入高速通道

隧道方式接入（公网）

隧道方式接入高速通道（ 公网）新建表单如图3所示

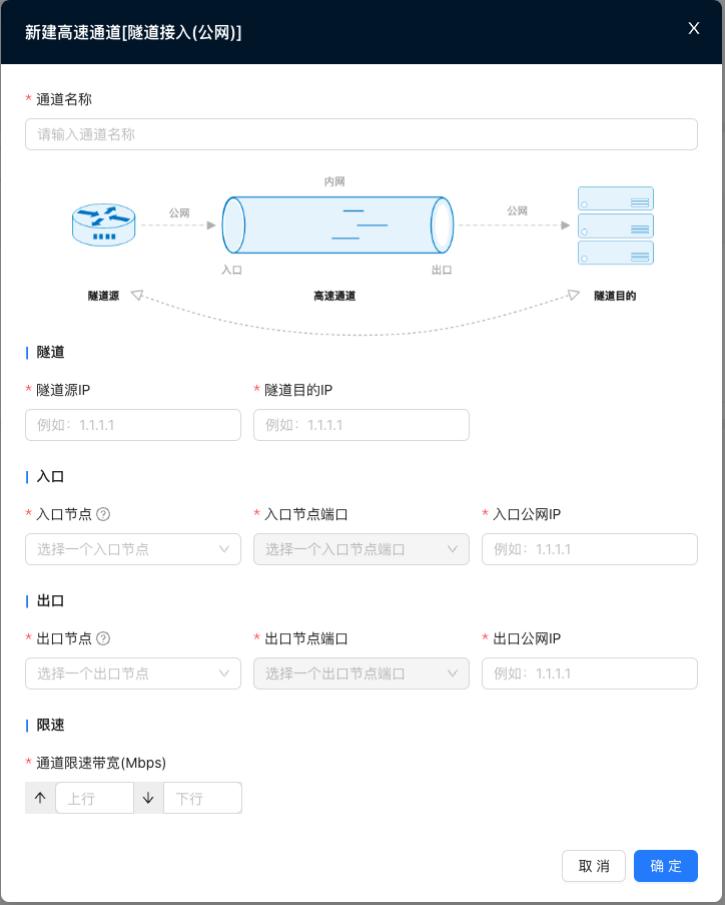


图3 隧道方式接入高速通道（ 公网）

隧道方式接入（ 内网）

隧道方式接入高速通道（ 内网）新建表单如图4所示



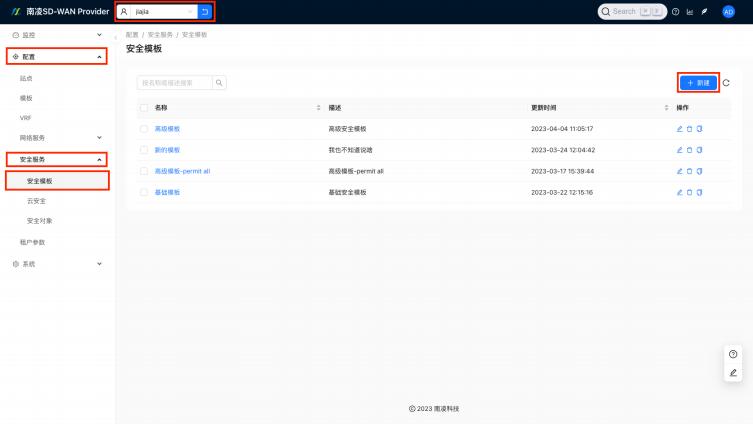
图4 隧道方式接入高速通道（ 内网）

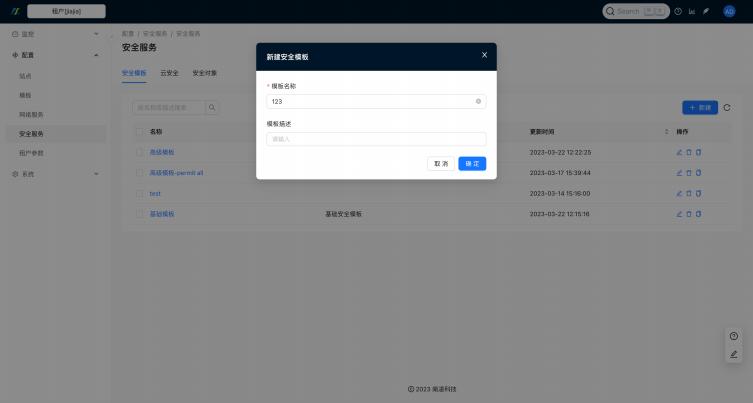
配置-安全服务-安全模版

通过安全模板来做—些安全配置，例如URL过滤 、文件过滤 、内容过滤 、邮件过滤 、反病毒以及设置安全服 务策略等

新建安全模板

『租户』 →『配置』 →『安全服务』 →『安全模板』 →『新建』 → 【新建安全模板】





编辑安全模板

 INFO

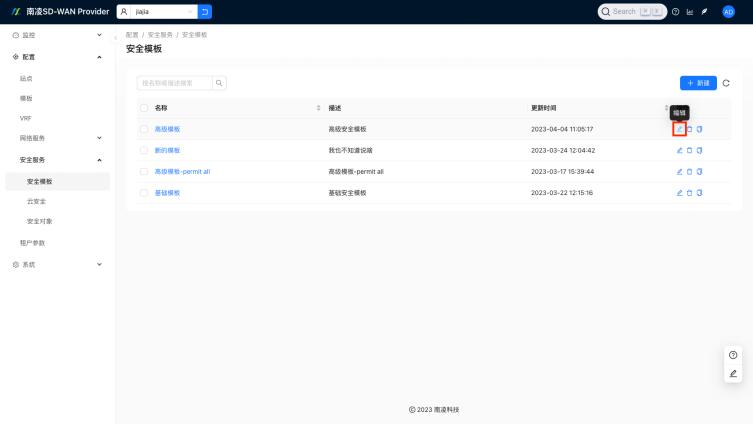
新建安全模板后会自动跳转至编辑安全模板页面， 同时也可自己点击进入编辑界面

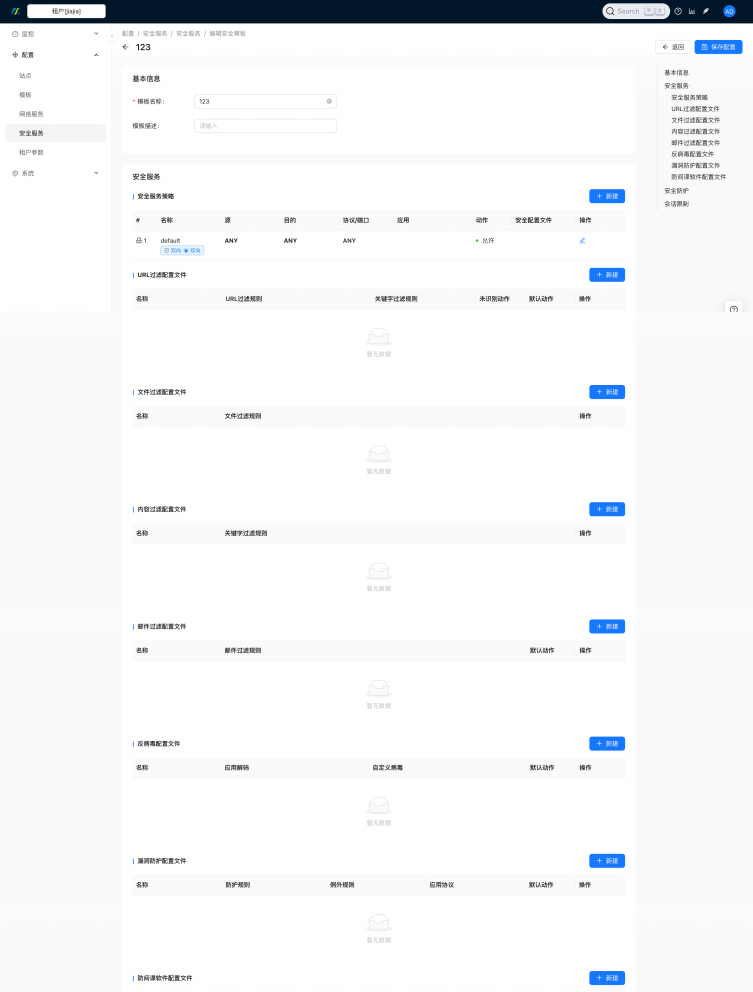
配置过程中的动作有3种：

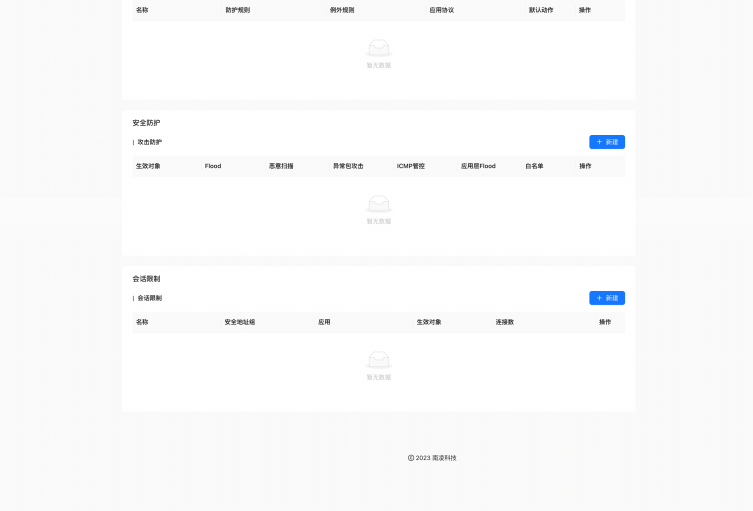
 允许：允许通过且不记录日志

 阻断：不允许通过且记录日志

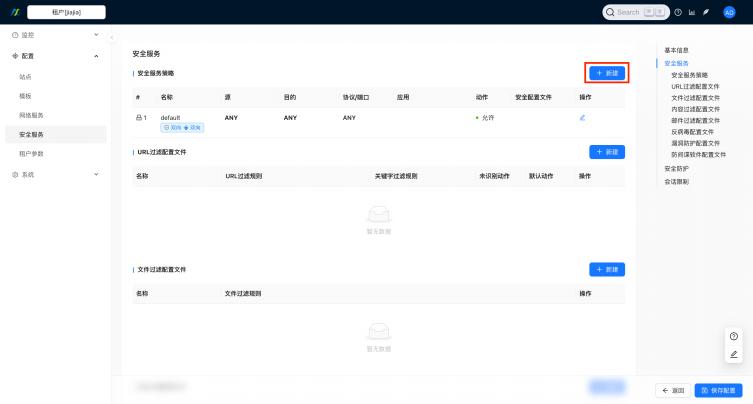
 日志：允许通过且记录日志



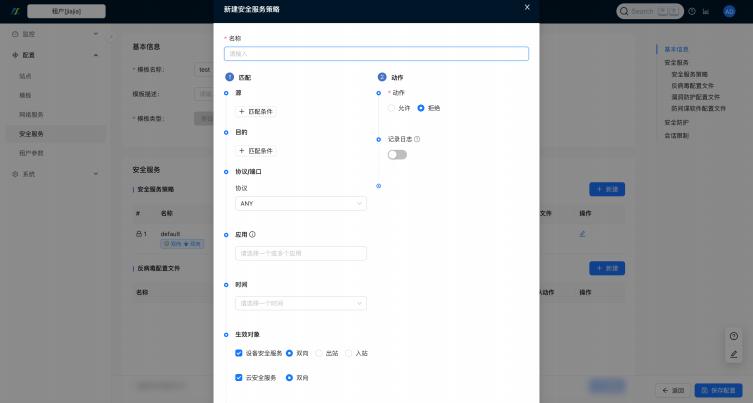




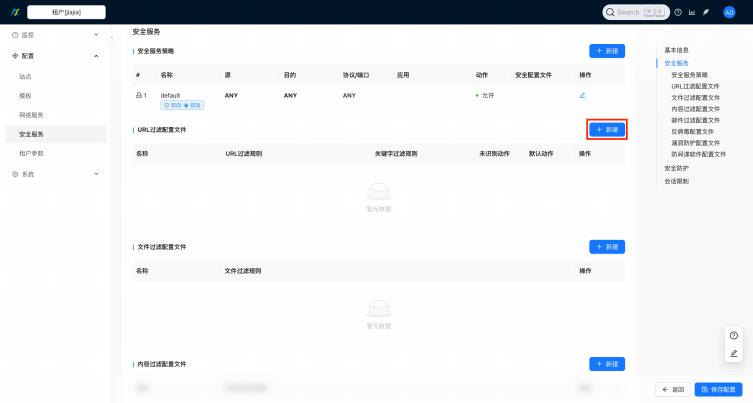
安全服务策略



记录日志若打开，则将匹配的规则以日志的形式记录下来

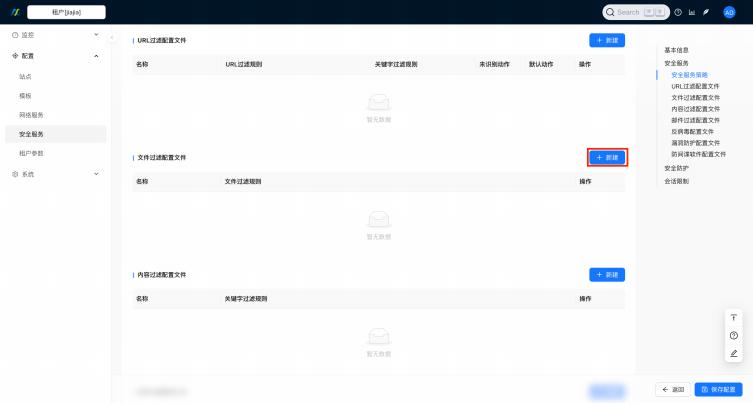


URL过滤配置文件



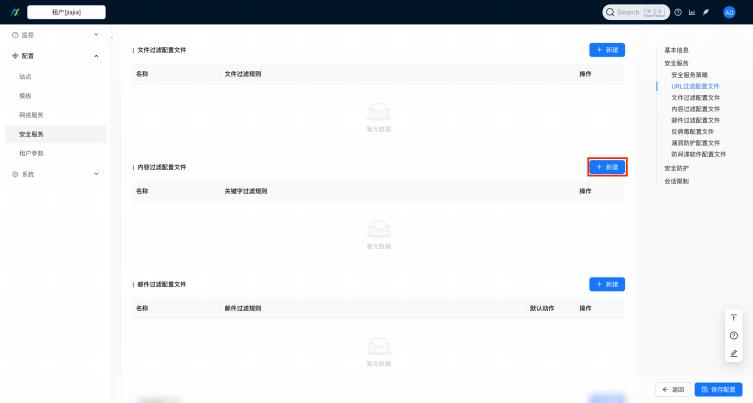


文件过滤配置文件





内容过滤配置文件





邮件过滤配置文件



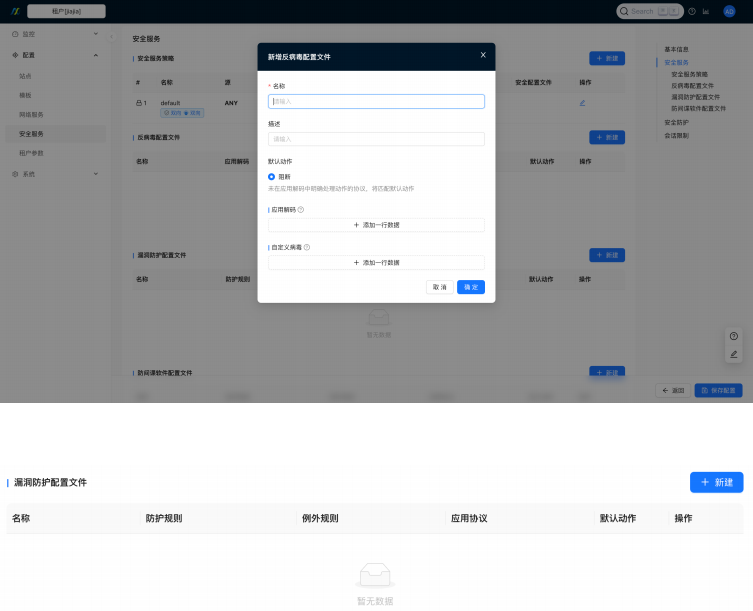


反病毒配置文件



应用解码：通过对 HTTP 、SMB 和 FTP 方式上传 、下载文件， 或 SMTP 、POP3 、IMAP 协议发送的 电子 邮件及其附件等进行病毒扫描， 并可以根据扫描结果进行相应的处理

自定义病毒：对 AV 病毒库的补充 。 自定义病毒的优先级高于病毒库中的优先级 。进行 AV 检测时， 先匹配自定义病毒



漏洞防护配置文件

例外规则：仅支持128条例外规则



防间谍软件配置文件





安全防护



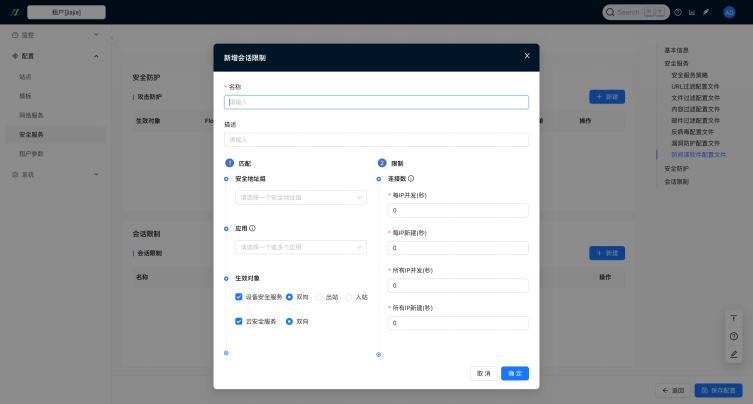
警戒值：0-50000包/秒， 0表示不开启



会话限制

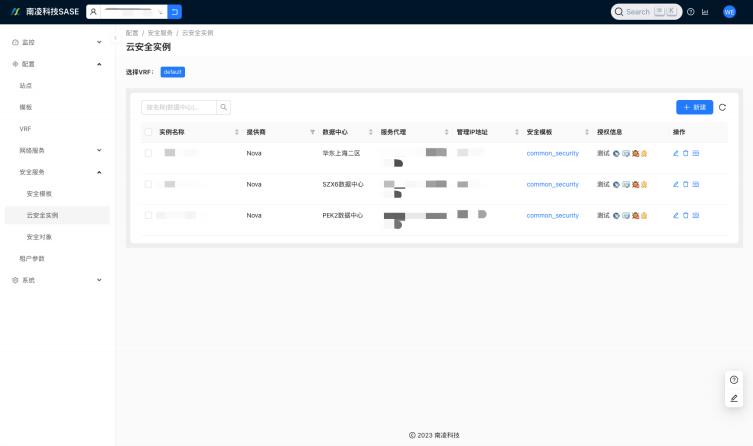


0-3000000， 0不表示限制， 默认不限制

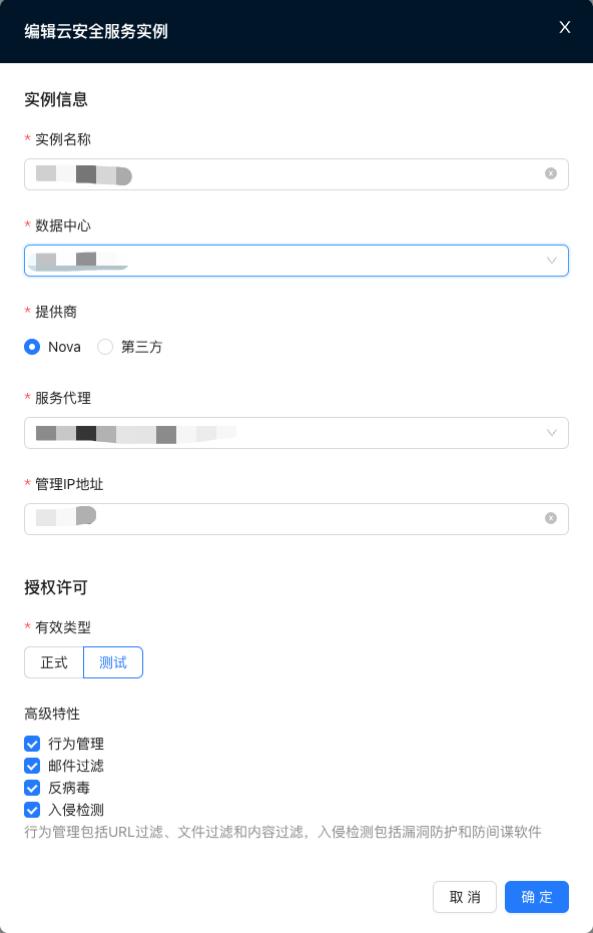


配置-安全服务-云安全实例

『租户』 →『配置』 →『安全服务』 →『云安全实例』 →『新建』 → 【新建云安全服务实例】



编辑云安全实例



关联安全模板

关联相应安全模板，启用安全服务 。安全模板需在『租户』 →『配置』 →『安全服务』 →『安全模

板』 中配置





配置-安全服务-安全对象

· 服务器连接技术

应用

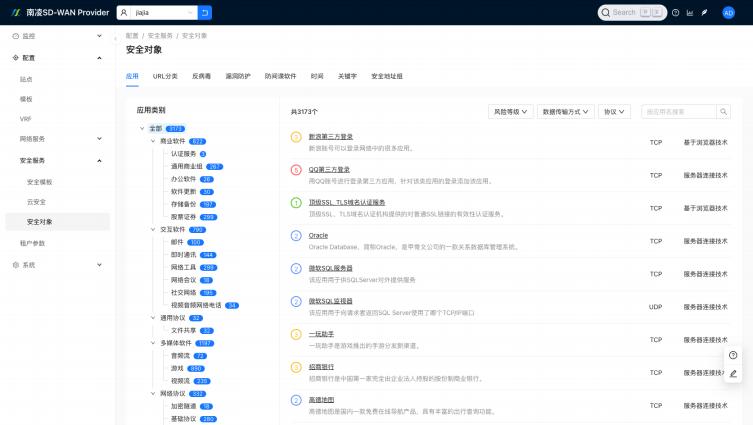
数据传输方式：

 基于浏览器技术

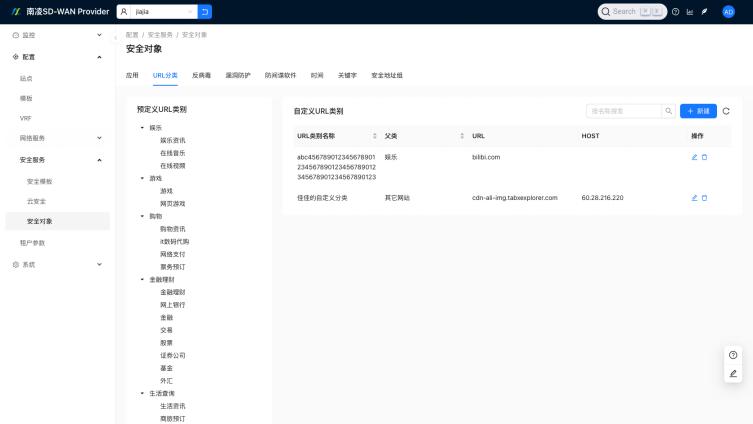
 P2P技术

 网络协议技术

可按应用名称搜索



URL分类



 INFO

URL中一行一条记录，每条记录不能超过127个字符， 可以加通配符\*代表任意字符串， 只能加在输 入内容的前面或者后面 。 例如：

 [www.example.com/example/example](http://www.example.com/example/example)

 [www.example.com](http://www.example.com/)

· www.example\*

· \*example.com

 192.168.0.1

 INFO

HOST中一行一条记录，每条记录不能超过63个字符， 可以加通配符\*代表任意字符串 。 例如：

 [www.example.com](http://www.example.com/)

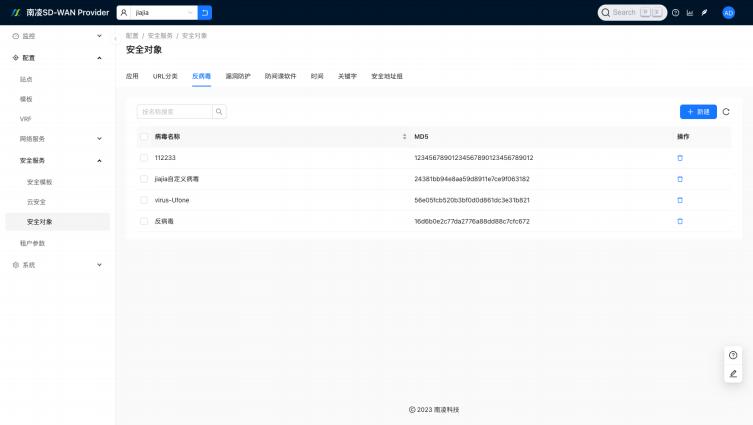
· www.example\*

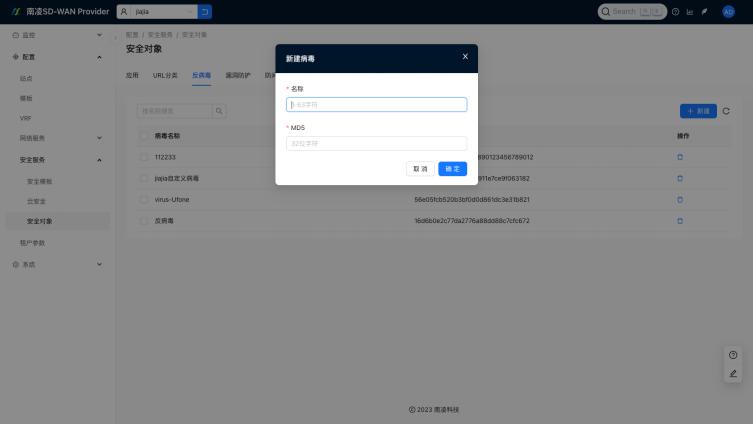
· \*example.com

 192.168.0.1

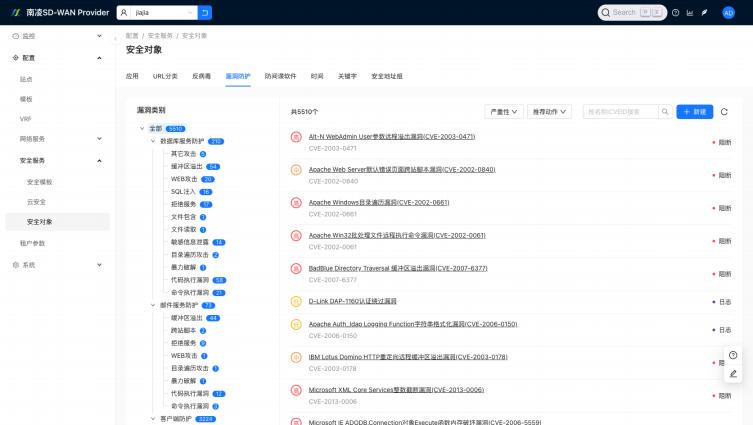


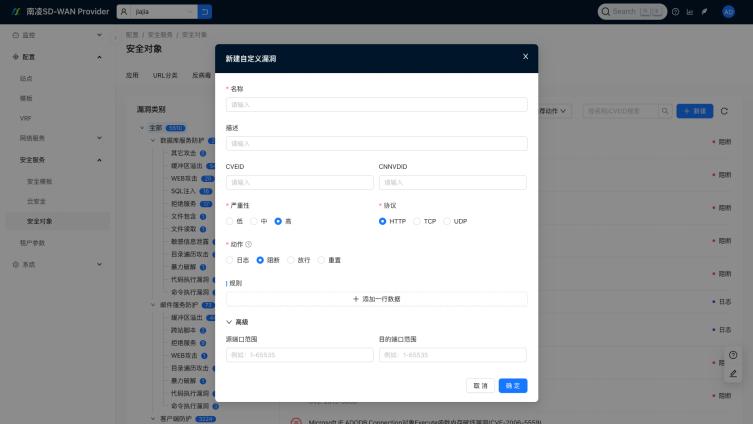
反病毒



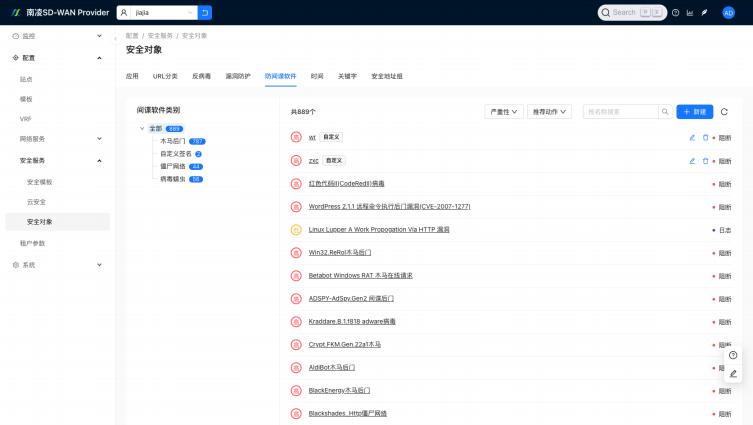


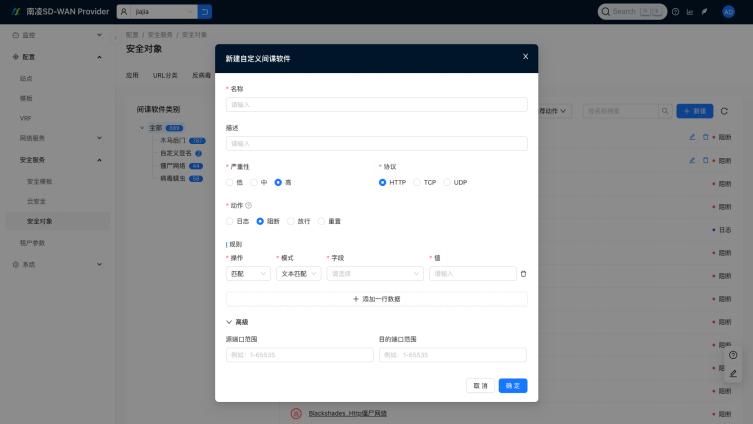
漏洞防护



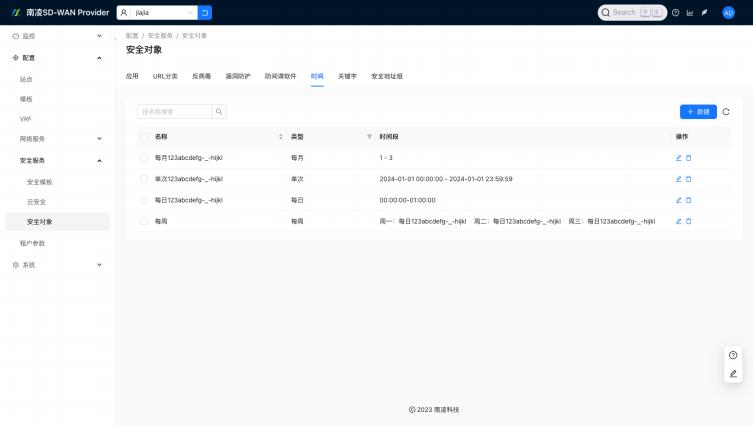


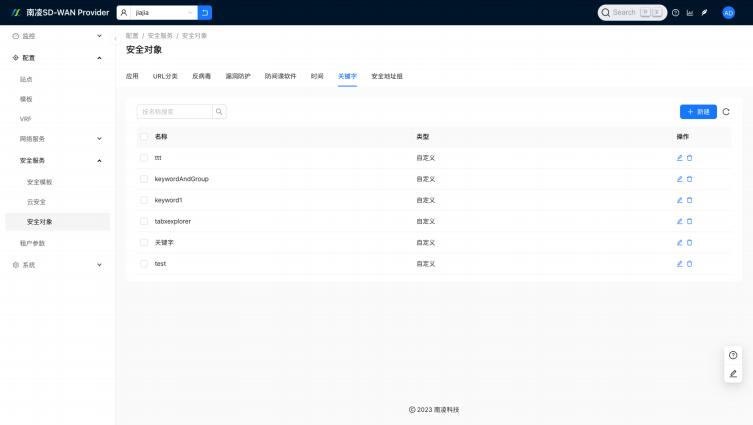
防间谍软件





时间



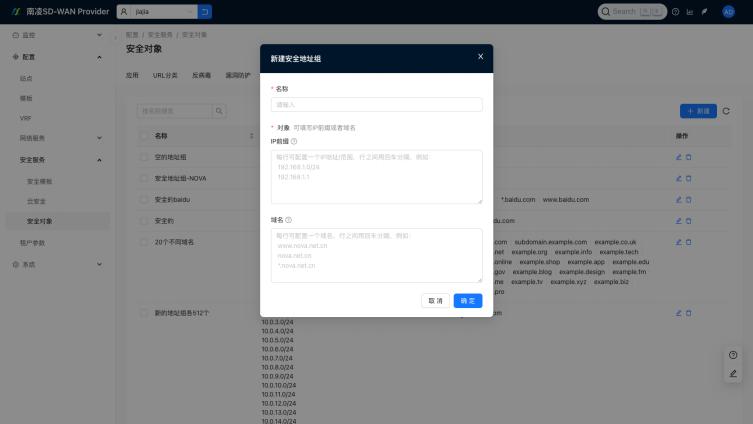
关键字

关键字匹配规则：最多32条匹配规则。

地址安全组

IP前缀不能超过512个

域名不能超过512个



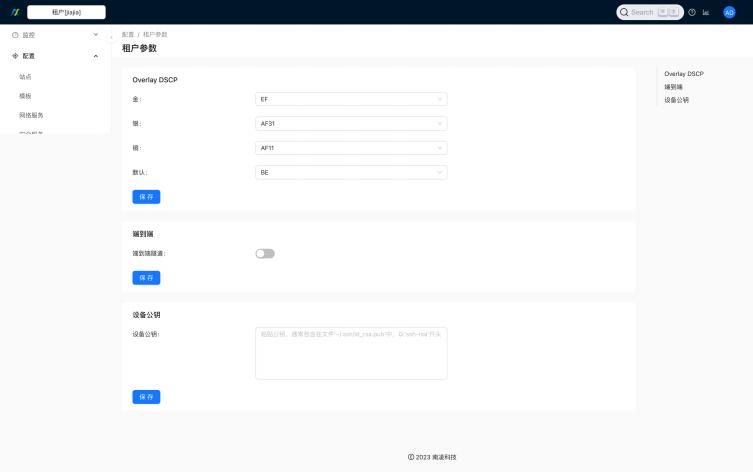
配置-租户参数

『租户』 →『配置』 →『租户参数』

Overlay DSCP：在租户级别给金 、银 、铜和默认设置对应的DSCP值

端到端：是否开启端到端隧道

设备公钥：用于身份验证 、加密解密等

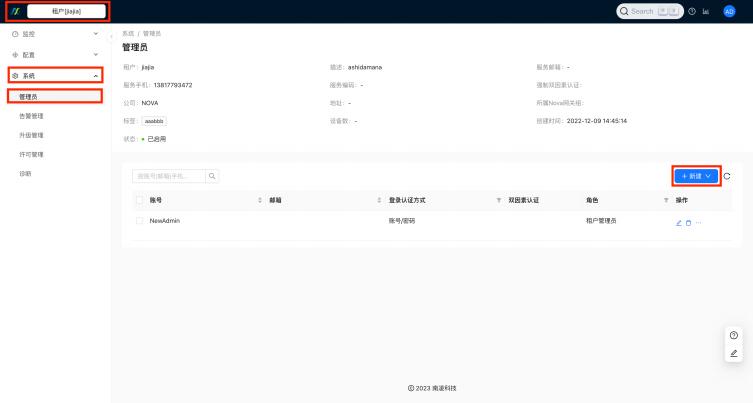


系统-用户

『租户』 →『系统』 →『管理员』 →『新建』 → 【新建租户管理员/新建租户站点管理员】

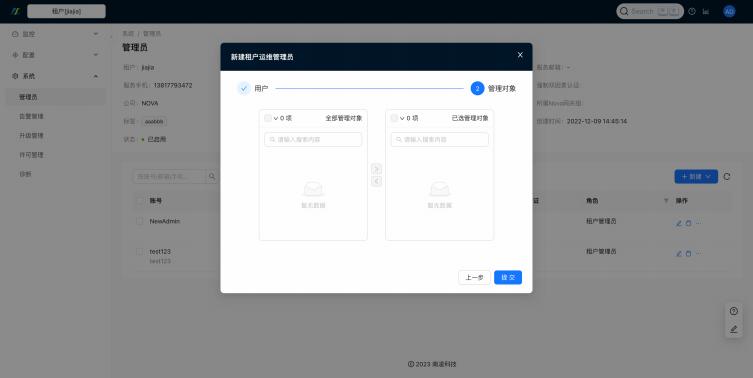
租户用户分租户管理员和租户站点管理员，租户管理员拥有该租户所有站点的只读权限，租户站点 管理员拥有部分站点的只读权限；

租户站点管理员通过标签识别可管理的站点，每个站点都可以配置标签， 把需要管理的站点与之关 联即可。









系统-告警管理

告警规则

『租户』 →『系统』 →『告警管理』 →『新建』 → 【新建告警规则】

告警管理页面如图1

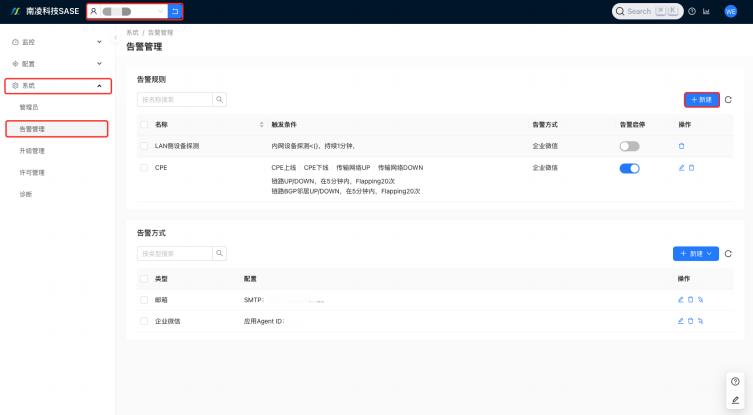
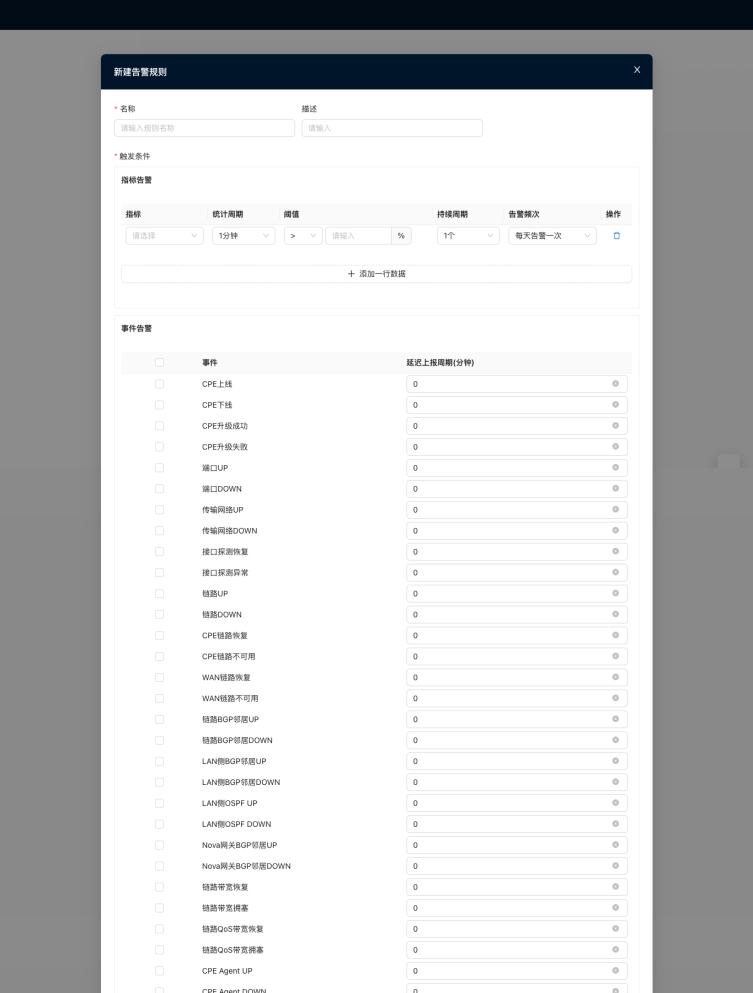


图1 告警管理页面图

新建告警规则

新建告警规则表单如图2



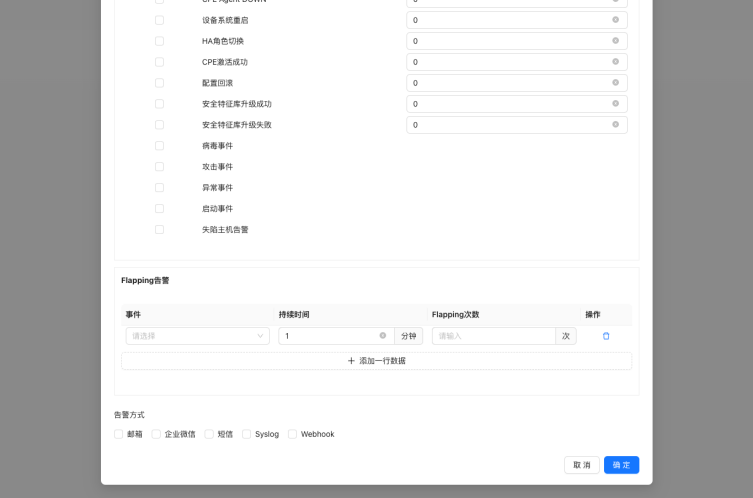


图2 新建告警规则表单图

其中指标可选择如下选项：

 CPE CPU

· CPE 硬盘

 CPE 温度

· CPE 内存

· VRF连接数

 安全服务CPU

 安全服务内存

 安全服务硬盘

告警频次可选择如下选项：

 每5分钟告警—次

 每10分钟告警—次

 每15分钟告警—次

 每30分钟告警一次

 每1小时告警一次

 每2小时告警一次

 每3小时告警一次

 每6小时告警一次

 每12小时告警一次

 每天告警一次

Flapping告警事件可选择如下选项：

· CPE上线/下线

· CPE升级成功/失败

· 端口UP/DOWN

· 传输网络UP/DOWN

· 接口探测恢复/异常

· 链路UP/DOWN

· 链路BGP邻居UP/DOWN

· LAN侧BGP邻居UP/DOWN

· LAN侧OSPF UP/DOWN

· Nova网关BGP邻居UP/DOWN

· 链路带宽恢复/拥塞

· 链路QoS带宽恢复/拥塞

· CPE Agent UP/DOWN

· 设备配置恢复/失败

· 安全特征库升级成功/失败

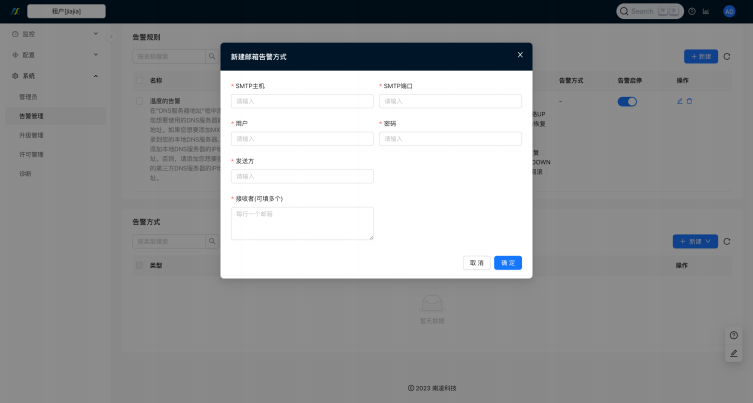
告警事件可在『租户』 →『监控』 →『告警』 → [事件]中查看

告警方式

『租户』 →『系统』 →『告警管理』 →『新建』 → [邮箱/短信/企业微信/Syslog/Webhook]

邮箱 短信 企业微信 Syslog Webhook





系统-升级管理

云安全实例升级管理 设备升级管理



『租户』 →『系统』 →『升级管理』

注意：此处升级管理为云安全实例升级管理，故前提是必须具备安全服务能力并安全服务状态是开启的



(手动)升级步骤：点击『实例名称』 → 『立即升级』

(自动)升级步骤：点击『启用自动升级』 → 填写『CRON表达式』 → 『保存』

安全服务开启步骤：在租户级别点击『配置』 →『站点』 →『更多』 →『授权许可』 →『启用安全许 可』 →

填写『可以应用的VRF数』 → 按需勾选『高级特性』并保存



系统-许可管理

注意：此处升级管理为云安全实例升级管理，故前提是必须具备安全服务能力并安全服务状态是开启的

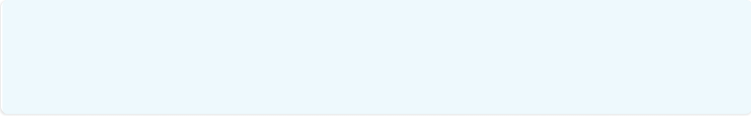


『租户』 →『系统』 →『许可管理』 ,根据『授权状态』看是否有安全服务许可。



系统-诊断

『租户』 →『系统』 →『诊断』



 INFO

管理员可以查看租户配置的站点对应的VRF路由和设备SN，根据路由信息来诊断VRF是否正常；也 可以根据租户配置的LAN侧IP来查询所属站点以及设备SN来诊断

