奇安信
新一代网络安全领军者

网神 SecGate 3600 防火墙
版本说明书 V1.0

网络安全服务热线：95015

公司网址：https://www.qianxin.com/

联系地址：北京市西城区西直门外南路 26 号院 1 号楼

邮编：100044

● 版权声明

目录

1 手册概述

1.1 手册简介

本手册是《网神 SecGate 3600 防火墙 版本说明书》，主要介绍网神 SecGate 3600 防火墙本版本的软件变更情况、硬件变更、已解决 bug。

1.2 适用产品

本手册适用于网神 SecGate 3600 防火墙产品。

与本文档相对应的产品版本如下所示。

产品名称	产品版本
网神 SecGate 3600 防火墙（非国产）	X86 平台：V3.6.6.0(-6.1.15. 170368) ARM913x 平台：V3.6.6.0(-6.91.15. 170368) ARM CN96 平台：V3.6.6.0(-6.90.15. 170368)
网神 SecGate 3600 防火墙（国产化）	X86（海光和兆芯）平台：V3.6.6.0(-60.1.15.170368) ARM（飞腾）平台：V3.6.6.0(-61.1.15. 170368)

1.3 读者对象

本文档主要适用于负责升级和部署防火墙的运维人员、配置和维护防火墙的管理员。帮助快速熟悉该版本的新变更。

1.4 配套手册

《网神 SecGate 3600 防火墙 V3.6.6.0 升级指导书》为用户提供升级指导。帮助用户选择升级版本、提供升级方法并提供升级失败时的处理方法。

《网神 SecGate 3600 防火墙 V3.6.6.0 快速上线部署手册》为首次安装、使用提供指导。同时列举管理产品的基本操作方法。

《网神 SecGate 3600 防火墙 V3.6.6.0 用户手册》为管理员提供功能说明和配置指导。

《网神 SecGate 3600 防火墙 V3.6.6.0 配置指南》以案例的形式为用户提供配置指导，并列举常见问题解决方法。

1.5 符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号名称	说明
 警告	以本标志开始的文本表示有潜在危险，如果不能避免，可能导致人员伤害。
 注意	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
 说明	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。
 窍门	以本标志开始的文本能帮助您解决某个问题或节省您的时间。

1.6 修订记录

修订记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 V1.0（发布日期 2023-12-20）

第一次正式发布。

2 版本配套说明

2.1 产品版本信息

2.1.1 国产化防火墙型号

产品名称	网神 SecGate3600 防火墙		
产品平台	X86 国产化平台	ARM 平台	
产品版本	61.1.15.170061	60.1.15.170061	
适用型号	NSG3300-1860-Z、 NSG3300-7620-H、 NSG3300-7660-H、 NSG3300-TA55、 NSG2300-ZX05、 NSG2300-ZX10、 NSG2300-ZX15、 NSG6300-HG15、 NSG6300-HG25、 NSG6300-HG35、 NSG3300-3660-H、 NSG4300-HG20、 NSG4300-HG25、 NSG6300-HG45、 NSG6300-HG55、 NSG6300-HG65、	NSG3300-1680-F、 NSG3300-1660-F、 NSG3300-1640-F、 NSG3300-2680-F、 NSG3300-3620-F、 NSG3300-3680-F、 NSG3300-5680-F、 NSG3300-5620-F、 NSG3300-5610-F、 NSG3300-7680-F、 NSG3300-TA15、 NSG3300-TA25、 NSG3300-TA35、 NSG3300-TA45、 NSG4300-FT05、 NSG4300-FT10、 NSG4300-FT15、 NSG6300-FT05、 NSG6300-FT15、 NSG6300-FT25、 NSG6300-FT35、 NSG6300-FT45	NSG3300-1240-F NSG3300-1220-F NSG3300-1260-F NSG2300-FT20

2.1.2 非国产化防火墙型号

产品名称	网神 SecGate3600 防火墙		
产品平台	X86 平台 NSG3000/4900/5000/5900/7000/8000/9000 系列和其他型号	CN96&92 平台 NSG6000 系列	913x 平台 NSG2000/4000 系列和其他型号
产品版本	6.1.15.170061	6.90.15.170061	6.91.15.170061

适用型号	● NSG3000 系列 NSG3000-TE45/ TE35/ TE25/ TE15 ● NSG4900 系列 NSG4900-TQ85/TG75/TG65/TQ55/TG45/TG35 ● NSG5000 系列 NSG5000-TG65/ TG55/TG45/TG35/ TG25/ TG15 ● NSG5900 系列 NSG5900-TQ35/TX25/TQ15 ● NSG7000 系列 NSG7000-TX65/ TX55 / TX45/ TX35/ TX25 / TX15 ● NSG8000 系列 NSG8000-TX25/ TX15/RT35 ● NSG9000 系列 NSG9000- TZ75/ TZ65/ TZ55/ TZ45/ TZ35/ TZ25/ TZ15 ● 其他型号 NSG-1060/1260/1460 ● NSG2700 系列 NSG2700-TG15/TG25/TG35/TG45/TZ25	NSG6000-TX45/ TX35/ TX25 /TX15 NSG2700-TX15/TX25/TX35	● NSG2000 系列 NSG2000-TE25/ TE35/ TE45 ● NSG4000 系列 NSG4000-TG15/ TG25/ TG35/ TG45 ● 其他型号 NSG-1280/1284/1680/1612

2.2 兼容性列表

2.2.1 对接设备兼容性

产品名称	功能说明	版本配套说明
SSL VPN&ZTNA 客户端	客户端到网关模块拨入； Win 客户端支持 windows7、windows10、windows11、WinServer 的 32 位及 64 位系统。 Linux 客户端（Linux 命令行客户端(仅支持 sslvpn 功能)）系统支持 Centos7.9 以上/Ubuntu21.04 以上。 安卓客户端支持 Android 6.0 及以上。 IOS 客户端：支持 IOS 9.0 及以上 MACOS 客户端：支持 macOS 10.15 及以上。	Win 客户端版本： V 1.0.0.121002 CentOS 版本： V1.1.1.65082 Ubuntu 版本： V1.1.2.65082 安卓客户端版本： V 1.3.0.101040 IOS 客户端版本： V 1.2.0.65052 MACOS 客户端版本： V 1.4.5.10017

产品名称	功能说明	版本配套说明
网神智慧管理分析系统	实现防火墙的集中监控、安全配置、日志分析等。	V3.6.6.0（-8.8.8.26955）
网神防火墙日志审计系统	实现防火墙日志审计等。	V3.6.6.0（-8.8.8.26955）
网神云镜	通过对防火墙安全数据分析，实现风险主机发现，安全态势、策略执行可视化等。	-
天眼	支持与天眼系统联动。天眼可以向防火墙下发域名、URL、恶意 IP 等处置策略。	V3.0.11.0
天眼文件威胁鉴定器	防火墙支持与天眼的文件威胁鉴定器（沙箱）联动进行文件威胁检测	V4.0.9.2
NGSOC	支持与 NGSOC 联动。防火墙支持发送日志给 NGSOC。NGSOC 可以向防火墙下发处置策略。	V4.10.2.
终端安全管理系统（组件名称为“天堤数据联动组件”）	防火墙与终端安全管理系统通过“终端_协同防护”功能进行联动。 终端安全管理系统向防火墙发送终端是否安装终端安全管理系统，以及风险评估等级，防火墙可根据终端情况进行安全策略控制。 防火墙能够基于终端主机进行下发病毒查杀任务。	V 10.7.0.2000 及以上
终端安全管理系统 NAC	防火墙与终端安全管理系统 NAC 通过“终端_协同防护”功能进行联动。实现对终端用户认证并向防火墙下发终端准出策略。	NACV7.0.3.3000

2.2.2 浏览器兼容性

Firefox125 及以上或 chrome120 及以上内核的浏览器。

2.3 支持升级的版本

2.3.1 国产化防火墙版本

2.3.1.1 升级路径说明

- X86 国产化平台产品支持从 61.1.12.92325、61.1.12.95967、

61.1.12.107130、61.1.13.120328、61.1.13.121609、61.1.13.126346、61.1.13.127573、61.1.13.128778、61.1.13.130676、61.1.13.130981、61.1.13.131323、61.1.13.133790、61.1.14.164443、61.1.14.165103、61.1.14.166049、61.1.14.167069、61.1.14.167095、61.1.14.167635、61.1.14.167803、61.1.14.167932、61.1.14.168298

升级到 61.1.15.170061。

- ARM 国产化飞腾平台产品支持从 60.1.12.89655、60.1.12.95864、60.1.12.98957、60.1.12.107821、60.1.12.109137、60.1.12.113020、60.1.12.114858、60.1.12.116024、60.1.12.118076、60.1.12.118155、60.1.13.120326、60.1.13.120396、60.1.13.121999、60.1.13.122248、60.1.13.123097、60.1.13.124251、60.1.13.124591、60.1.13.126118、60.1.13.126275、60.1.13.128778、60.1.13.130981、60.1.13.131323、60.1.13.133550、60.1.13.133790、60.1.14.164443、60.1.14.165108、60.1.14.166049、60.1.14.167069、60.1.14.167095、60.1.14.167635、60.1.14.167803、60.1.14.167932、60.1.14.168298

  升级到 60.1.15.170061。
- ARM 国产化 E2000 平台产品支持从 60.1.14.164692、60.1.14.165103、60.1.14.167045、60.1.14.167069 、60.1.14.167095、60.1.14.167635、60.1.14.167803、60.1.14.167932、60.1.14.168298

  升级到 60.1.15.170061。

说明

- 60.1.9.64578 版本必须先升级到 60.1.12.109137 版本，重启设备后再升级到 60.1.15.170061 版本。
- 61.1.9.69291 版本必须先升级到 61.1.12.107130 版本，重启设备后再升级到 60.1.15.170061 版本。
- 60.1.14.167045 版本后 ARM（E2000）国产化平台和 ARM 国产化平台归一，采用相同版本号，但后缀不同。

2.3.1.2 升级包选择

请选择与设备硬件相对应的软件升级包。

在升级到 6x.1.15.170061 时需要注意：

- 6x.1.12 及以后的版本可以直接升级到 6x.1.15 最新版本。
- 6x.1.9 的版本必须先升级到 6x.1.12 版本再升级到 6.1.15 最新版本。

说明

6x 代表 60（ARM 平台）或 61（X86 国产化平台）。

不同版本对应的升级包说明如下：

升级前版本	升级包
60.1.9	先升级 hw60.1.12.109137.ft.sign 再升级 hw60.1.15.170061.FT2000.sign
60.1.12、60.1.13、60.1.14	hw60.1.15.170061.FT2000.sign（包括 E2000 平台）
61.1.9	先升级 hw61.1.12.107130.sign 再升级 hw61.1.15.170061.X86.sign
61.1.12、61.1.13、61.1.14	hw61.1.15.170061.X86.sign

2.3.2 非国产化防火墙版本

2.3.2.1 升级路径说明

- X86 平台支持从 6.1.12.72317、6.1.12.84453、6.1.12.85868、6.1.12.92650、6.1.13.95963、6.1.13.101226、6.1.13.101713、6.1.13.103040、6.1.13.103377、6.1.13.103547、6.1.13.104063、6.1.13.104327、6.1.13.105116、6.1.13.105244、6.1.13.105949、6.1.13.106629、6.1.13.107345、6.1.13.107723、6.1.13.107831、6.1.13.108145、6.1.13.108212、6.1.13.108451、6.1.13.108691、6.1.13.108975、6.1.13.111514、6.1.13.111818、6.1.13.112993、6.1.13.113054、6.1.13.114173、6.1.13.115709、6.1.13.116533、6.1.13.117707、6.1.13.118055、6.1.13.118980、6.1.13.118180、6.1.13.119085、6.1.13.120151、6.1.13.150656、6.1.13.150857、6.1.13.150885、6.1.13.150963、6.1.13.150934、6.1.13.151389、6.1.13.151587、6.1.13.151638、6.1.13.152610、6.1.13.152414、6.1.13.152469、6.1.13.152851、6.1.13.153060、6.1.13.153187、6.1.13.153801、6.1.13.153857、6.1.13.153905、6.1.13.153937、6.1.13.154029、6.1.13.154042、6.1.13.154150、6.1.13.154210、6.1.13.154432、6.1.13.155089、6.1.13.155129、6.1.13.155154、6.1.13.155198、6.1.13.155312、6.1.13.156124、6.1.13.156158、6.1.13.156252、6.1.13.156479、6.1.13.156551、6.1.13.156595、6.1.13.156693、6.1.13.156898、6.1.13.157066、6.1.13.157155、6.1.13.157252、6.1.13.157282、6.1.13.157631、6.1.13.157790、6.1.13.158207、6.1.13.159197、6.1.13.159543、6.1.13.159835、

6.1.13.160925、6.1.13.161715、6.1.14.164546、6.1.14.165103、6.1.14.166049、6.1.14.166285、6.1.14.166935、6.1.14.167069、6.1.14.167095、6.1.14.167635、6.1.14.167803、6.1.14.167932、6.1.14.168298 版本升级到 6.1.15.170061。

●ARM 平台支持从 6.91.13.98086、 6.91.13.103588、6.91.13.104322、6.91.13.104327、 6.91.13.116907、6.91.13.117898、 6.91.13.150656、6.91.13.151131、 6.91.13.151389、 6.91.13.151638、 6.91.13.152469、6.91.13.152851、 6.91.13.153060、 6.91.13.153801、 6.91.13.153857、6.91.13.154150、 6.91.13.154361、 6.91.13.155198、 6.91.13.155312、6.91.13.156124、 6.91.13.156693、 6.91.13.156764、 6.91.13.156898、6.91.13.157066、 6.91.13.157586、 6.91.13.157631、 6.91.13.157790、6.91.13.159197、 6.91.13.159506、 6.91.13.159543、 6.91.13.159835、6.91.13.161715、 6.91.14.164546、 6.91.14.165103、 6.91.14.166049、6.91.14.166285、 6.91.14.166935、 6.91.14.167069、 6.91.14.167095、6.91.14.167635、 6.91.14.167803、 6.91.14.167932、 6.91.14.168298 版本升级到 6.91.15.170061。

- CN96 平台支持从 6.90.13.104327、 6.90.13.150656、6.90.13.151389、6.90.13.151638、6.90.13.152469、6.90.13.152851、6.90.13.153060、6.90.13.153801、6.90.13.153857、6.90.13.154150、6.90.13.155312、6.90.13.156124、6.90.13.156150、6.90.13.156693、6.90.13.156898、6.90.13.157066、6.90.13.157631、6.90.13.157790、6.90.13.159197、6.90.13.159543、6.90.13.159835、6.90.13.161715、6.90.14.164546、6.90.14.165103、6.90.14.166285、6.90.14.166935、6.90.14.167069、6.90.14.167095、6.90.14.167635、6.90.14.167803、6.90.14.167932、6.90.14.168298 版本升级到 6.90.15.170061

2.3.2.2 升级包选择

请选择与设备硬件相对应的软件升级包。

防火墙的升级包分为 sign 版本和 enc.sign 版本，在升级到 6.x.15.170061 时需要注意：

- 跨版本（6.1.12 之前版本）升级，首先选择某个版本的 enc.sign 版本进行升级，再升级到最新版本。

注意

- 如果 6.1.6、6.1.8 版本升级了不带 enc 的版本，会导致设备无法启动，需要使用串口才能修复。
- 如果 6.1.9、6.1.10、6.1.11 升级了不带 enc 的版本，上传版本失败，但是没有提示错误，会提示保存配置并重启，但是重启后还是原来的版本。

- 如果 6.1.12 版本升级了带 enc 的版本，会提示“升级包解签名失败”，升级失败。
- 6.1.12 之前的版本不推荐升级 6.X.15 版本

不同版本对应的升级包说明如下：

- 6.1.15.170061 对应的软件升级包为 hw6.1.15.170061.86.sign。
- 6.91.15.170061 对应的软件升级包为 hw6.91.15.170061.91.sign。
- 6.90.15.170061 对应的软件升级包为 hw6.90.15.170061.96.sign。

2.3.3 升级影响

说明

- 从 6x.xx.15 版本开始，流量编排功能开始受控于许可证授权，软件版本默认 30 天免费体验，到期之后原有配置不会被删除，用户无法新增、编辑流量编排配置且原有流量编排配置不生效。
- 6x.xx.15 的 IP-MAC 绑定默认开启 MAC 检查，之前的老版本升级到该版本后可能会导致一些流量在 MAC 检查时不通过，从而被丢弃，导致业务流量不通。
- 6x.xx.15 版本会话限制功能优化，旧配置会话限制方向为双向时，新的实现无法构成同样的效果，故升级乔治湖版本后旧配置丢失，需要手动重新配置。
- 由于蜜罐对象的引入导致旧版本的蜜罐策略、威胁引流都需要引用蜜罐对象，因此旧版本配置不兼容升级后蜜罐策略及威胁引流配置会丢失
- 富士山版本网关与 ADSL 或隧道接口同时配置的静态路由，升级至乔治湖版本后配置丢失
- 富士山及以前的版本引擎 ID 支持空格，乔治湖版本引擎 ID 增加空格字符限制，不允许输入空格

- 6x.xx.15 版本抓包工具与之前版本配置不兼容，升级之后，之前配置的抓包任务会被清空，需要重新配置。

  - 60.1.14.167045 版本后 ARM（E2000）国产化平台和 ARM 国产化平台归一，采用相同版本号，但后缀不同（一个 e2000 后缀，一个 ft2000 后缀）。60.1.15 版本 E2000 平台和飞腾平台再次归一，E2000 平台也采用.ft2000 后缀的发布包，因此从 14 版本升级到 15 版本时，需要选择 ft2000 后缀的发布包。

  - 6x.xx.14 版本日志存储架构发生了变化，老版本升级到该版本后可能会导致如下问题：

    - 根系统和虚拟子系统下 SSL 解密日志全丢。
    - 根系统下除操作日志和系统日志外的其他日志每种日志类型仅保留 1 万条，超出 1 万条则会丢失。虚拟子系统下除操作日志和系统日志外的其他日志每种日志类型仅仅保留 6000~1 万条，超出的日志则会丢失。说明：操作日志和系统日志不会丢失。
    - 因为日志丢失导致统计和分析中心分析结果不准确。

  - 6x.xx.1.14 后文件过滤和内容过滤支持的应用下删除了“中华论坛网”，若 6x.xx.13.版本的文件过滤或内容过滤中配置的应用中选中了“中华论坛网”，则升级到 6x.xx.14.版本后文件过滤或内容过滤相应的这条规则丢失。

  - 由于 6x.1.14.版本上功能增加，升级到新版本后 8G 内存的设备批量黑名单规格由 30 万调整为 10 万，4G 内存的设备批量黑名单规格由 30 万调整为 5 万。6x.xx.1.14 版本解决了威胁情报库同时受【云联防】页面下的代理服务器和【特征库升级】页面的代理服务器代理，从而造成代理服务器修改混乱的问题。6x.xx.1.13 之前的版本升级到 6.xx.1.14 版本，【云联防】页面下的代理服务器对威胁情报库升级不生效，威胁情报库仅使用【特征库升级】页面的代理服务器。

  - 6x.xx.1.14 版本日志服务器组描述信息对反斜杠（\）、英文双引号（”）、英文单引号（’）、尖括号（<>）等特殊字符进行了限制，导致之前的版本中若日志服务器组描述信息中包含以上特殊字符时升级到本版本会丢失相应的配置。

  - 6.xx.14 版本 X-Forwarded-For 黑名单过滤的功能开关在 WAF 下，之前的版本则在 URL 过滤下。若老版本的 URL 过滤下开启了 X-Forwarded-For 黑名单过滤则升级到 6.xx.14 版本后配置会丢失。

  - 6x.1.14 版本的管理员 Ukey 认证跟 6x.1.13 之前版本不兼容，会导致从上个版本升级到本版本后管理员 ukey 配置丢失，需要重新配置。6x.xx1.14 之前的版本升级到 6x.xx.1.14 版本后，web 认证的自定义背景图片的“启用”状态会默认修改为“禁用”。

  - 6.1.13.156124 之前的版本及 6x.1.14 版本以前的版本使用的 SSL VPN

客户端，无法在线升级到新版本防火墙采用的客户端。原因是新版本的协议支持为 tls1.2，而旧的客户端支持 tls1.0 或 tls1.1。若要对旧版本的 WIN 客户端进行升级，需要将 SSL VPN 配置中的算法强度修改为“中”，然后再进行在线升级。

- 6.1.13.155312 之前的版本升级到 6.1.13.156124 版本及以后版本，或 6x.1.13.版本及之前的版本升级到 6x.1.14 版本可能会存在管理主机无法管理设备的问题。原因是 155312 及以后版本保存配置信息时，针对空格的描述信息会增加英文双引号，而之前的版本针对空格的描述信息没有增加英文双引号；而管理主机的配置描述信息合地址由一条命令下发，因此会导致管理地址及描述信息同时丢失。

- 6.1.12.72317 之前的版本升级到 6.1.13 版本后，或 6x.1.13.版本及之前的版本升级到 6x.1.14 版本后，配置为 access vlan1 的接口，vlan1 相关配置会丢失。需要在升级后重新配置。

- 6.1.12.72317 及之前的版本升级到 6.1.13 版本后，或 6x.1.13.版本及之前的版本升级到 6x.1.14 版本后，聚合接口的负载算法置会被自动修改成“根据 IP 地址和 TCP/UDP 端口组合均衡”。需要在升级后修改为实际使用的算法。

- 6x.1.13.版本及之前的版本，引用了预定义服务 THUNDER 的策略配置在升级后可能会丢失。

- 6.1.12.72317 之前的版本升级到 6.1.13 版本后，短信网关地址升级为“sdk3.028lk.com”，会产生短信告警配置丢失、功能不可用等问题。需要在升级后重新配置。

- 6.1.12.72317 之前的版本升级到 6.1.13 版本后，DNS 代理配置将会被清空。

- 6.1.12.72317 之前的版本升级到 6.1.13 版本后，RA 功能的最小时间间隔、最大时间间隔、路由生命周期参数自动恢复到缺省值。

- 6.1.12.72317 之前的版本升级到 6.1.13 版本后，电源故障时日志告警的功能。由于老的设备中缺少电源信号检测 ttl 线，导致系统误以为电源故障，会有“电源状态异常”的系统日志。

- 6.1.12 及之前的版本升级到 6.1.13 版本后，或 6x.1.13.版本及之前的版本升级到 6X.1.14 版本后，部分特征库会变为默认库。

- 6.1.12 及之前的版本升级到 6.1.13 版本后，或 6x.1.14 之前的版本升级到 6x.1.14 版本后，DHCP 服务器或中继接口配置可能会丢失。

  6.1.12 及之前的版本或 6x.1.13.版本及之前的版本，DHCPv4 客户端、服务器和中继可以共用 1 个接口，升级到 6.1.13 版本或 6x.1.14 版本后，三者不再允许共用接口。

  - DHCP 客户端优先级高于 DHCP 服务器和 DHCP 中继，若接口同

时开启 DHCP 客户端和 DHCP 服务器或 DHCP 中继，升级后，仅 DHCP 客户端配置生效，DHCP 服务器和 DHCP 中继的接口的配置会丢失。

- DHCP 服务器优先级高于 DHCP 中继，若接口开启了 DHCP 服务器和 DHCP 中继，升级后，仅作为 DHCP 服务器接口。DHCP 中继的接口的配置会丢失。

- 6.1.12 及之前的版本升级到 6.1.13 版本后，或 6x.1.14 之前的版本升级到 6x.1.14 版本后，描述信息可能会丢失。

2.4 可获得性说明

访问奇安信官网下载中心（https://download.qianxin.com/），使用个人账户登录后，即可获取目标版本。

6.1.15 版本从老版本升级可能需要跨版本升级，跨版本升级需要同时下载 enc 版本和目标版本。

说明

若访问下载中心时无法看到版本文件，请检查是否已经登录，或联系管理员确认个人账户权限是否正确。

3 版本更新说明

3.1 设备管理

3.1.1 页面命令行

使用 TLS1.3，页面命令行优化后重新上线，默认不开启，需要 CLI 下启用该功能。

3.1.2 NTP

NTP 的变更包括：

1、 支持使用 Web 页面配置通告管理口进行 NTP 时钟同步。以前仅支持命令行配置。

2、 支持配置同步模式。新增“立即同步”，之前仅支持“平滑同步”。

3.1.3 管理账号

选择【系统配置】>【设备管理】>【管理账号】，添加或编辑管理员时，变更如下：

认证类型新增“本地/远程”。可同时配置认证服务器和密码。优先进行远程认证，当无法进行远程认证时，采用本地用户名、密码认证。

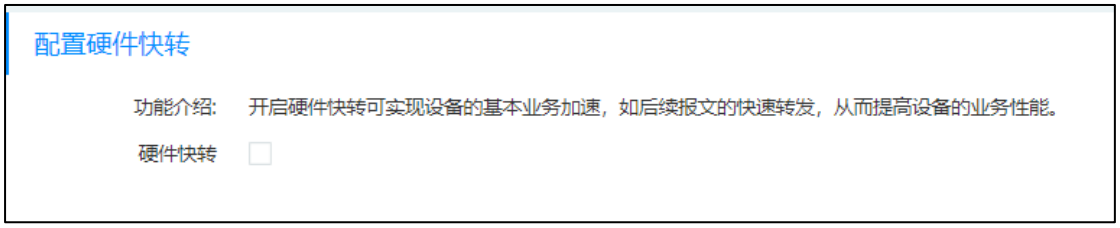
- 新增支持设置在线连接数。默认超出在线连接数后，使用该管理员账号无法上线。

3.1.4 登录设置

选择【系统配置】>【设备管理】>【登录设置】，新增设置在线管理员数。该参数为全局参数，对全部管理员账号生效。超出设置值后管理员无法上线。

3.1.5 硬件快转

选择【系统配置】>【设备管理】新增【硬件快转】页面。仅 NSG8000-RT35 型号支持硬件快转功能。



3.1.6 高级配置

选择【系统配置】>【设备管理】>【高级配置】，页面新增【QoS 监管】开关。

大流量情况下需要开启 QoS 监管功能。开启后针对大流量可以提高 QoS 准确性和处理性能。

3.2 高可用性

3.2.1 HA 设置

新增支持配置是否同步接口别名。仅命令行支持。

3.3 配置文件

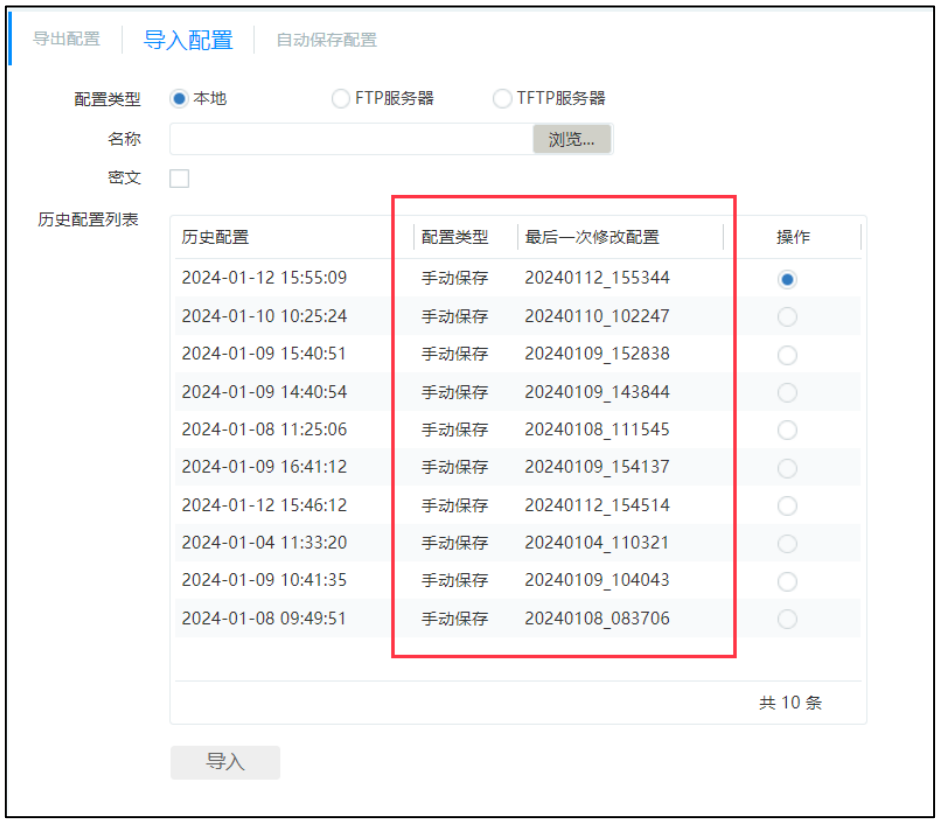
3.3.1 自动保存配置

选择【系统配置】>【配置文件】，新增【自动保存配置】页面。

自动保存配置默认关闭，可修改自动配置时间间隔。

3.3.2 导入配置

选择【系统配置】>【配置文件】>【导入配置】。20 历史配置（手工保存配置 10 个，自动保存配置 10 个）列表中新增显示配置类型和配置文件名称。



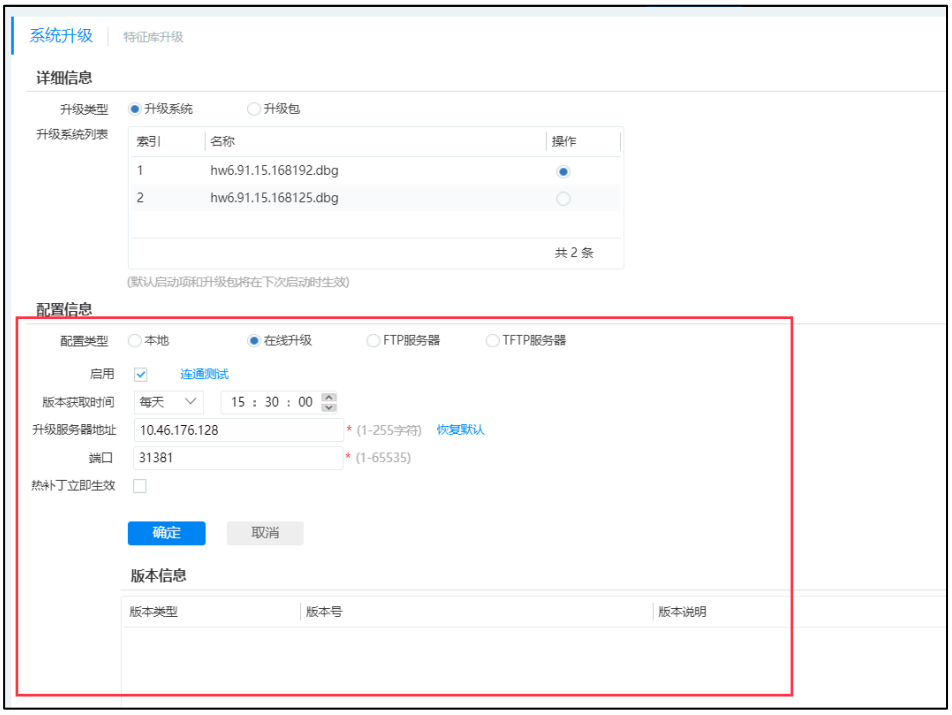
3.4 SNMP

SNMPv3 用户的密码支持括号字符。

新增 SNMP mib 节点: 42 支持读取接口描述（别名）和 43 支持读取光接口模块功率信息。

3.5 升级管理

新增支持自动在线升级功能。



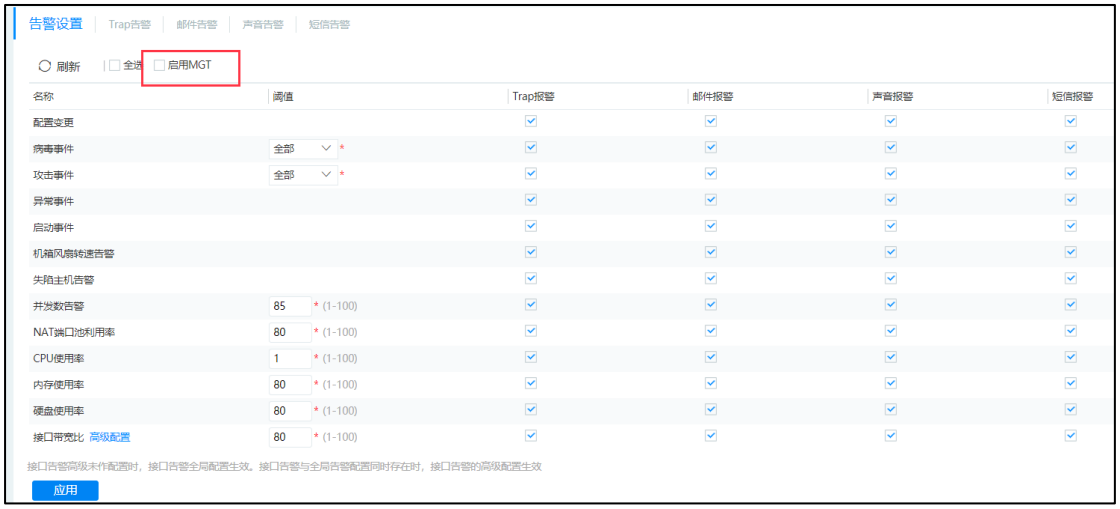
升级系统识别防火墙设备平台信息、CPU 核数、存储大小、内存大小、版本号等信息来判断当前版本是否可升级。如果可升级，升级系统自动推送可升级的最新版本信息。

防火墙会提示管理员是否进行升级，升级过程跟手动上传后升级过程一样，升级完成后，也需要重启设备后版本才会生效。

3.6 告警管理

3.6.1 告警设置

新增支持 web 页面设置通过 MGT 口告警管理。

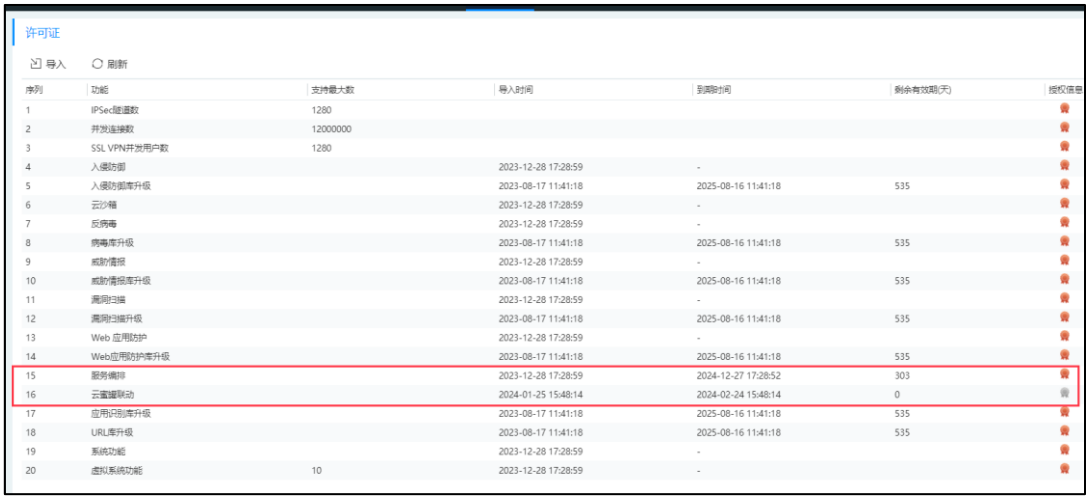


3.6.2 邮件告警

SMTP 服务器地址支持配置 IPv6 地址或域名解析为 IPv6 地址。

3.7 许可证

选择【系统配置】>【许可证】。新增“服务编排”和“云蜜罐联动”许可，分别对流量编排和云蜜罐功能在有效期内进行授权。

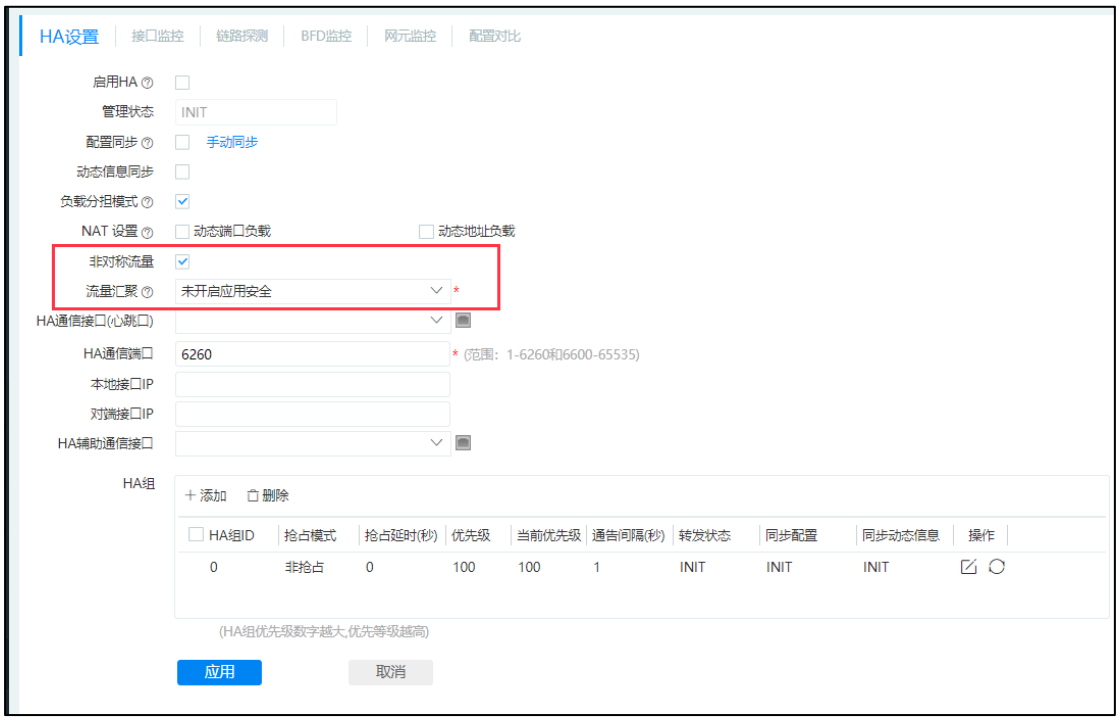


3.8 高可用性

选择【系统配置】>【高可用性】。原负载分担模式下的“增强功能”删除。

新增【非对称流量】开关。当防火墙做 HA 路由双主或者透明双主的情况下，如果存在来回流量不一致的场景，开启【非对称流量】功能，能使同一会话的流量汇聚到同一台防火墙设备（主 FW 或备 FW）进行安全检测。

流量汇聚支持 4 种模式，分别是未开启应用安全、应用安全无状态汇聚、应用安全无状态汇聚路径保持和应用安全有状态汇聚。未开启应用安全和无状态分流，简化了原来非对称环境流量分发机制。



3.9 产品联动

选择【系统配置】>【协同防护】>【产品联动】

3.9.1 态势感知协同防护

新增态势感知协同防护，防火墙支持和态势感知平台联动，响应态势感知平台的处置策略，实现威胁的拦截和防护。用户可以在态势感知平台上对网络流量进行分析，并对威胁进行处置。防火墙支持响应态势感知的处置策略，对威胁进行阻拦和防护。

3.9.2 IDP 协同防护

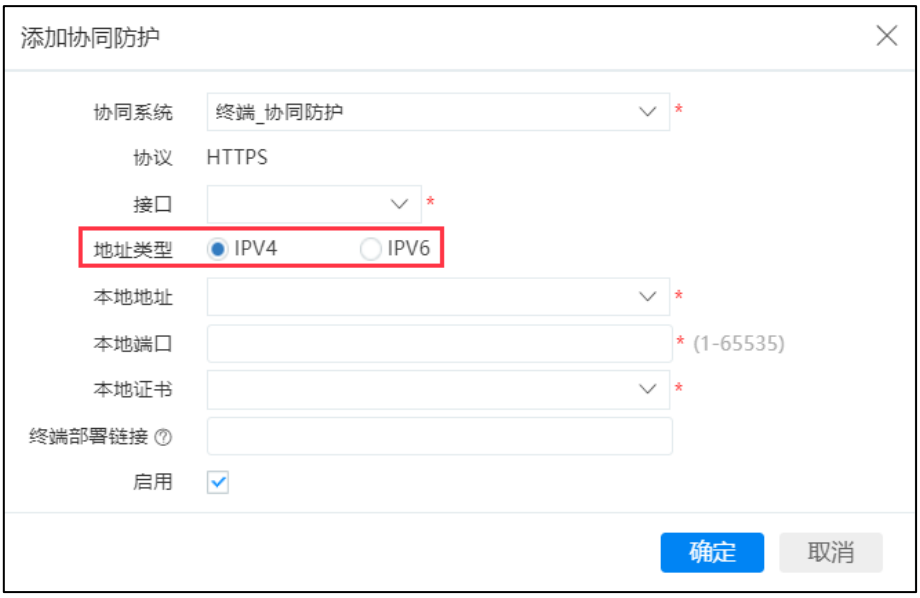
IDP 协同防护新增支持 IPV6 地址类型。

接口新增支持管理口、VLAN 接口、聚合接口、桥接口。

3.9.3 终端协同防护

终端协同防护新增支持 IPV6 地址类型。

接口新增支持管理口、VLAN 接口、聚合接口、桥接口。



3.9.4 NGSOC 协同防护

NGSOC 协同防护新增支持 IPV6 地址类型。

接口新增支持管理口、VLAN 接口、聚合接口、桥接口。

3.9.5 天眼云蜜罐

新增天眼云蜜罐联动。

3.9.6 天眼协同防护

天眼协同防护新增支持 IPV6 地址类型。

接口新增支持管理口、VLAN 接口、聚合接口、桥接口。

3.9.7 终端联动全盘扫描

新增终端联动全盘扫描。

3.10 云联防

3.10.1 威胁情报

选择【系统配置】>【协同防护】>【云联防】。【威胁云情报平台】区域框下新增支持威胁情报白名单，威胁情报白名单仅是针对威胁情报功能生效的白名单。加入威胁情报白名单的地址对应流量不进行威胁情报检测。

3.11 虚拟系统

选择【系统配置】>【虚拟系统】。虚拟系统可分配的资源增加“IPSec 隧道数”、“SSLVPN 隧道数”和“用户数”。

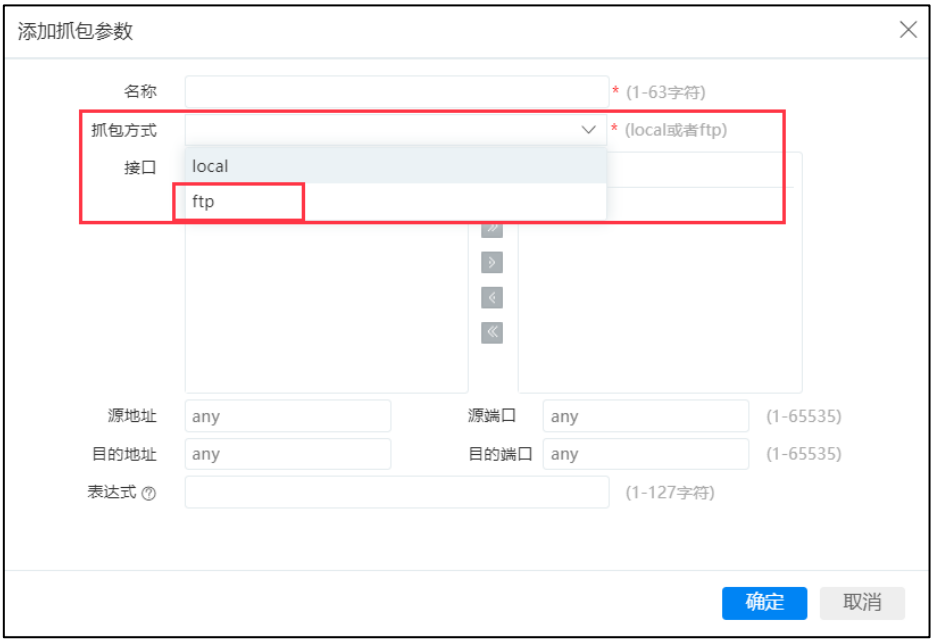
3.12 诊断工具

3.12.1 抓包工具

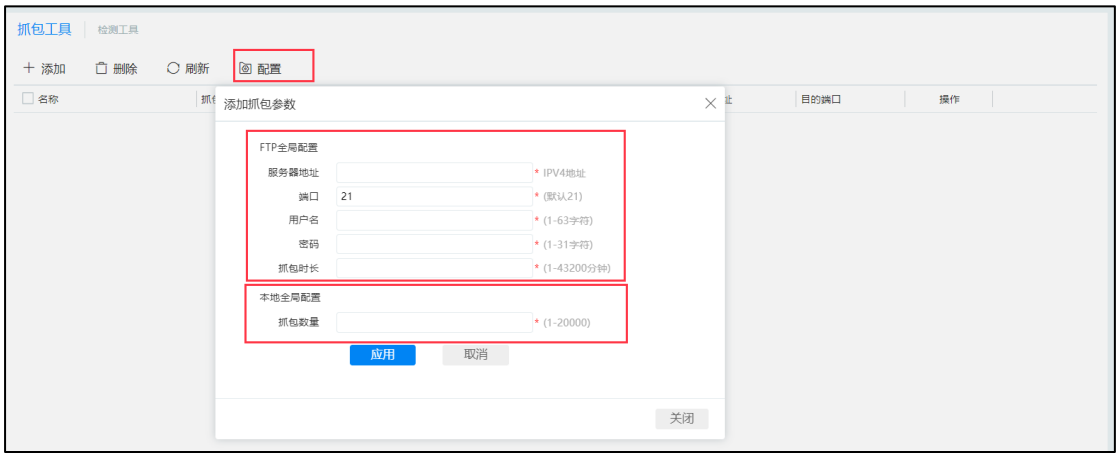
选择【系统配置】>【诊断工具】>【抓包工具】。抓包工具变更如下：

- 新增 FTP 方式

  FTP 方式下抓包文件上传到 FTP 服务器。



- 增加【配置】按钮。支持 FTP 全局配置和本地全局配置。



- 本地抓包数量上限增大至 20000。

3.12.2 报文示踪

选择【系统配置】>【诊断工具】，新增【报文示踪】功能。

- 支持模拟报文处理流程跟踪功能，使用模拟报文转发流程命令查看模拟构造的报文应经过的处理流程。

- 支持真实报文处理流程跟踪功能，可以在防火墙上看到指定访问的报文处理流程。

3.13 协议识别

3.13.1 新增 DNS over HTTPS 协议解析

新增 DNS over HTTPS（简称 DoH）协议的识别和解析，并支持 DOH 解析后匹配域名黑白名单、静态 DNS、域名被动学习、DNS 过滤和 IPS 过滤。

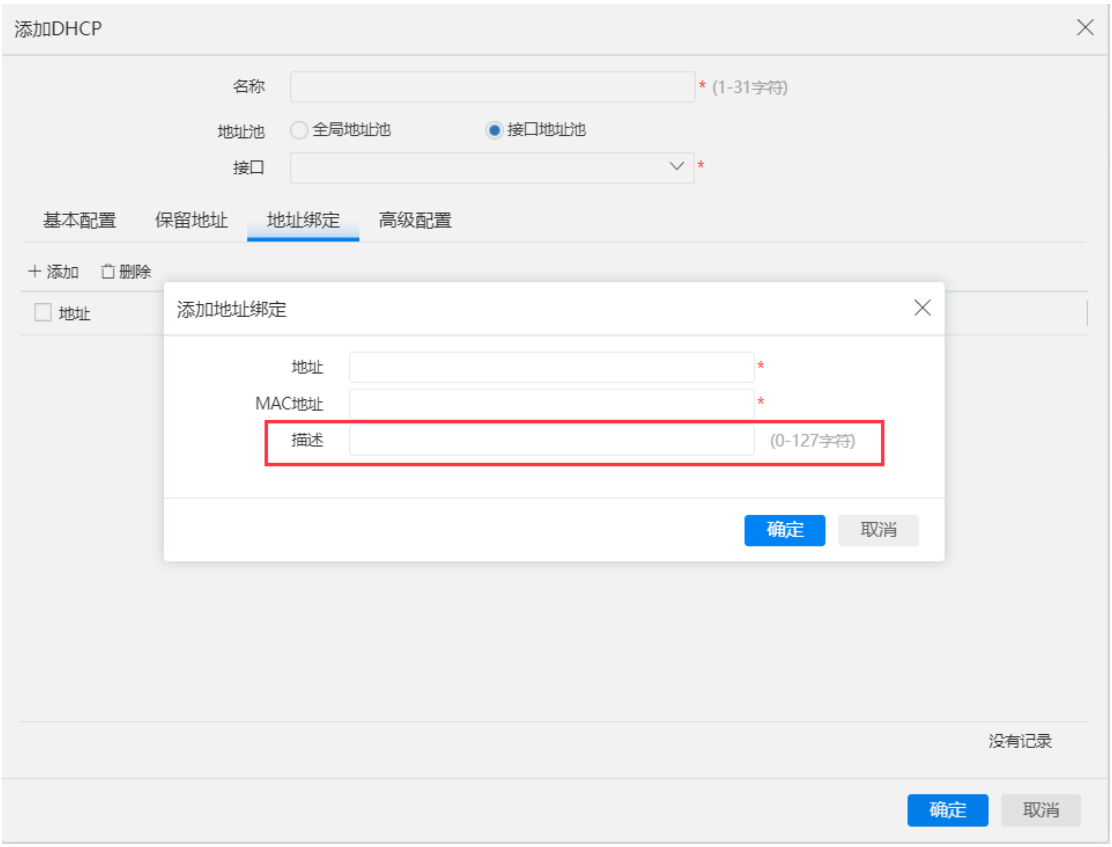
3.13.2 新增 DCERPC 协议解析

新增支持 DCERPC 协议识别和解析，能实现对 DCERPC 报文的 IPS 检测功能。

3.14 DHCP

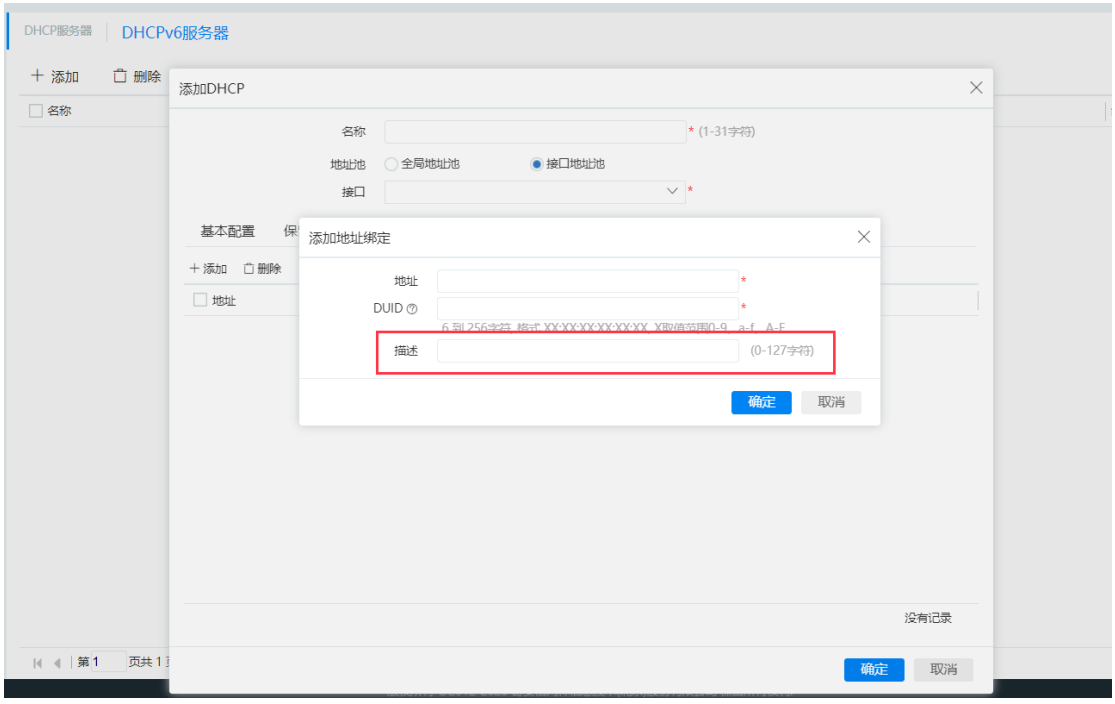
3.14.1 DHCP 服务器

选择【网络配置】>【DHCP】>【DHCP 服务器】。地址绑定下新增【描述】参数。



3.14.2 DHCPv6 服务器

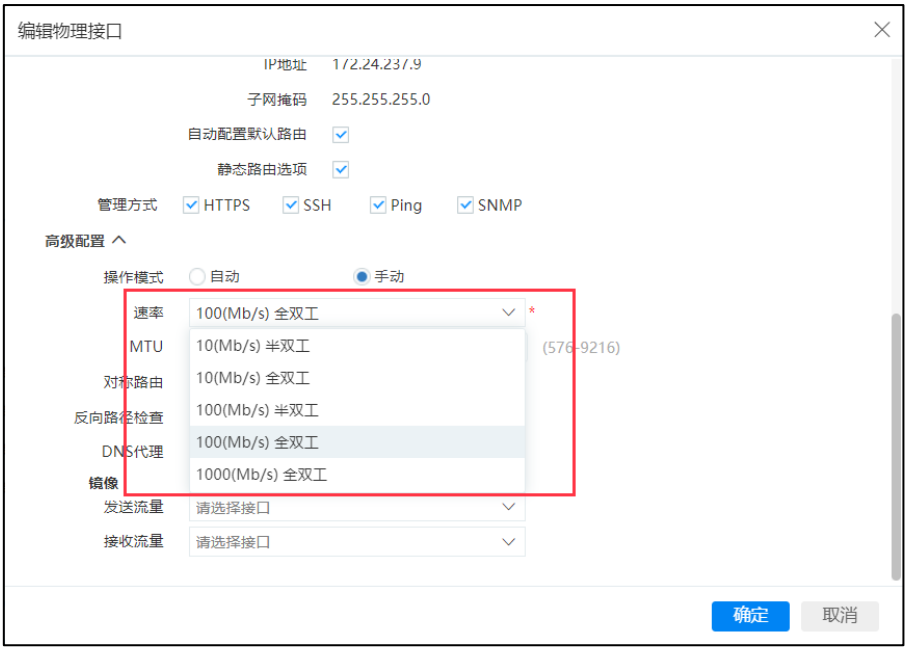
选择【网络配置】>【DHCP】>【DHCPv6 服务器】。地址绑定下新增【描述】参数。



3.15 接口

3.15.1 接口速率

手动设置速率改为下拉菜单形式，可以选择速率和模式。



3.15.2 聚合接口

聚合接口的聚合方式“热备方式”修改为“热备/冗余方式”。

“热备/冗余方式”下监控模式删除支持“ARP 探测”方式，仅支持“Link”。

3.15.3 Ping

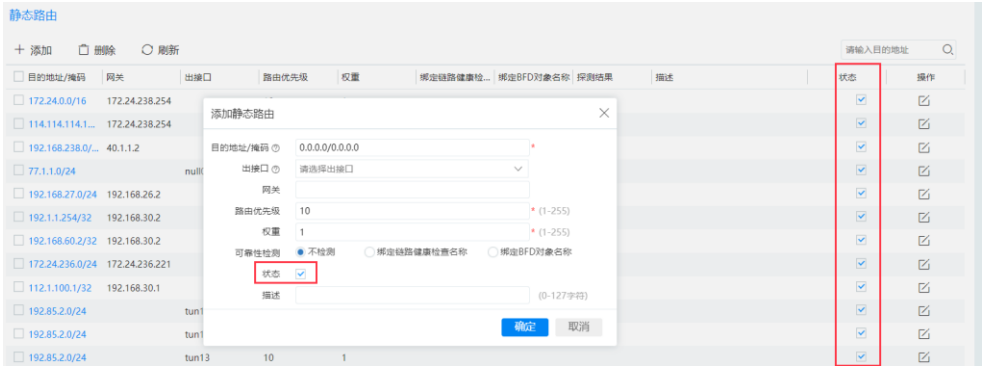
vlan 接口、桥接口、隧道接口、聚合接口支持 all-ping 功能。

3.16 路由

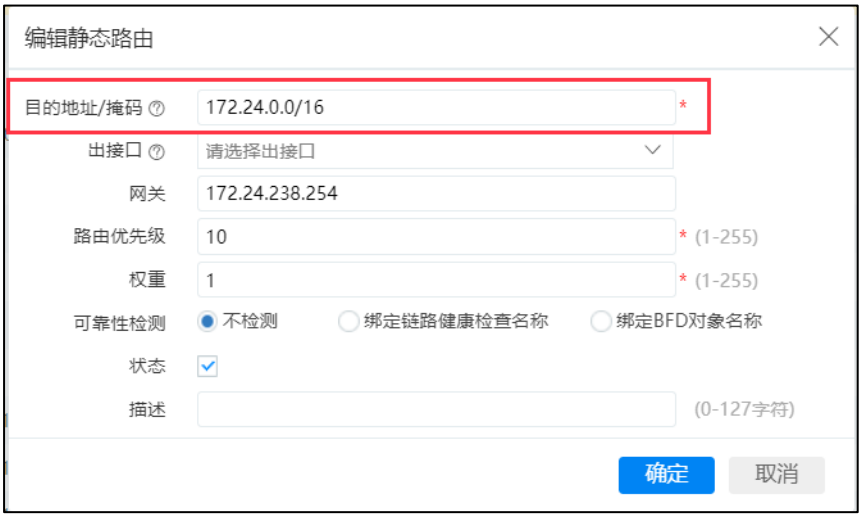
3.16.1 静态路由

选择【网络配置】>【路由】>【静态路由】。

- 新增支持配置静态路由的状态。默认状态为开启。



- 支持编辑静态路由的目的地址和掩码参数。



3.16.2 策略路由

3.16.2.1 支持默认策略路由

选择【网络配置】>【路由】>【策略路由】。策略路由分为策略路由和默认策略路由，默认策略路由的配置跟策略路由的配置参数一致，但优先级低。

3.16.2.2 支持基于目的区域选路

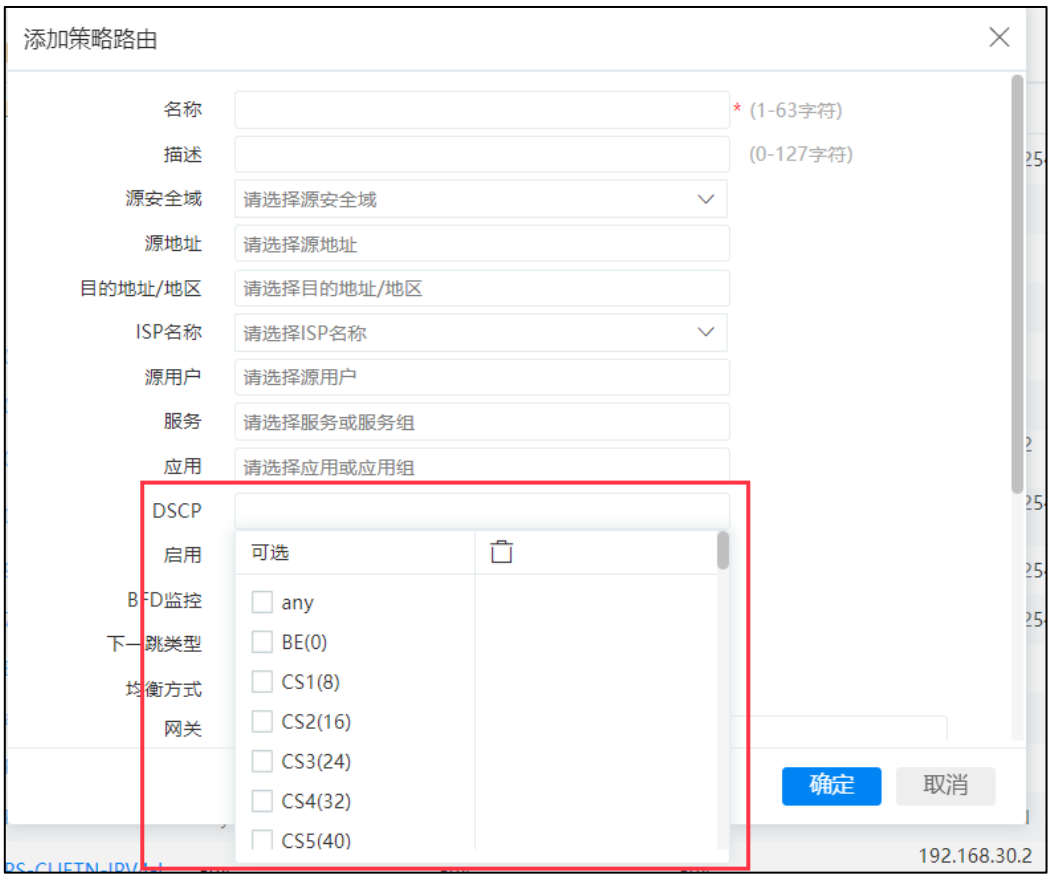
选择【网络配置】>【路由】>【策略路由】。

新增支持基于目的区域进行选路。

3.16.2.3 支持基于 DSCP 选路

选择【网络配置】>【路由】>【策略路由】。

新增支持基于 DSCP 进行选路。



3.16.3 OSPF

3.16.3.1 OSPF 路由重发布支持 tag

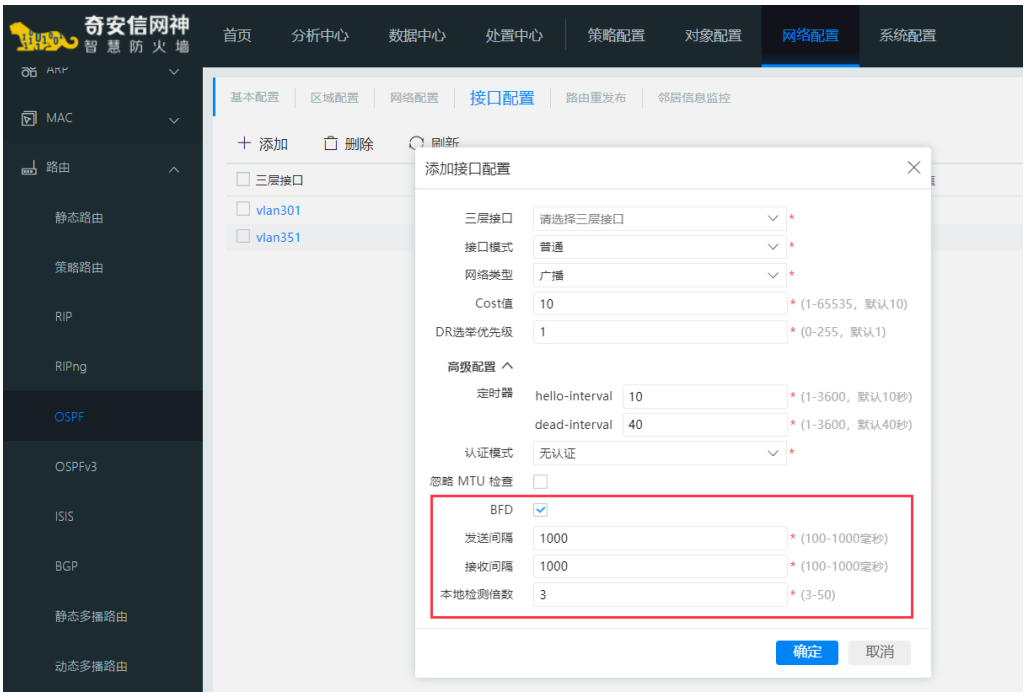
通过给 OSPF 路由在路由重发布时支持添加 tag 标签，可以支持在路由策略里进行标记过滤。

选择【网络配置】>【路由】>【OSPF】,【基本配置】页面新增支持路由重发布 Tag 缺省值。

单击【路由重发布】页签，添加或编辑路由重发布页面新增支持 Tag。此处配置的 tag 优先级高于 tag 缺省值。

3.16.3.2 OSPF 与 BFD 联动

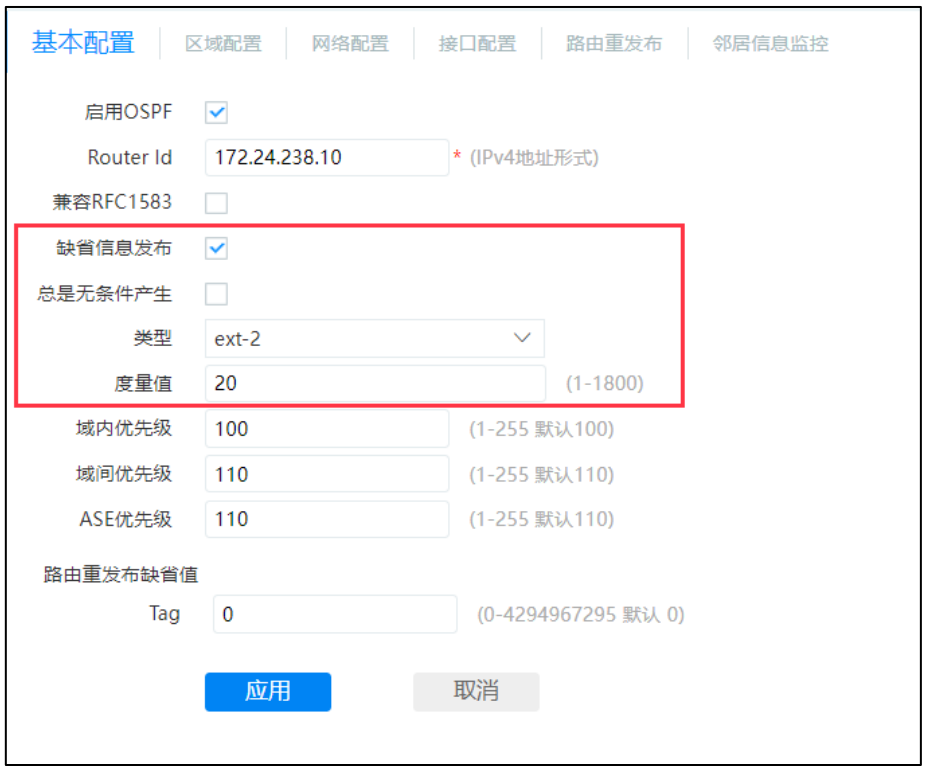
新增 OSPF 与 BFD 联动，可以实现 OSPF 路由快速收敛，收敛速度由秒级变为毫秒级。



3.16.4 OSPFv3

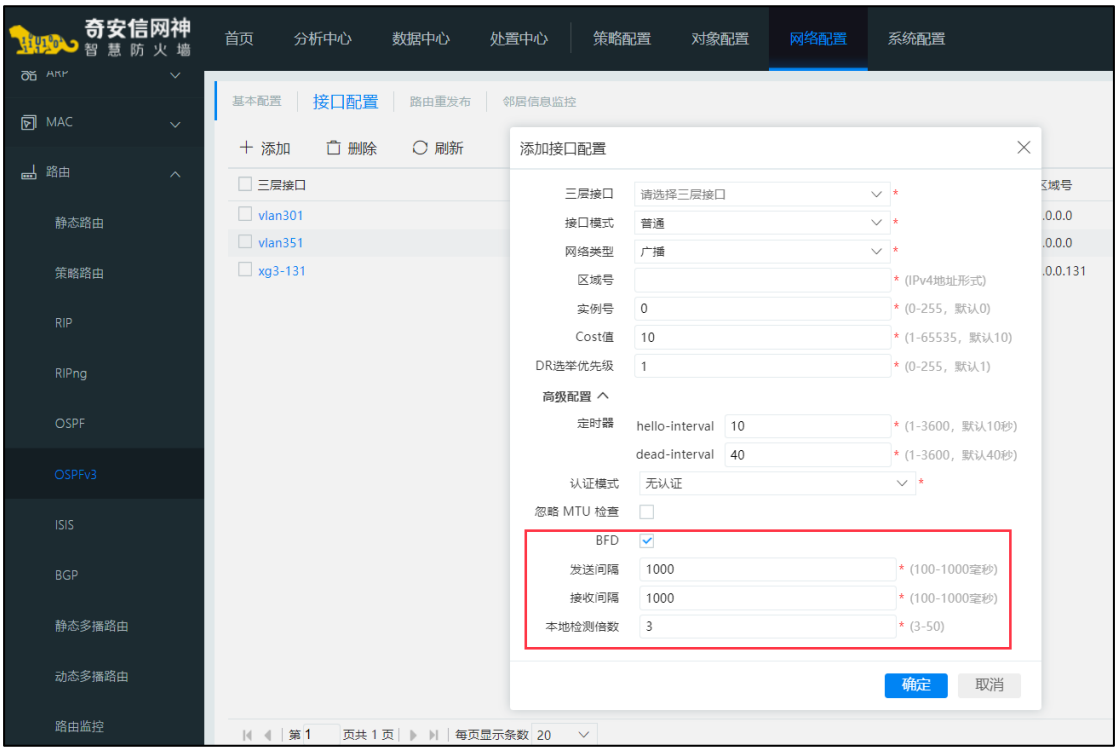
3.16.4.1 OSPFv3 路由支持缺省路由发布

选择【网络配置】>【路由】>【OSPFv3】。【基本配置】页面，新增支持缺省路由发布。



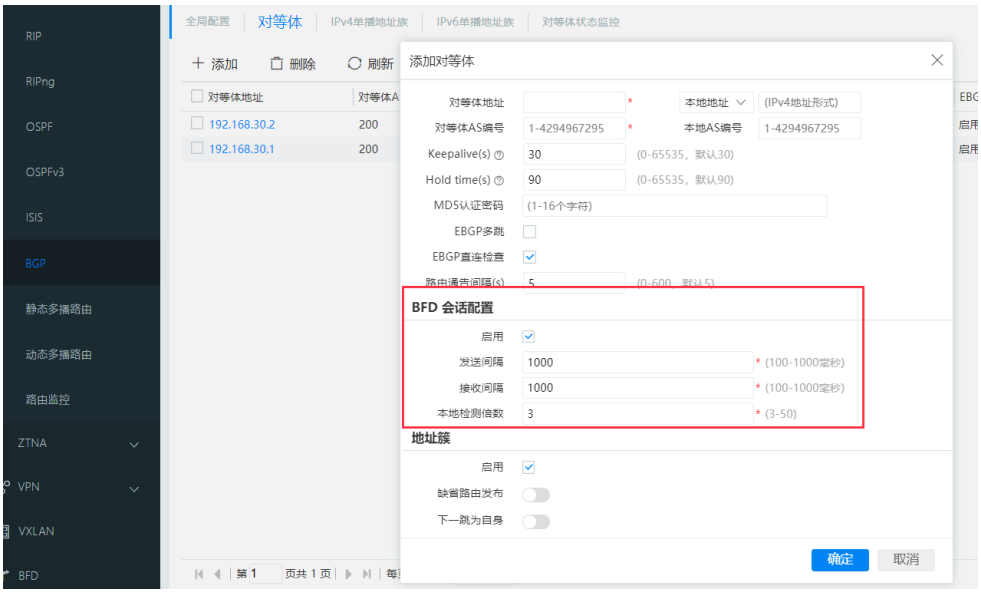
3.16.4.2 OSPFv3 与 BFD 联动

新增 OSPFv3 与 BFD 联动，可以实现 OSPFv3 路由快速收敛，收敛速度由秒级变为毫秒级。



3.16.5 BGP

BGP 支持 BFD 会话配置。支持通过 BFD for BGP 实现 BGP 路由快速收敛。



3.17 NAT

3.17.1 NAT 处理优化

修改前：SNAT/DNAT 为单链，每添加或编辑一次都会锁 dp 一次，导致流量无法转发，市场问题多次遇到编辑 nat 后页面长时间无法管理的情况。

修改后：SNAT/DNAT 改为多链，可以解决单链导致的问题。

3.17.2 源 NAT 新增导入导出

选择【策略配置】>【NAT 策略】>【源 NAT】，源 NAT 页面新增【导入】、【导出】功能。

3.17.3 目的 NAT 新增导入导出

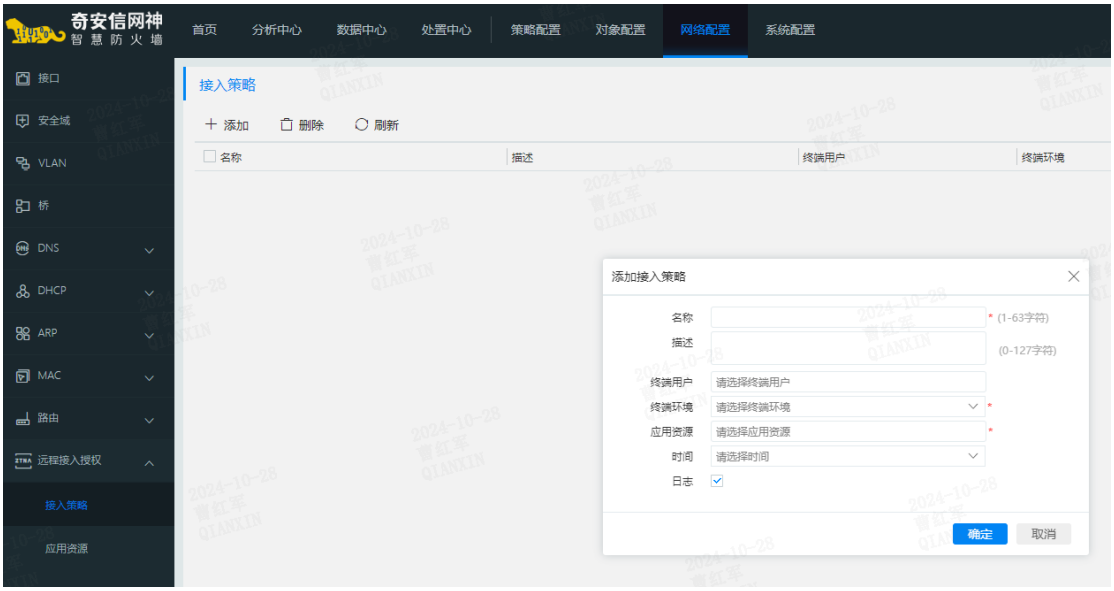
选择【策略配置】>【NAT 策略】>【目的 NAT】，目的 NAT 页面新增【导入】、【导出】功能。

3.18 远程接入授权

3.18.1.1 接入策略

防火墙网络配置菜单新增远程接入授权功能，支持客户端接入客户内部网络，可实现终端环境感知、应用资源访问策略获取等功能，相比传统的 SSL VPN 接入，连接更加安全，业务访问更加可控。

选择【远程接入授权】接入策略配置接入授权相关的基础功能配置，包括认证方式、加密方式、认证服务器、证书信息等

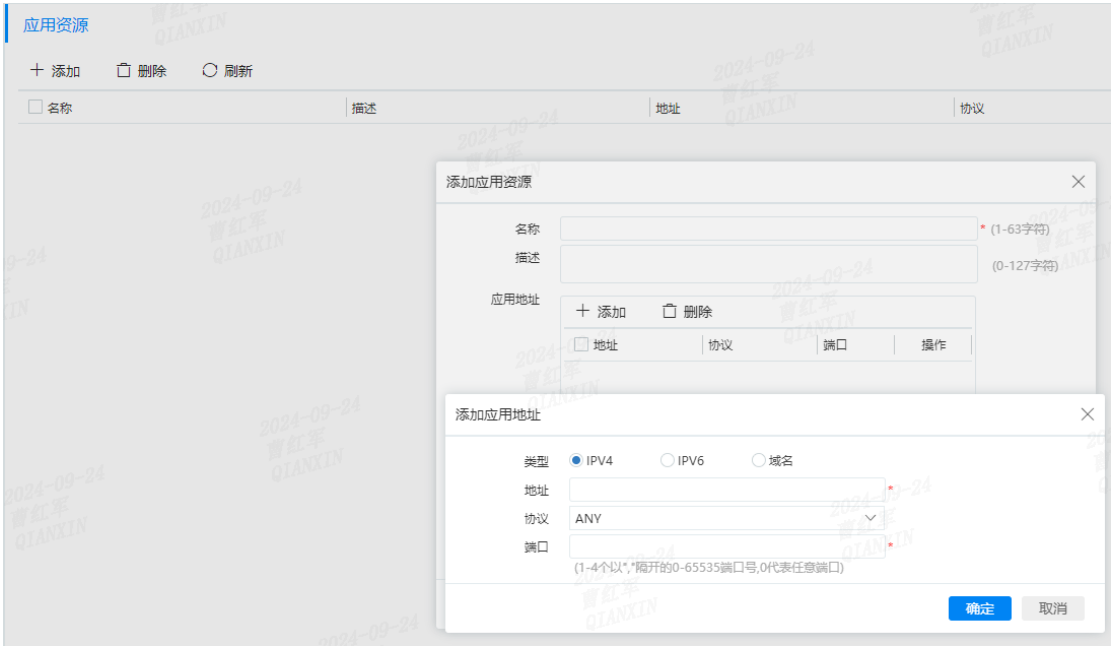


3.18.1.2 终端环境

选择【终端环境】配置组网终端环境信息 OS 类型，包括 Windows、MacOS、IOS、Linux、Android，和高级感知维度。

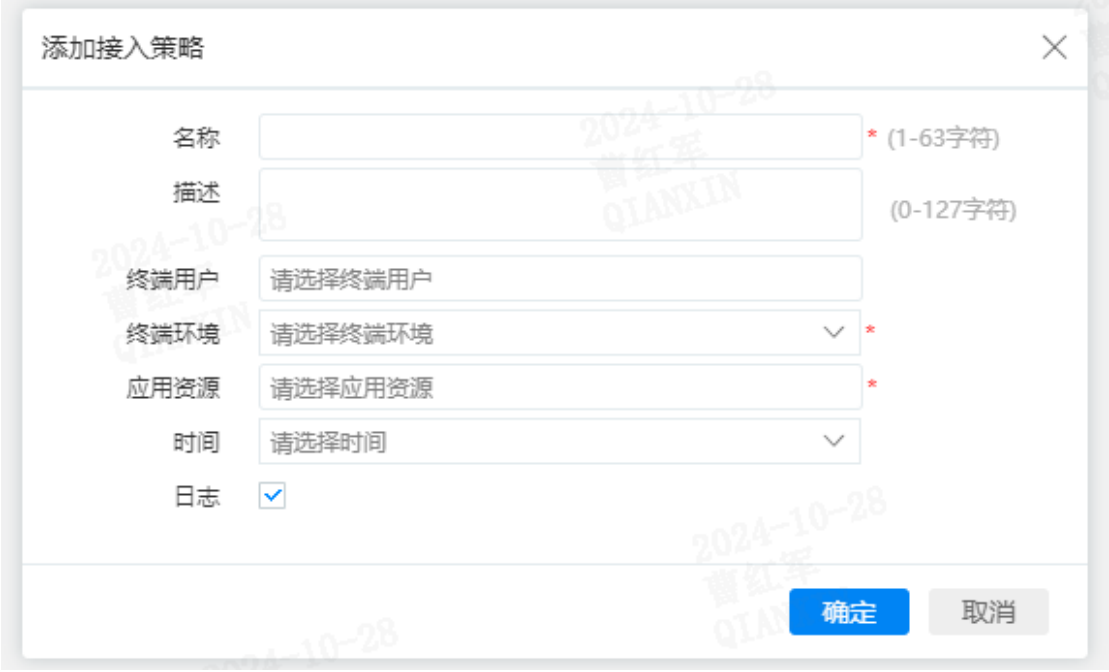
3.18.1.3 应用资源

选择【应用资源】应用资源为终端提供业务访问，类似目标业务系统，支持 Ipv4、Ipv6 以及域名类型。



3.18.1.4 接入策略策略

选择接入策略，终端用户访问应用资源通过接入策略匹配生成相关的终端访问策略。



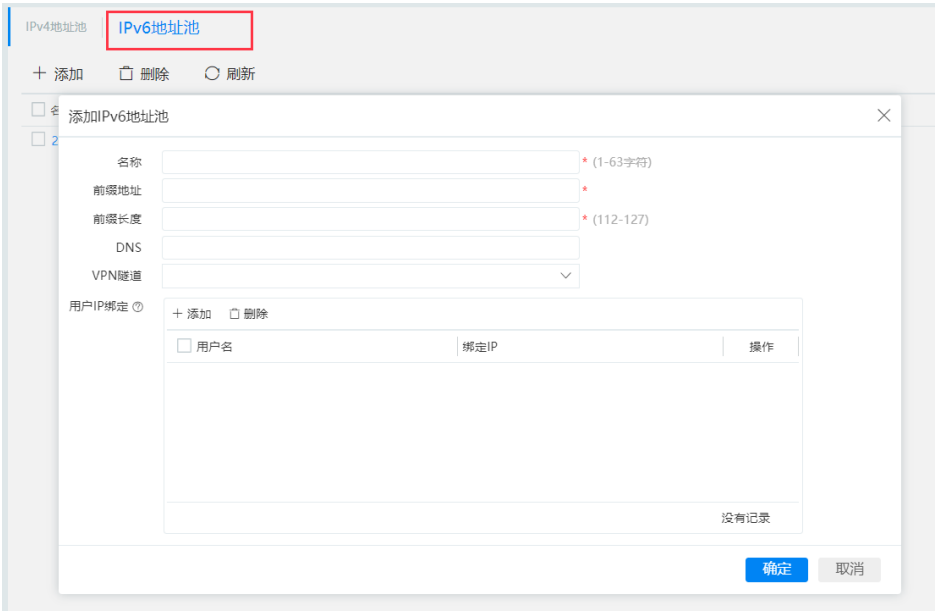
3.18.1.5 OAuth 服务器

选择【OAuth 服务器】Oatuh 为远程接入授权提供 SSO 单点登录服务，使用该服务需要改造原有应用业务系统。

3.19 VPN

3.19.1 VPN 地址池

选择【网络配置】>【VPN】>【VPN 地址池】，新增支持 IPv6 地址池。

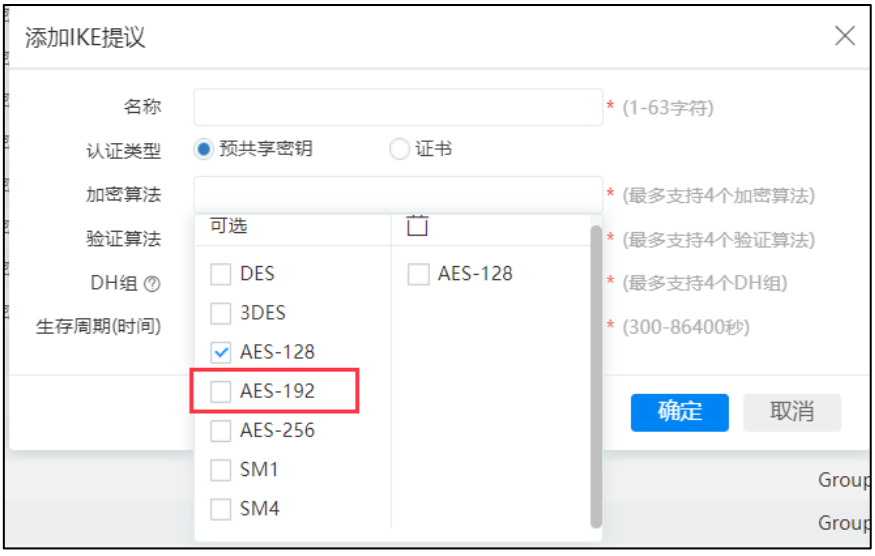


3.19.2 IPSec VPN

选择【网络配置】>【VPN】>【IPSec 自动隧道】。

3.19.2.1 IKEv1 提议

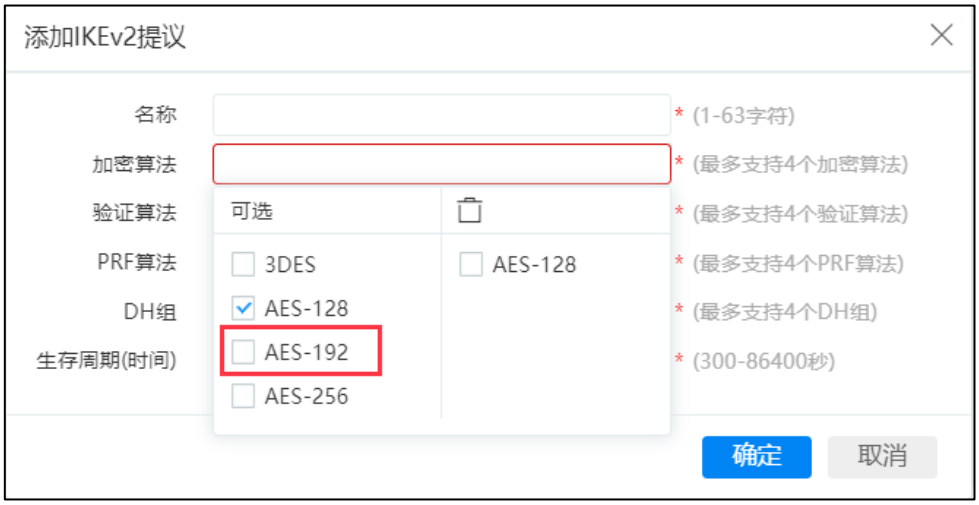
- 加密算法新增支持 AES-192。



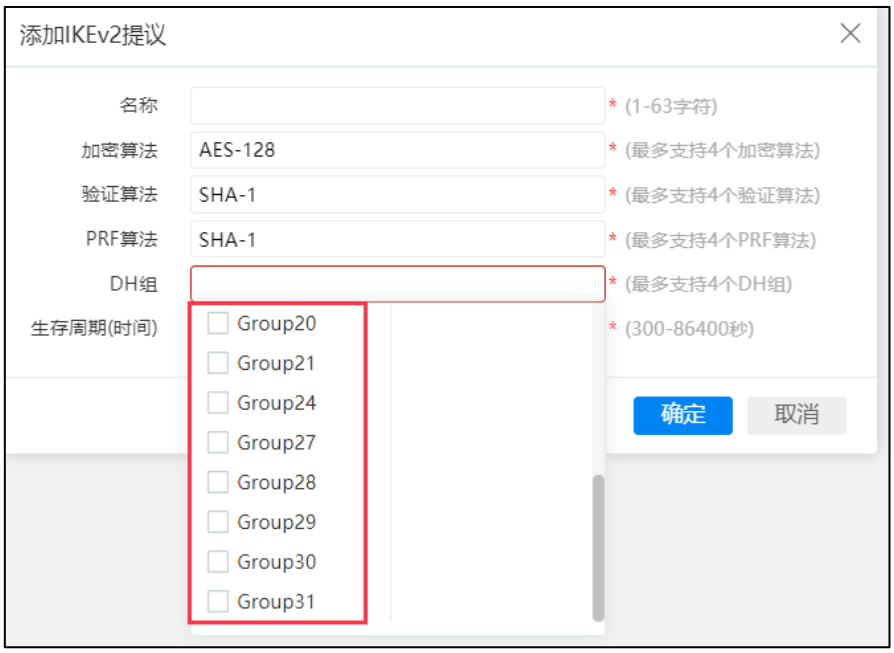
- DH 组新增支持 Group20、Group21、Group24、Group27、Group28、Group29、Group30。

3.19.2.2 IKEv2 提议

- 加密算法新增支持 AES-192。

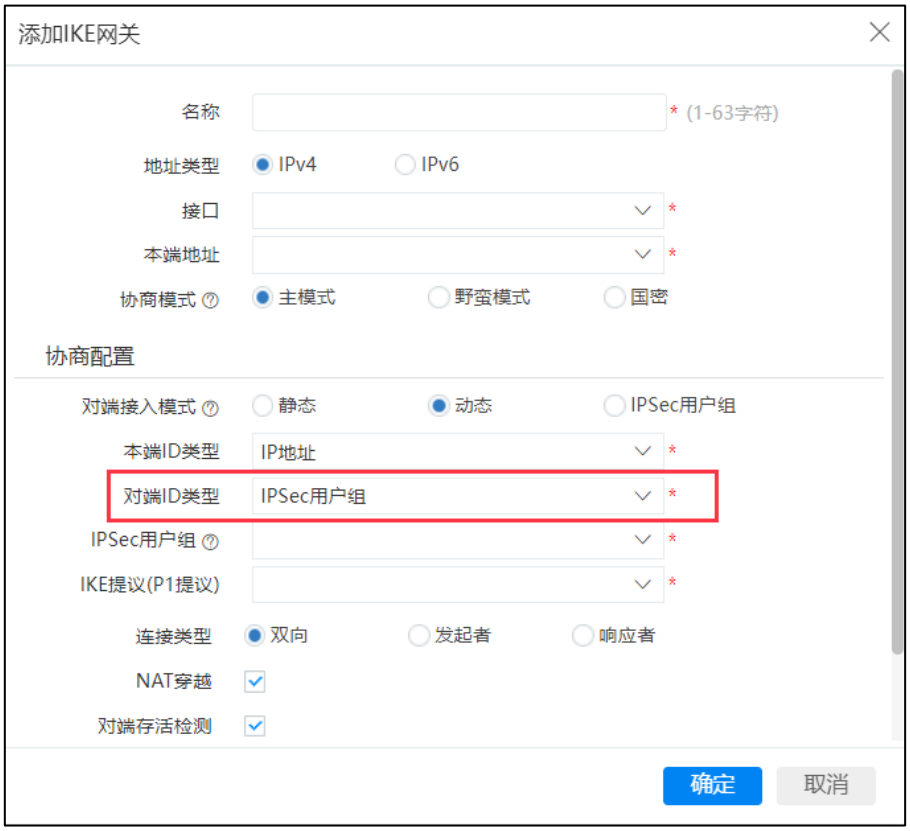


- DH 组新增支持 Group20、Group21、Group24、Group27、Group28、Group29、Group30、Group31。



3.19.2.3 IPSec IKEv1 网关

IKEv1 对端接入模式为“动态”时，对端 ID 类型支持“IPSec 用户组”。此方式可以实现 hub-spoke 模式下为每个网关配置单独的密钥。

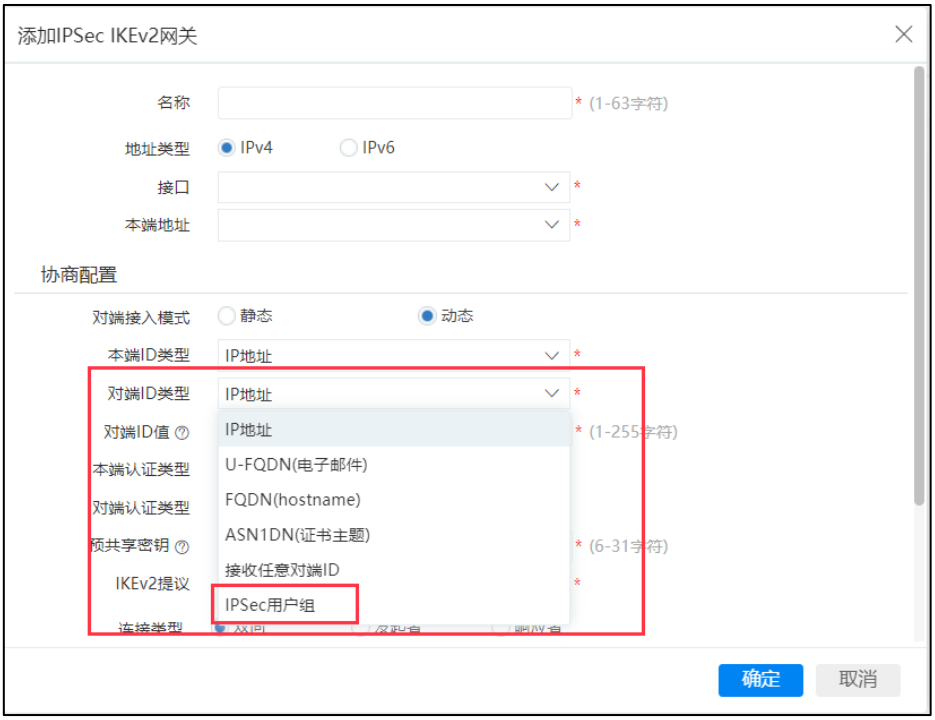


3.19.2.4 IPSec IKEv2 网关

选择【网络配置】>【VPN】>【IPSec 自动隧道】>【IPSec IKEv2 网关】。

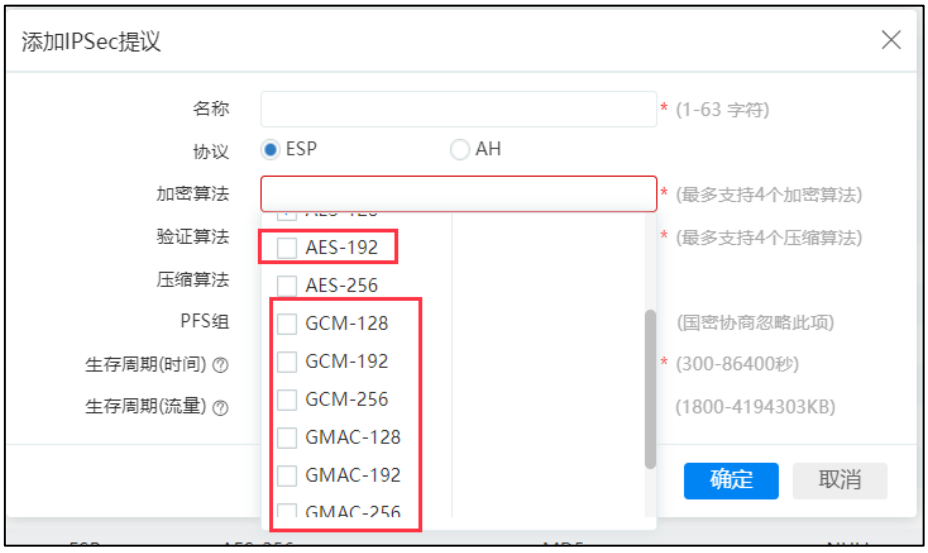
- 新增对端 ID 类型为 IP 地址、U-FQDN（电子邮件）和 FQDN（hostname）时，对端 ID 值可以直接配置通配符“*”。之前仅证书类型支持。

- IKEv2 对端接入模式为“动态”时，对端 ID 类型支持“IPSec 用户组”。此方式可以实现 hub-spoke 模式下为每个网关配置单独的密钥。

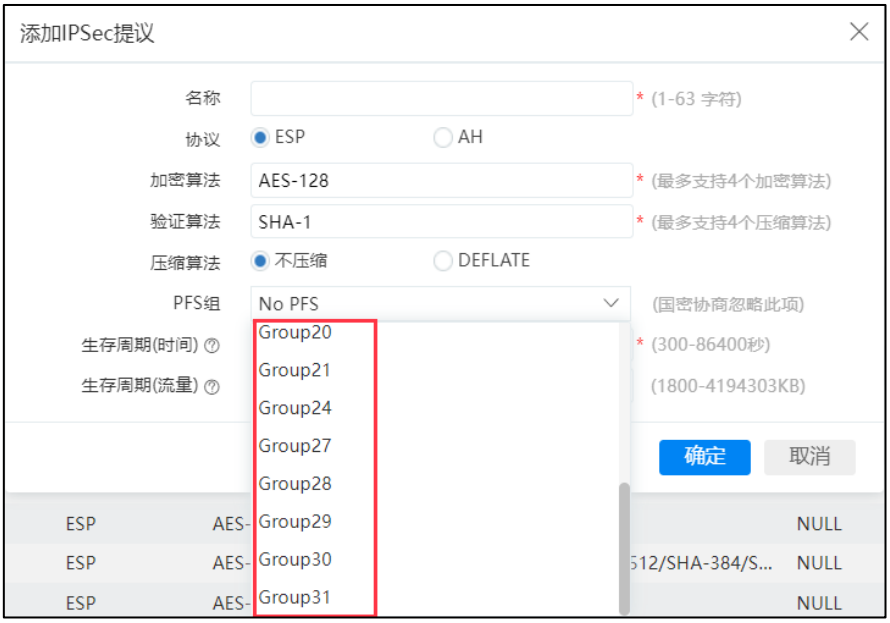


3.19.2.5 IPSec 提议

- 加密算法新增支持 AES-192、GCM-128、GCM-192、GCM-256、GMAC-128、GMAC-192、GMAC-256。



- PFS 组新增支持 Group20、Group21、Group24、Group27、Group28、Group29、Group30、Group31。采用 IKEv1 协商 IPSec 隧道时，Group31 不生效。



3.19.2.6 IPSec 隧道

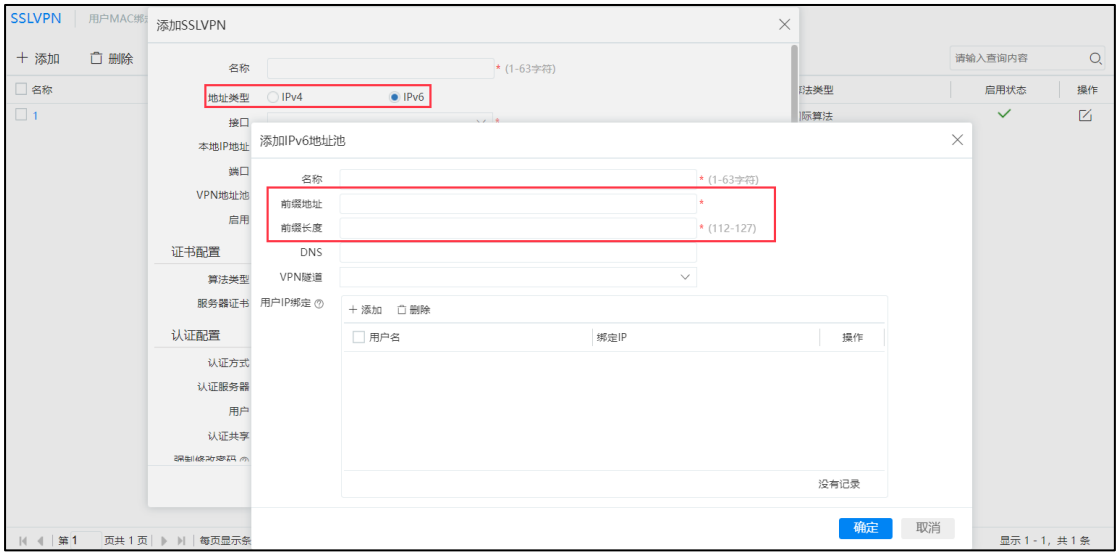
- 采用 IKEv2 协商隧道时支持反向路由注入功能。原来仅 IKEv1 协商时支持该功能。
- 采用 IKEv2 协商隧道时支持 ipv4 over ipsec6 / ipv6 over ipsec4，原来仅 IKEv1 支持。
- IPSec 数据流源地址、目的地址新增支持地址段格式，例如 1.1.1.1-1.1.1.254。IPv4 和 IPv6 数据流都支持地址段格式。只要隧道响应方的数据流 IP 范围包含隧道发起方的数据量 IP 地址范围，数据流就可以匹配成功；反之则不成功。

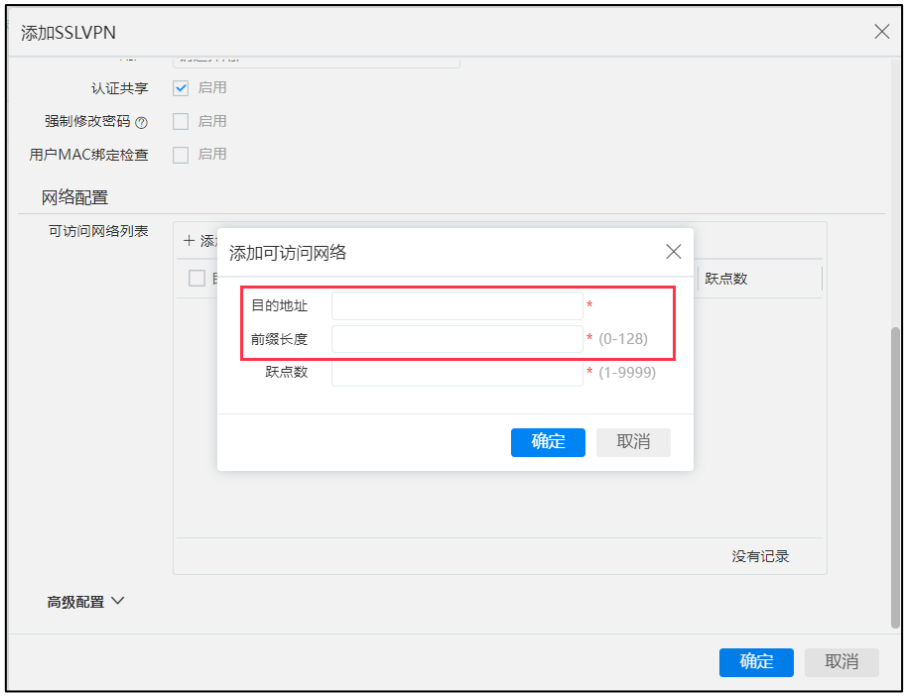
3.19.3 SSL VPN

选择【网络配置】>【VPN】>【SSL VPN】。

3.19.3.1 支持 IPv6 SSL VPN

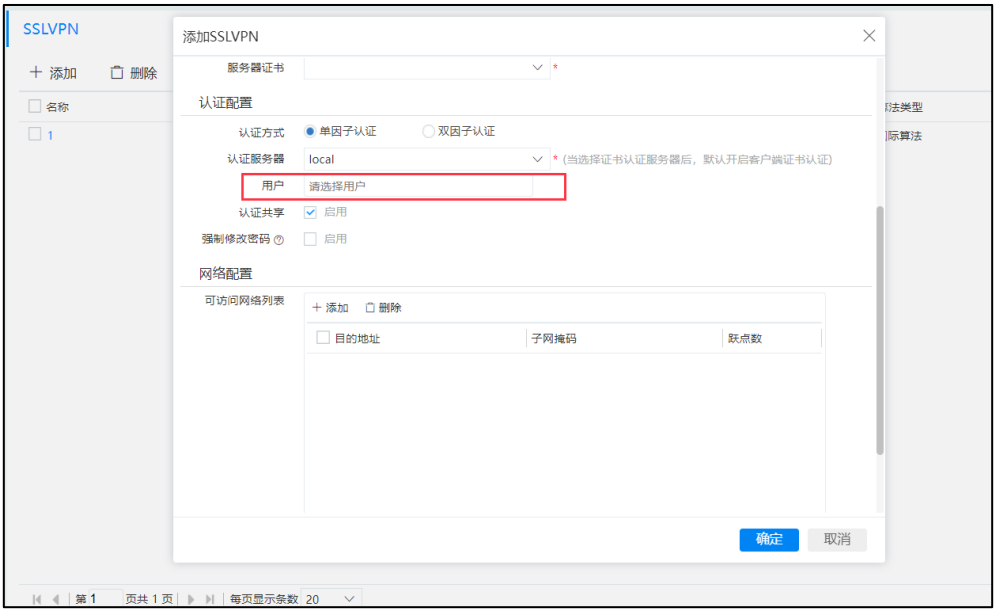
- SSLVPN 支持选择 IPv6 作为服务地址，可以基于此地址下载、连接客户端。支持访问 IPv6 网络。
- 地址类型未 IPv6 时，对应的 VPN 地址池为 IPv6 地址池，支持分发 IPv6 虚拟地址。
- SSLVPN 客户端（包括 windows、macos、ios、Android、linux 客户端）支持 IPv6 拨入，且可以正常转发业务。

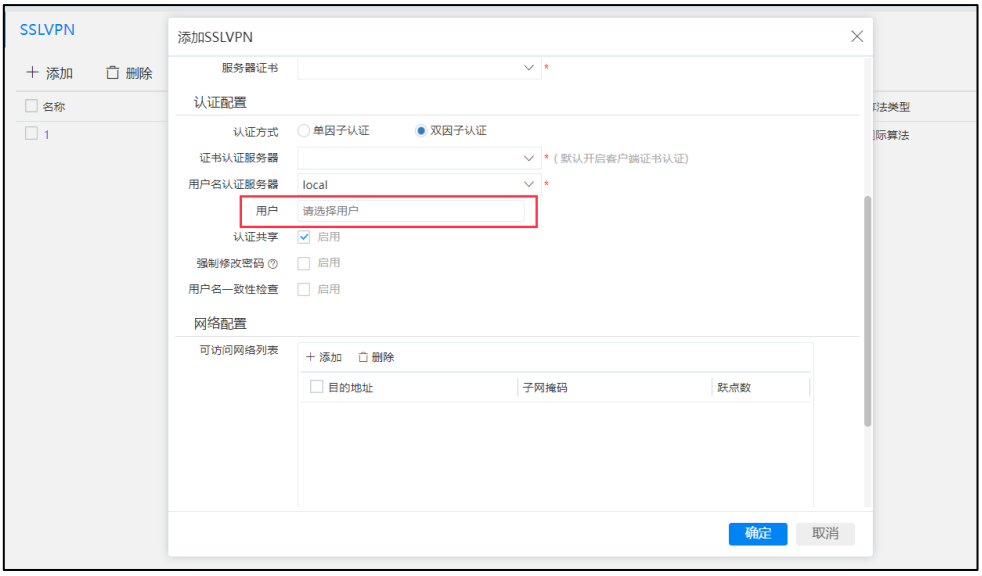




3.19.3.2 双因子场景校验用户和 CN 一致性

SSL VPN 新增支持指定接入隧道的用户。对接入隧道的用户基于用户名、用户组、用户角色等进行限制。

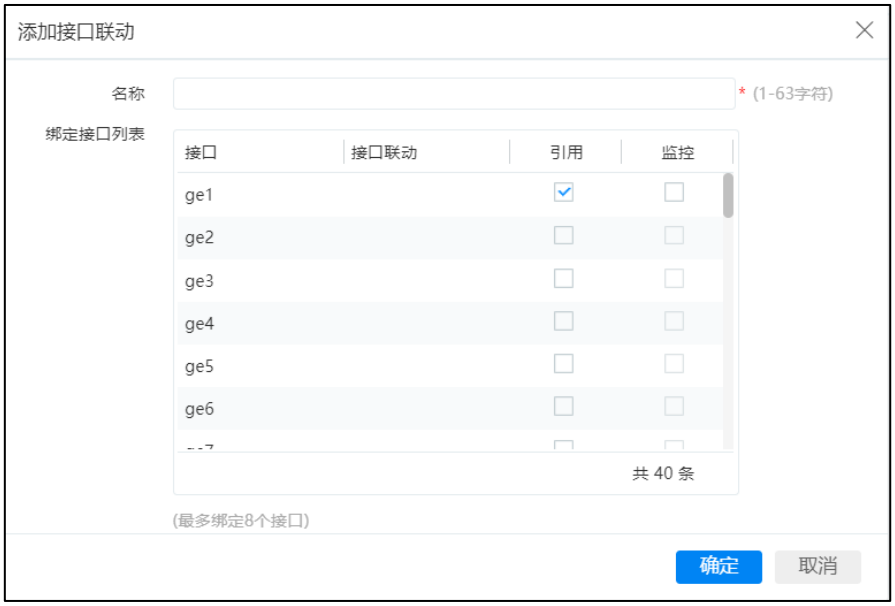




3.20 接口联动

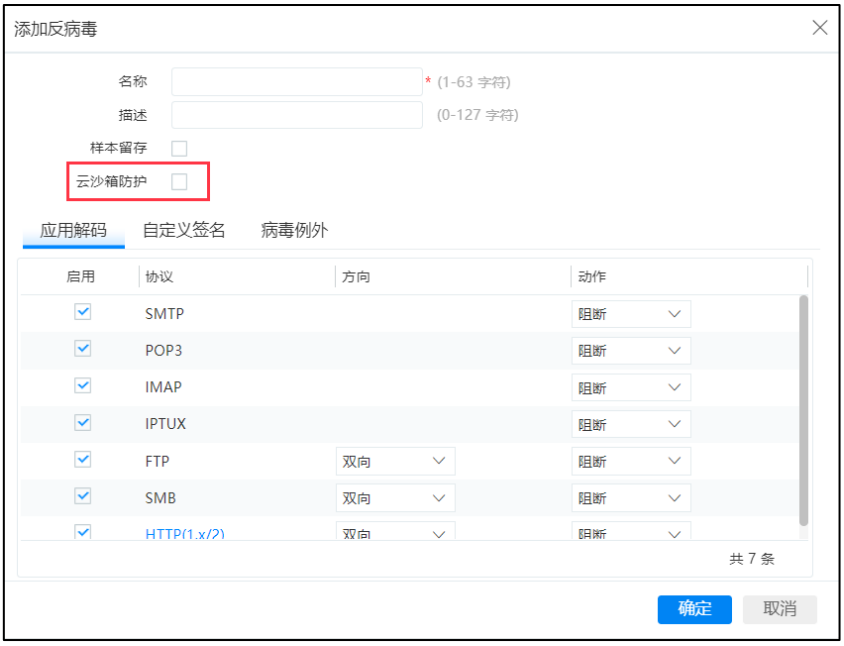
接口联动组中支持非监控状态接口。非监控状态接口 down，不会影响接口联动组状态，但接口联动状态 down 会导致非监控接口 down。

接口联动组中必须至少有一个接口为监控接口。



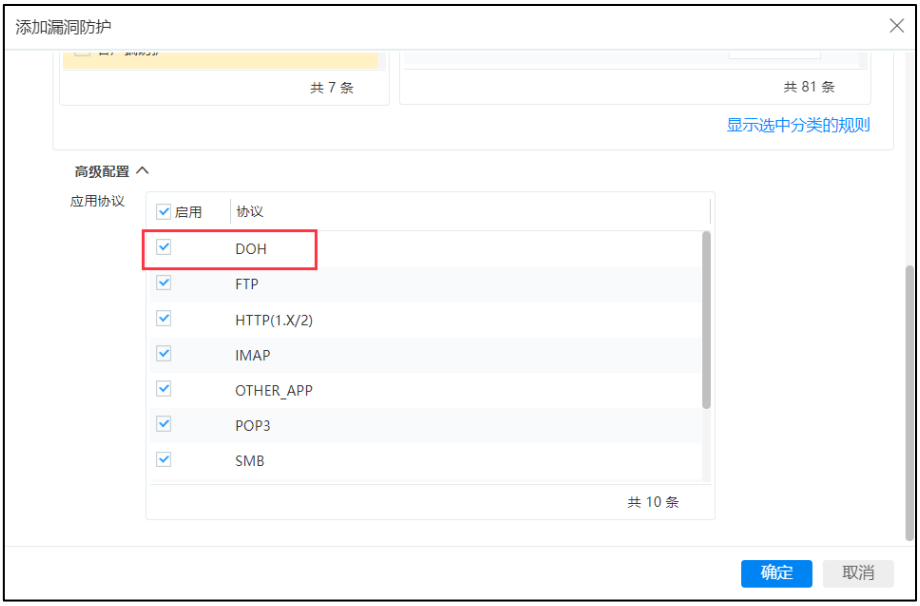
3.21 反病毒

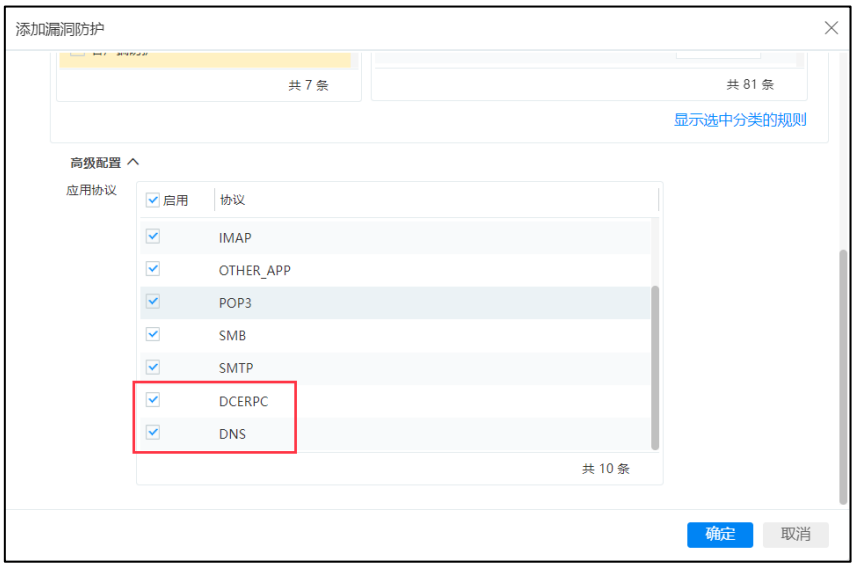
反病毒功能支持与云沙箱联动。防火墙将本地留存样本上传到核心云平台进行云沙箱检测，并将沙箱检测结果和沙箱报告发送给防火墙。沙箱结果返回后，如果是黑样本或灰样本，记录沙箱日志；白样本不记录日志。



3.22 漏洞防护

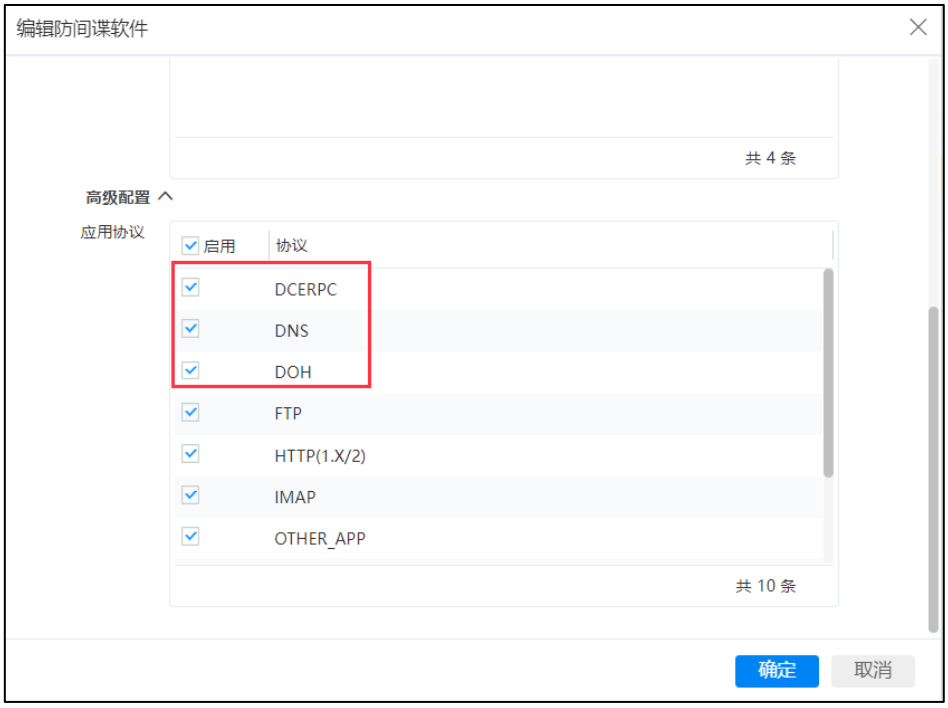
选择【对象配置】>【安全配置文件】>【漏洞防护】。新增支持基于 DOH 协议、DCERPC 和 DNS 协议的漏洞防护。





3.23 防间谍软件

选择【对象配置】>【安全配置文件】>【防间谍软件】。新增支持基于 DOH 协议、DCERPC 协议和 DNS 协议的防间谍软件。



3.24 攻击防护

3.24.1 恶意扫描

选择【策略配置】>【安全防护】>【攻击防护】，IP 扫描攻击和端口扫描攻击新增支持“动态防御”防护方式。

选择“动态防御”处理，在检测到发生扫描攻击后将攻击 IP 加入动态黑名单。该动态黑名单为防火墙的全局黑名单，当匹配动态黑名单的 IP 地址流量经过防火墙时报文将被直接丢弃。

支持为动态黑名单配置封禁时长，封禁时长取值范围为 1-60 分钟，默认为 16 分钟。只有动态黑名单的 IP 地址被手动删除后老化后，该 IP 才可以正常访问防火墙保护的网络。

3.24.2 NTP Reply Flood

选择【策略配置】>【安全防护】>【攻击防护】,【应用层 Flood】区域框的下 NTP Reply Flood 新增支持源认证智能防御方式。

3.25 IP-MAC 绑定

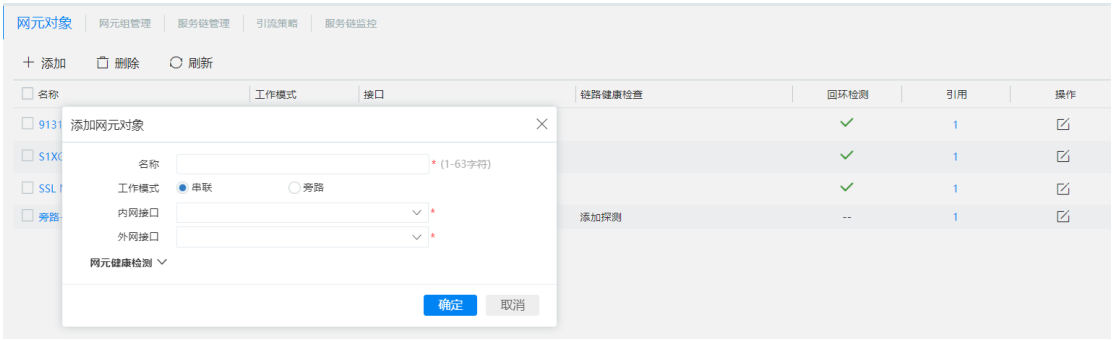
修改匹配逻辑。

修改前的逻辑为“基于 IP 地址查询是否命中 IP-MAC 绑定策略”。只有 IP 地址命中了 IP-MAC 策略才会检查 MAC 地址是否正确。这个逻辑存在的问题是，当数据包 IP 地址不是我们配置的 IP-MAC 绑定条目中的地址，那么数据包在 IP-MAC 处理流程中一定会被放行，不管 MAC 地址是否命中 IP-MAC 绑定策略。

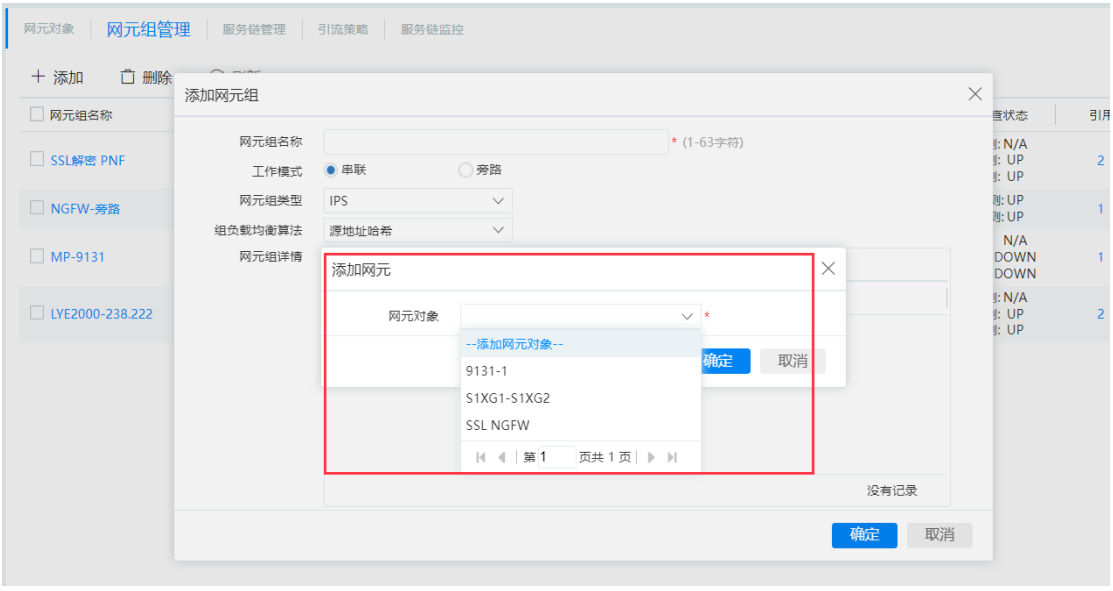
修改后的逻辑为“基于 MAC 地址查询是否命中 IP-MAC 绑定策略”。只有命中 MAC 地址，那么再检查 IP 地址是否为该 MAC 绑定的 IP 地址中的一个。此方式不会有遗漏。

3.26 流量编排

选择【策略配置】>【流量编排】，新增网元对象。

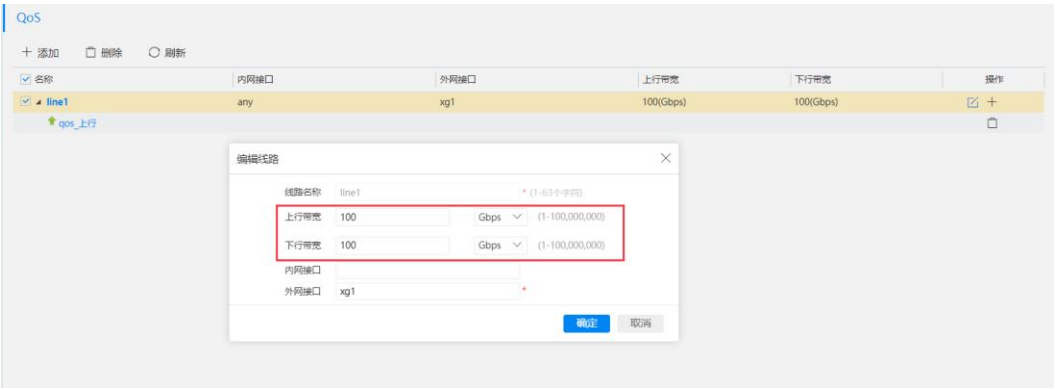


网元组下修改为添加网元时引用网元对象。



3.27 QoS

选择【策略配置】>【QoS】。支持对 QoS 线路上行带宽和下行带宽进行编辑修改。



3.28 黑白名单

3.28.1 地址黑名单

选择【策略配置】>【黑白名单】>【地址黑名单】。新增支持配置地址对象黑名单。

地址黑名单的匹配优先级为“地址对象黑名单 > 单 IP 地址黑名单 > 批量黑 IP > MAC 地址黑名单”。

3.28.2 批量黑 IP 封堵

选择【策略配置】>【黑白名单】>【批量黑 IP 封堵】。

- 新增支持配置匹配模式。

  单击列表上方的【匹配模式】按钮，弹出【匹配模式】设置页面。

  批量黑 IP 默认匹配源 IP，即只有流量的源 IP 命中批量黑 IP 才会记录威胁日志。

  可以根据用户的使用场景修改匹配模式。匹配模式支持“源 IP”、“目的 IP”和“源目的 IP”。

- 支持添加批量黑 IP

  支持添加 IP 地址或地址范围。可以支持 IPv4 地址和 IPv6 地址。每行添加一个 IP 地址或 IP 地址范围，最多支持添加 128 行。

添加的黑 IP 默认不在列表中显示，查询具体的 IP 地址后可以在列表中显示该 IP 地址。

- 批量黑 ip 支持 web 查看，可删除显示的黑 IP

支持在右侧的搜索框框中输入具体的 IPv4 地址或 IPv6 地址，不支持输入关键字，必须是完整的 IP 地址。搜索后的 IP 地址在列表中显示。

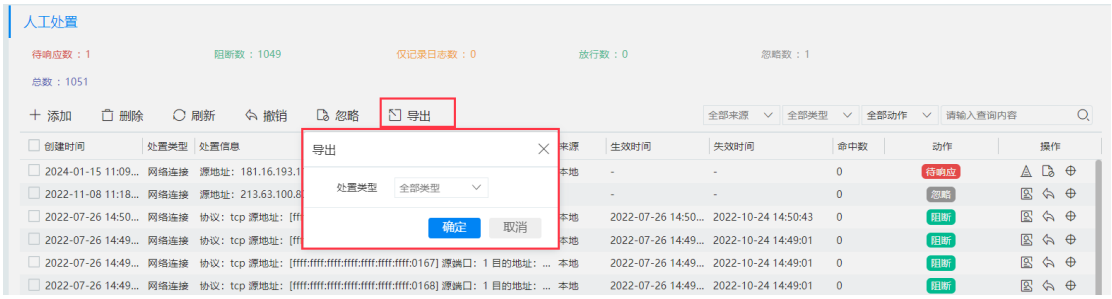
选中列表中显示的 IP 地址前的复选框，单击列表上方的【删除】按钮，可以删除该黑 IP。

3.29 处置中心

【处置中心】>【人工处置】。

- 支持 Web 方式导出人工处置策略。

  命令行还支持导出人工处置策略详情。



- 支持批量忽略和撤销。

支持基于类型清空人工处置策略仅命令行支持。

3.30 数据中心

3.30.1 日志

3.30.1.1 流量日志

【数据中心】>【日志】的流量日志中增加【会话删除原因】参数，该参数默认显示。

详细信息中也增加会话删除原因。

3.30.1.2 域名日志

记录 DNS 应答方向的域名日志，新增支持记录 DNS 请求方向的域名日志。

3.30.2 日志外发

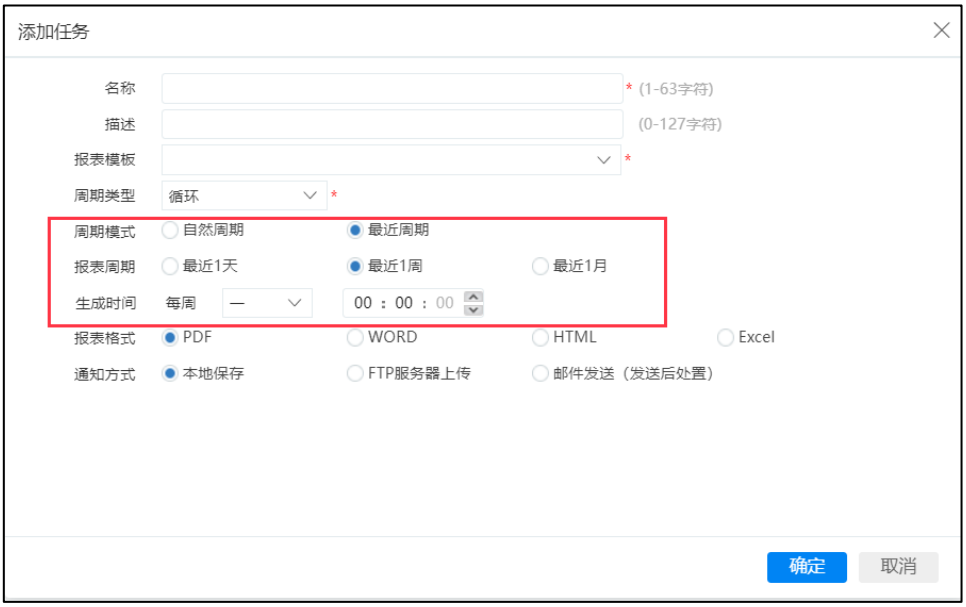
Syslog 日志支持 WEB 配置使用 MGT 口进行日志外发。

3.30.3 报表

选择【数据中心】>【报表】>【报表配置】>【报表任务】，添加或编辑报表任务页面。

报表任务新增支持设置周期模式。新增“最近周期”模式，可以生成“最近 1 天”、“最近 1 周”和“最近 1 月”的报表。

新增支持设置生成时间。



3.30.3.1 报表模板

选择【数据中心】>【报表】>【报表配置】>【报表模板】。

新增支持 LOGO 定制。

3.30.3.2 报表查看

选择【数据中心】>【报表】>【报表查看】。

报表过滤新增支持最近一小时、自定义时间范围进行查询当前设备上的报表。

支持在线查看 html 报表。

4 硬件更新说明

4.1.1 新增产品型号及配套板卡

新增产品	说明	配套板卡
NSG8000-RT35	板载 MGT+HA 接口 16 电+8 千兆光+16 万兆光+2 个 40G+2 个 100G+4 扩	NSG8000-RT-4T4S-EBC NSG8000-RT-8S-EBC NSG8000-RT-4X-EBC NSG8000-RT-4XP-MM-EBC NSG8000-RT-4XP-SM-EBC

4.1.2 新增单板及配套产品

新增板卡	说明	配套产品
NSG8000-RT-4T4S-EBC	4 口 10/100/1000Base-T 和 4 口千兆 SFP 板卡 （选配）：4 电口和 4 个 SFP 插槽	NSG8000-RT35

新增板卡	说明	配套产品
NSG8000-RT-8S-EBC	8 口千兆 SFP 板卡（选配）：8 个 SFP 插槽	
NSG8000-RT-4X-EBC	4 口万兆光口板卡（选配）：4 个 SFP+插槽	
NSG8000-RT-4XP-MM-EBC	4 口万兆多模 SFP 板卡（选配）：4 个 SFP+插槽，支持 2 对硬件 bypass	
NSG8000-RT-4XP-SM-EBC	4 口万兆单模 SFP 板卡（选配）：4 个 SFP+插槽，支持 2 对硬件 bypass	

新增板卡	说明	配套产品

4.1.3 其他硬件变更

无

5 修正 Bug 清单

表 5-1 修正 Bug 清单说明

编号	功能模块	描述	Bug 号
1			
2			
3			
5			
6			
7			
8			
9			

6 发布文件列表

表 6-1 6.1.14.版本发布文件列表说明

编号	文件说明	文件名称
1	产品安装包	
2	版本号	
3	文件大小	
4	MD5	
5	SHA-1	
6	SHA-256	

表 6-2 6.91.14.1 版本发布文件列表说明

编号	文件说明	文件名称
1	产品安装包	
2	版本号	
3	文件大小	
4	MD5	
5	SHA-1	
6	SHA-256	

表 6-3 6.90.14.版本发布文件列表说明

编号	文件说明	文件名称
1	产品安装包	
2	版本号	
3	文件大小	
4	MD5	
5	SHA-1	
6	SHA-256	

7 资料获取

表 7-1 资料获取清单说明

编号	资料名	文件说明	归档地址
1	网神 SecGate 3600 防火墙 V3.6.6.0 升级指导书	为用户提供升级指导。帮助用户选择升级版本、提供升级方法并提供升级失败时的处理方法	
2	网神 SecGate 3600 防火墙 V3.6.6.0 快速上线部署手册	为首次安装、使用提供指导。同时列举管理产品的基本操作方法。	
3	网神 SecGate 3600 防火墙 V3.6.6.0 用户手册	为管理员提供功能说明和配置指导。	
4	网神 SecGate 3600 防火墙 V3.6.6.0 配置指南	以案例的形式为用户提供配置指导，并列举常见问题解决方法。	