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

奇安信集团，保留所有权利。

奇安信集团及其关联公司对其发行的或与合作伙伴共同发行的产品享有版权，本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程描述等内容，除另有特别注明外，所有版权均属奇安信集团及其关联公司所有；受各国版权法及国际版权公约的保护。

对于上述版权内容，任何个人、机构未经奇安信集团或其关联公司的书面授权许可，不得以任何方式复制或引用本文的任何片断；超越合理使用范畴、并未经上述公司书面许可的使用行为，奇安信集团或其关联公司均保留追究法律责任的权利。

由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

1 手册概述 7
1.1 手册简介 7
1.2 适用产品 7
1.3 读者对象 7
1.4 配套手册 7
1.5 符号约定 7
1.6 修订记录 8
2 版本配套说明 9
2.1 产品版本信息 9
2.2 兼容性列表 10
2.2.1 对接设备兼容性 10
2.2.2 浏览器兼容性 11
2.2.3 支持升级的版本 11
3 可获得性说明 15
4 版本更新说明 16
4.1 管理员密码找回 16
4.2 设备管理 16
4.2.1 NTP 16
4.2.2 管理端口 17
4.2.3 管理账号 17
4.2.4 管理角色 18
4.2.5 设备管理高级配置 18
4.3 升级管理 19
4.3.1 特征库升级 19
4.4 许可证 20
4.5 高可用性 20
4.5.1 HA 设置 20
4.5.2 BFD 监控 21
4.6 集中管理 21
4.7 CA 中心 22
4.7.1 生成一般证书 22
4.7.2 导出一般证书 23

4.8 协同防护 23
4.8.1 IDP 联动 23
4.8.2 云联防 24
4.9 云镜 25
4.10 接口 25
4.10.1 接口管理方式 25
4.10.2 DHCP 获取 IP 地址 26
4.11 路由 27
4.11.1 静态路由 27
4.11.2 策略路由 28
4.11.3 RIP 29
4.11.4 RIPng 29
4.11.5 OSPF 30
4.11.6 OSPFv3 32
4.11.7 BGP 33
4.11.8 IS-IS 35
4.11.9 路由监控 36
4.12 VPN 37
4.12.1 VPN 地址池 37
4.12.2 SSL VPN 37
4.12.3 IPSec VPN 38
4.13 VXLAN 40
4.14 BFD 41
4.15 链路健康检查 41
4.16 地址组 42
4.17 服务 43
4.17.1 服务 43
4.17.2 服务组 43
4.18 用户 44
4.18.1 用户 44
4.19 URL 44
4.20 资产识别 45
4.20.1 资产指纹库升级 45
4.20.2 自定义资产指纹库 46
4.21 反病毒 47
4.21.1 新增支持 IPTUX 协议 47

4.21.2 新增病毒样本上传 47
4.22 漏洞防护和防间谍软件 48
4.22.1 IPS 引擎优化 48
4.22.2 TCP/UDP 协议检测深度定制 48
4.23 Web 攻击防护 49
4.24 URL 过滤 54
4.25 行为管控 55
4.26 安全配置文件组 56
4.27 SSL 解密配置文件 57
4.27.1 SSL 服务器证书 57
4.27.2 SSL 代理白名单 58
4.27.3 SSL 解密证书 59
4.27.4 SSL 全局配置 60
4.28 漏洞扫描模板 61
4.29 安全策略 61
4.29.1 策略组 61
4.29.2 安全策略 62
4.29.3 冗余策略 63
4.30 NAT 策略 64
4.30.1 源 NAT 64
4.30.2 目的 NAT 64
4.31 流量编排 65
4.32 SSL 解密策略 66
4.33 IP-MAC 绑定 68
4.34 QoS 68
4.35 黑白名单 70
4.35.1 域名黑白名单 70
4.35.2 IDP 联动黑名单 70
4.36 会话限制 70
4.37 安全防护 71
4.37.1 攻击防护 71
4.37.2 RA 管控策略 73
4.37.3 弱口令检测 74
4.38 共享接入 75
4.39 漏洞扫描策略 76

4.40 处置中心 76
4.41 数据中心 76
4.41.1 日志 76
4.41.2 统计 80
4.41.3 监控 80
5 硬件更新说明 81
5.1.1 新增产品型号及配套板卡 81
5.1.2 新增单板及配套产品 83
5.1.3 其他硬件变更 88
6 修正 Bug 清单 89
7 发布文件列表 90
8 资料获取 90

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 和遗留 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	X86 平台：V3.6.6.0(-6.1.14.164546) ARM913x 平台：V3.6.6.0(-6.90.14.164546) ARM CN96 平台：V3.6.6.0(-6.91.14.164546)

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 2023-11-22）

第一次正式发布。

2 版本配套说明

2.1 产品版本信息

产品名称	网神 SecGate3600 防火墙		
产品平台	X86 平台 NSG3000/5000/7000/9000 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	6.1.14.164546	6.90.14.164546	6.91.14.164546
适用型号	● NSG3000 系列 NSG3000-TE45/ TE35/ TE25/ TE15 ● 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 ● NSG9000 系列 NSG9000- TZ75/ TZ65/ TZ55/ TZ45/ TZ35/ TZ25/ TZ15 ● 其他型号 NSG-1060/1260/1460	NSG6000-TX45/ TX35/ TX25 /TX15	● 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 客户端	客户端到网关模块拨入； Win 客户端支持 XP、windows7、windows10、WinServer 的 32 位及 64 位系统，直接管理 UI 获取即可。 Linux 客户端系统支持 Centos6.4/Ubuntu12.0。 安卓客户端支持 Android 6.0 及以上。 IOS 客户端（试用版）：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：V1.0.0.120866 CentOS 版本： V1.1.1.65079 Ubuntu 版本： V1.1.2.65079 安卓客户端版本：V1.3.0.101020 IOS 客户端版本：V1.2.0.65047，最低版本 V1.2.0.65039 MACOS 客户端版本：V1.4.3.10008
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.）
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.）
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。	V10.2.0.1000

产品名称	功能说明	版本配套说明
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

Firefox40 及以上或 chrome50 及以上内核的浏览器。

2.2.3 支持升级的版本

- 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、6.1.13.107345、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 版本升级到 6.1.14.164546。6.1.12 之前的版本必须选择 enc.sign 版本升级，或者跨版本升级。具体方式请参见《网神 SecGate3600 防火墙 V3.6.6.0(-6.xx.14.164546)-升级指导书》。
- 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、6.91.13.155312、6.91.13.156124、6.91.13.156764、

6.91.13.156693、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 升级到 6.91.14.164546。具体的升级方式请参见《网神 SecGate3600 防火墙 V3.6.6.0(-6.xx.14.164546)-升级指导书》。

- 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 升级到 6.90.14.164546。具体的升级方式请参见《网神 SecGate3600 防火墙 V3.6.6.0(-6.xx.14.164546)-升级指导书》。

2.2.3.1 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 6.1.14.164546 时需要注意：

- 6.1.12 及以后的版本可以直接升级到 6.1.14 最新版本。
- 6.1.12 之前的版本要直接升级到 6.1.14 最新版本，可以选择相应的 enc.sign 版本。若要升级的最新版本没有 enc.sign 版本，需要跨版本升级。首先选择 6.1.13 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。

不同版本对应的升级包说明如下：

- 6.1.14.164546 对应的软件升级包为 6.1.14.164546.86.sign。
- 6.91.14.164546 对应的软件升级包为 6.91.14.164546.91.sign。
- 6.90.14.164546 对应的软件升级包为 6.90.14.164546.96.sign。

2.2.3.2 升级影响

- 6.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。
- 6.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 6.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 6.xx.14.版本后文件过滤或内容过滤相应的这条规则丢失。
- 6.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。6.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。
- 6.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。
- 6.xx.1.13 版本及之前的版本升级到 6.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。
- 6.1.13.156124 之前的版本升级到 6.1.13.156124 版本及以后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，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，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。

- 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，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，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，描述信息可能会丢失。

3 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。

6.1.14 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。

4 版本更新说明

4.1 管理员密码找回

管理员密码重置方式有所变化。

4.2 设备管理

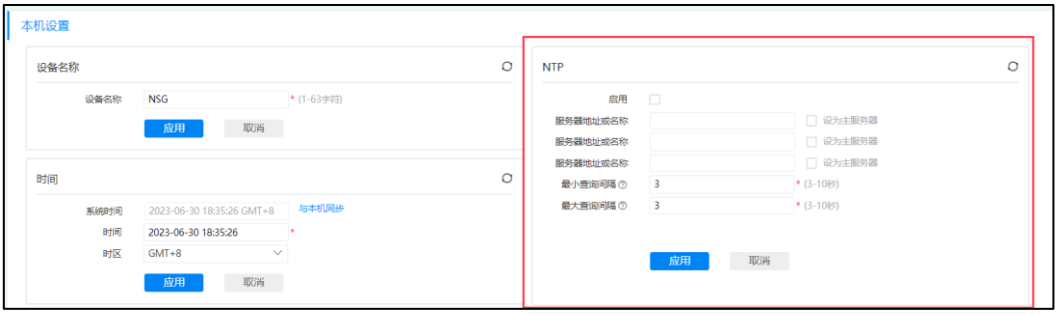
4.2.1 NTP

选择【系统配置】>【设备管理】>【本机设置】。

- NTP 由原来【本机设置】页面中去掉，单独放到【NTP】页面下。
- 之前只有一个服务器支持认证。修改后每个服务器都支持认证，支持对称式秘钥认证，认证算法支持“MD5”和“SHA1”。

修改后：

修改前：



4.2.2 管理端口

选择【系统配置】>【设备管理】>【管理主机】,【管理端口】页面修改如下：

- 新增“SSH 算法强度”配置。
- 删除 HTTP 和 Telnet 管理端口的配置。

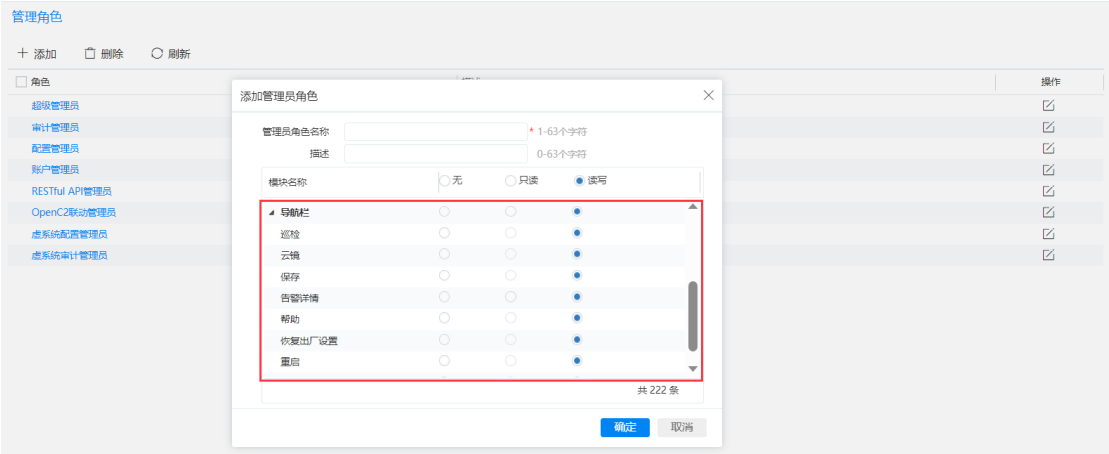
4.2.3 管理账号

【系统配置】>【设备管理】>【管理账号】下新增管理员 Ukey 认证。HTTPS 登录方式支持通过 Ukey 进行国密证书认证。

删除不安全的 HTTP 和 Telnet 登录方式。

4.2.4 管理角色

管理角色的权限控制新增【导航栏】。以前导航栏的功能没有控制。



4.2.5 设备管理高级配置

修改后：

修改前：

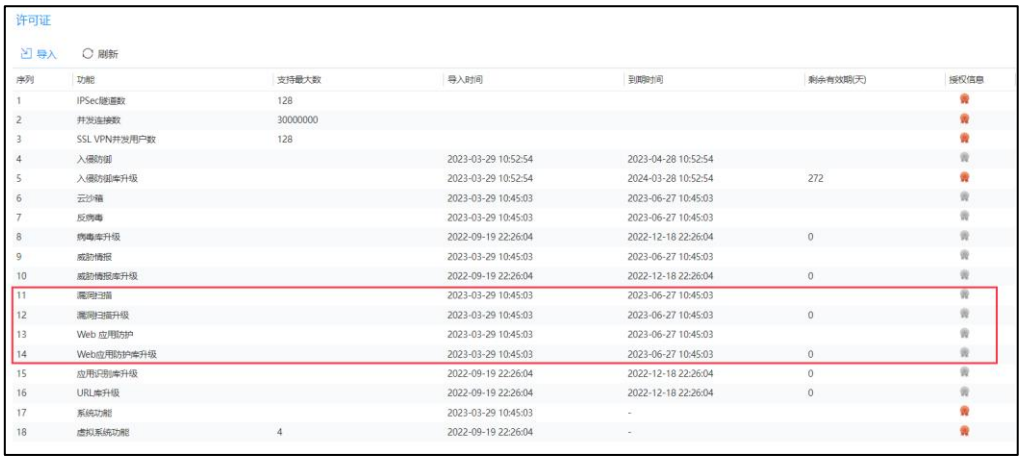
4.3 升级管理

4.3.1 特征库升级

选择【系统配置】>【升级管理】>【特征库升级】，特征库升级页面新增“资产识别库”、“文件类型库”、“漏洞扫描库”、“Web 应用防护”和“弱口令检测库”等 5 种库。

4.4 许可证

选择【系统配置】>【特征库】。新增“漏洞扫描”、“漏洞扫描升级”、“Web 应用防护”和“Web 应用防护库升级”控制项。



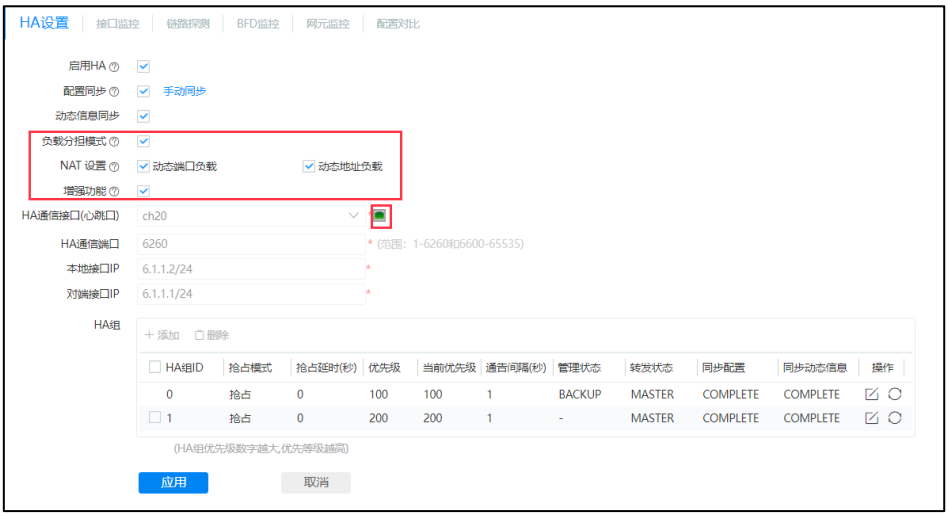
序列	功能	支持最大数	导入时间	到期时间	剩余有效期(天)	授权信息
1	IPSec隧道数	128				
2	并发连接数	30000000				
3	SSL VPN并发用户数	128				
4	入侵防御		2023-03-29 10:52:54	2023-04-28 10:52:54		
5	入侵防御库升级		2023-03-29 10:52:54	2024-03-28 10:52:54	272	
6	云沙箱		2023-03-29 10:45:03	2023-06-27 10:45:03		
7	反病毒		2023-03-29 10:45:03	2023-06-27 10:45:03		
8	病毒库升级		2022-09-19 22:26:04	2022-12-18 22:26:04	0	
9	威胁情报		2023-03-29 10:45:03	2023-06-27 10:45:03		
10	威胁情报库升级		2022-09-19 22:26:04	2022-12-18 22:26:04	0	
11	漏洞扫描		2023-03-29 10:45:03	2023-06-27 10:45:03		
12	漏洞扫描升级		2023-03-29 10:45:03	2023-06-27 10:45:03	0	
13	Web 应用防护		2023-03-29 10:45:03	2023-06-27 10:45:03		
14	Web应用防护库升级		2023-03-29 10:45:03	2023-06-27 10:45:03	0	
15	应用识别库升级		2022-09-19 22:26:04	2022-12-18 22:26:04	0	
16	URL库升级		2022-09-19 22:26:04	2022-12-18 22:26:04	0	
17	系统功能		2023-03-29 10:45:03	-		
18	虚拟系统功能	4	2022-09-19 22:26:04	-		

4.5 高可用性

4.5.1 HA 设置

选择【系统配置】>【高可用性】，HA 设置页面新增修改如下：

- 【非对称模式】复选框修改为【负载分担模式】复选框。
- 开启【负载分担模式】复选框后，新增“NAT 设置”和“增强功能”开关。
- 接口文本框右侧增加显示接口状态的图标。



4.5.2 BFD 监控

选择【系统配置】>【高可用性】，新增 BFD 监控功能。

BFD 监控可以保证网络中主用设备出现故障时，根据用户配置的优先级扣减权重值，判断防火墙是否进行主备切换。

4.6 集中管理

【系统配置】>【集中管理】>【集中管理】页面，新增 IPSec VPN 隧道监控信息上报功能。

4.7 CA 中心

4.7.1 生成一般证书

选择【系统配置】>【CA 中心】>【一般证书】，生成一般证书页面新增“用途”参数。证书的用途分为三类，分别是“NONE”、“加密”和“签名”。

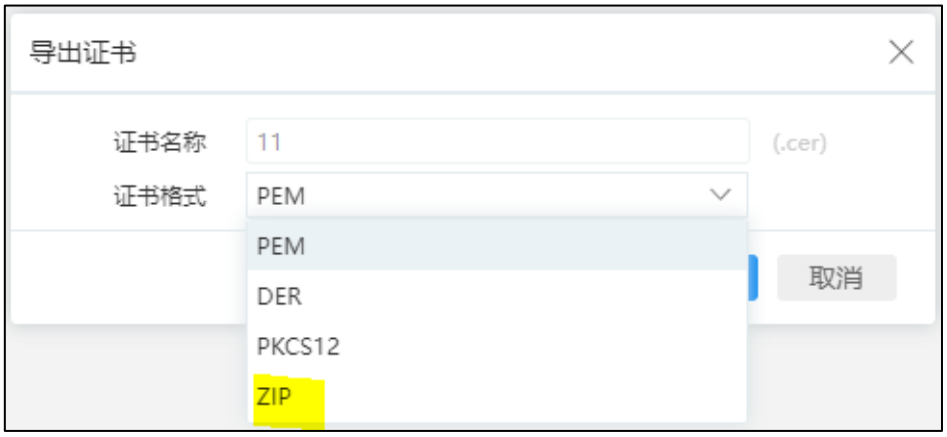
- “-”，代表原来的一般证书。
- “加密”，代表加密类别的证书。
- “签名”，代表签名类别的证书。

修改后：

修改前：

4.7.2 导出一般证书

导出证书格式新增“ZIP”格式。选择 ZIP 格式时导出 PEM 格式的证书，且把证书和私钥一起打包为 zip 格式。

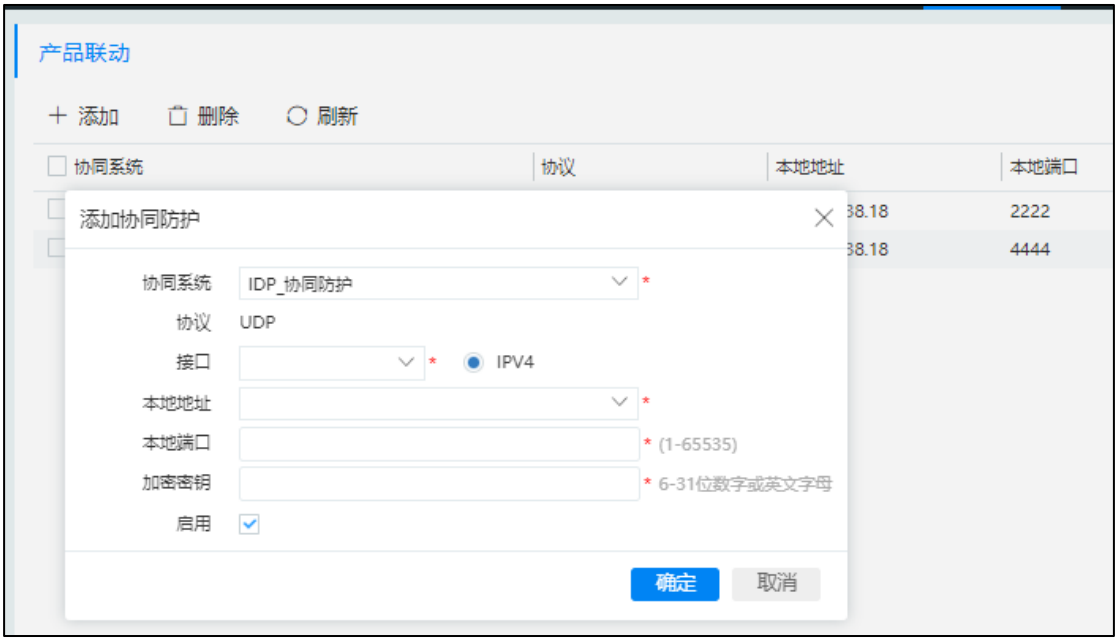


4.8 协同防护

4.8.1 IDP 联动

【系统配置】>【协同防护】>【产品联动】下新增 IDP 协同防护。

支持防火墙与 IPS 或 IDS 联动。防火墙将流量镜像到 IPS 或 IDS 设备进行检测，IPS 或 IDS 设备上有流量命中 IPS 库的漏洞后，将检测结果发送给防火墙，在防火墙上生成 IDP 联动黑名单。



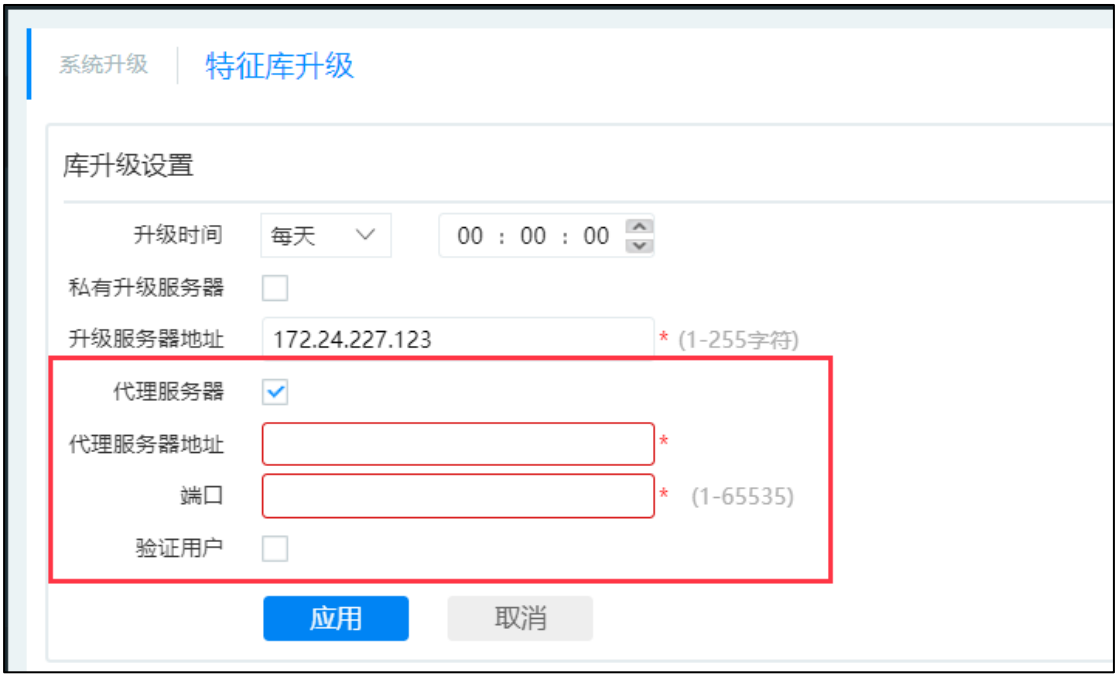
4.8.2 云联防

选择【系统配置】>【协同防护】>【云联防】,【云联防】页面的代理服务器修改后仅对云防生效。对本地威胁情报库升级不生效。

修改后:【威胁情报云检测设置】复选框作为云防的一个功能，放到云防下。【代理服务器】挪到【云防】后面,【威胁情报云平台】上面。

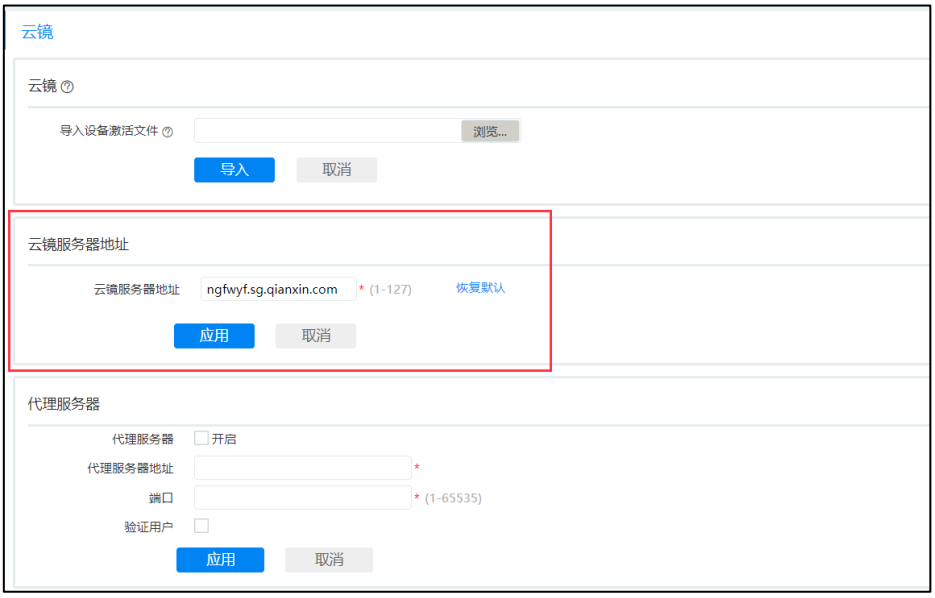
本地威胁情报库升级使用的代理服务器是特征库升级页面的代理服务器。

原因是由于老的版本中本地威胁情报库升级同时受云联防代理服务器和特征库升级代理服务器影响，造成混乱，所以新版本进行修改。



4.9 云镜

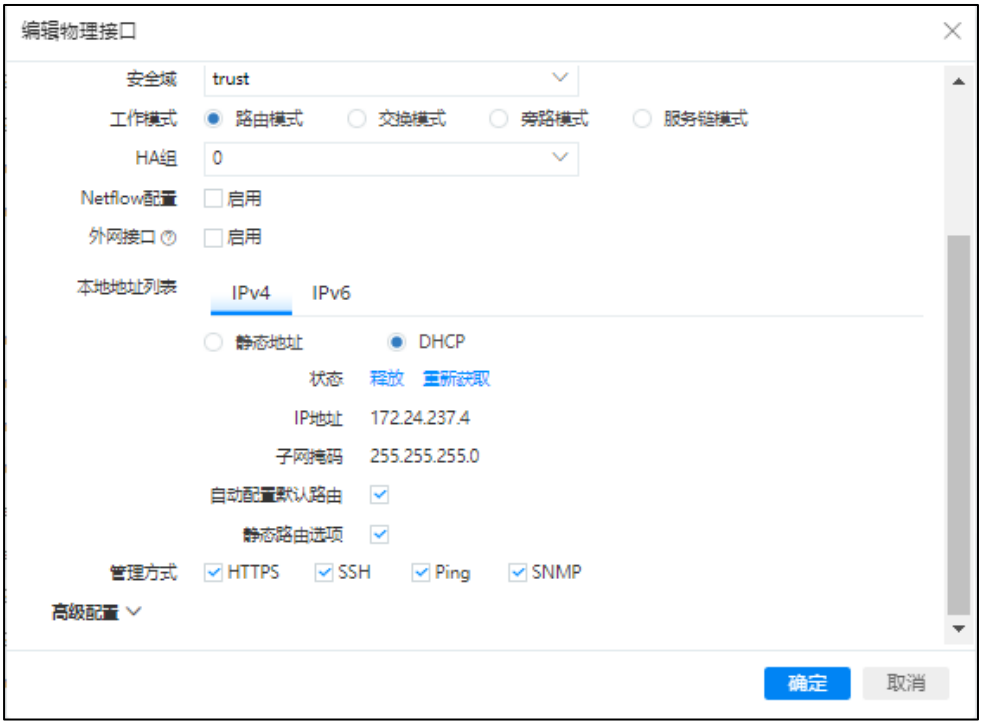
选择【系统配置】>【云镜】,【云镜服务器地址】区域框中的“重置”按钮修改名称为“恢复默认”。



4.10 接口

4.10.1 接口管理方式

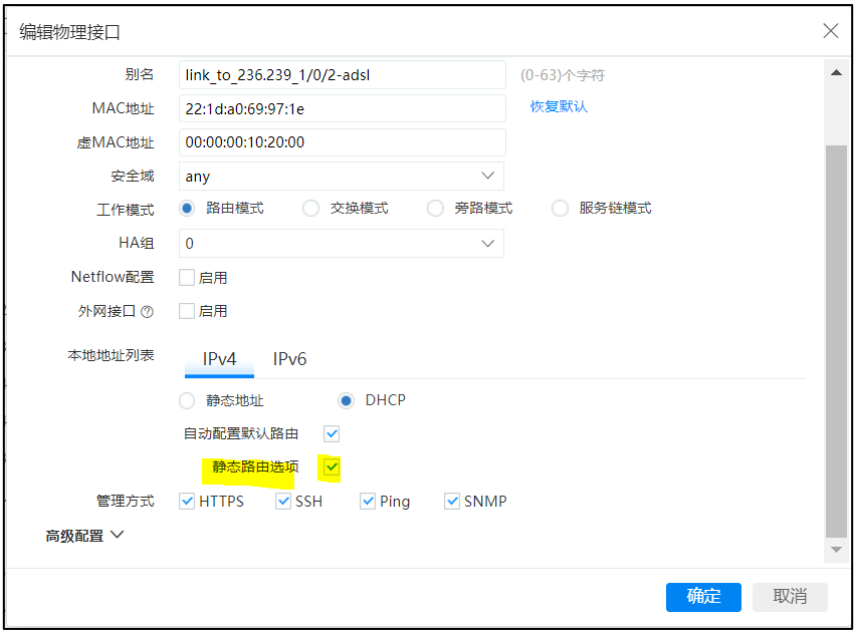
接口下管理方式删除了不安全的“HTTP”和“Telnet”方式。



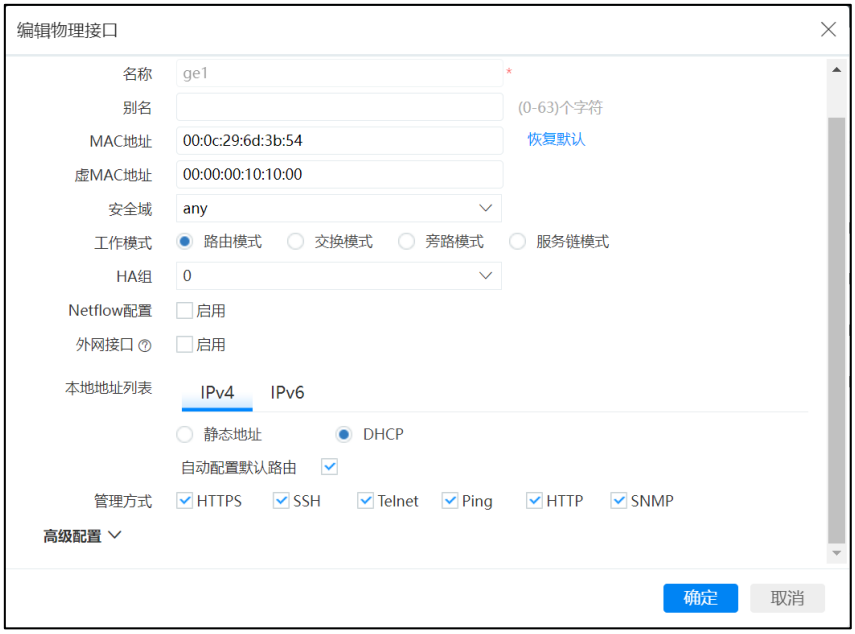
4.10.2 DHCP 获取 IP 地址

通过 DHCP 方式获取 IP，新增支持静态路由选项。该功能默认开启，接口获取 IP 地址后自动添加静态路由。

修改后：



修改前：



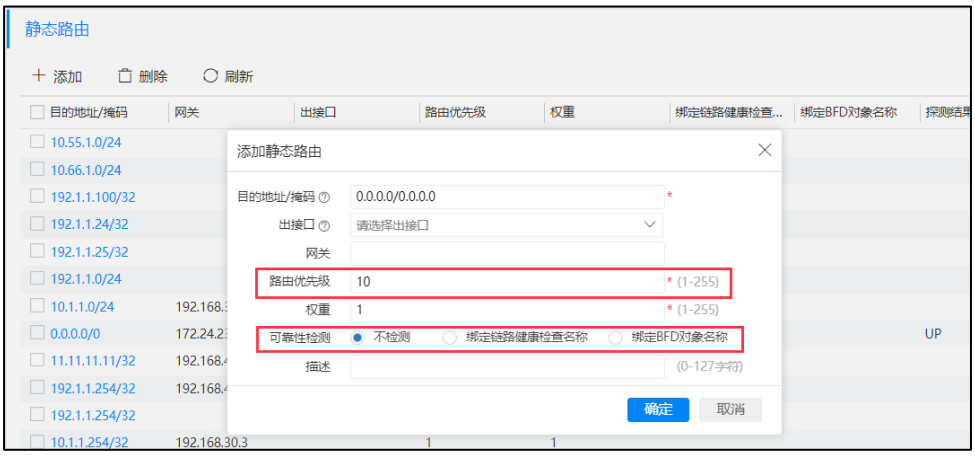
4.11 路由

4.11.1 静态路由

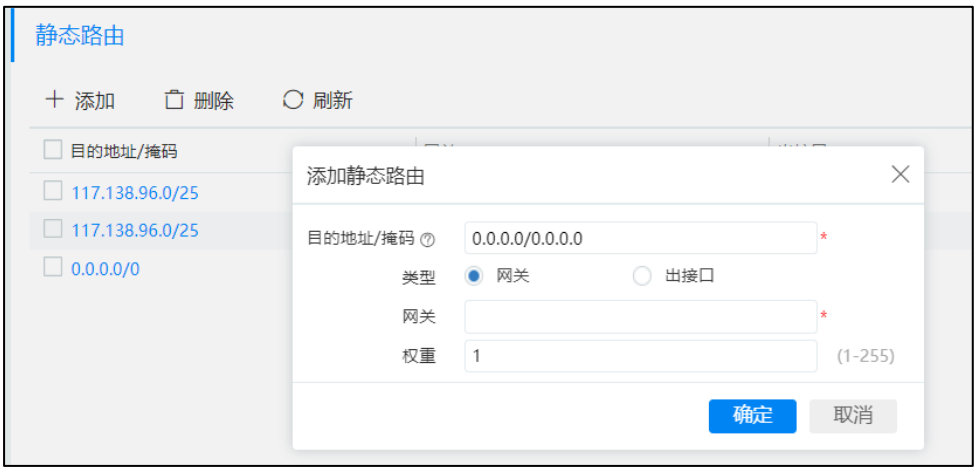
选择【网络配置】>【路由】>【静态路由】。

- 删除“类型”选项。可选择配置网关或出接口或同时配置。
- 增加“路由优先级”参数。
- 增加可靠性检测功能。支持链路健康检查和 BFD 监控。
- 增加“描述”参数。

本版本：



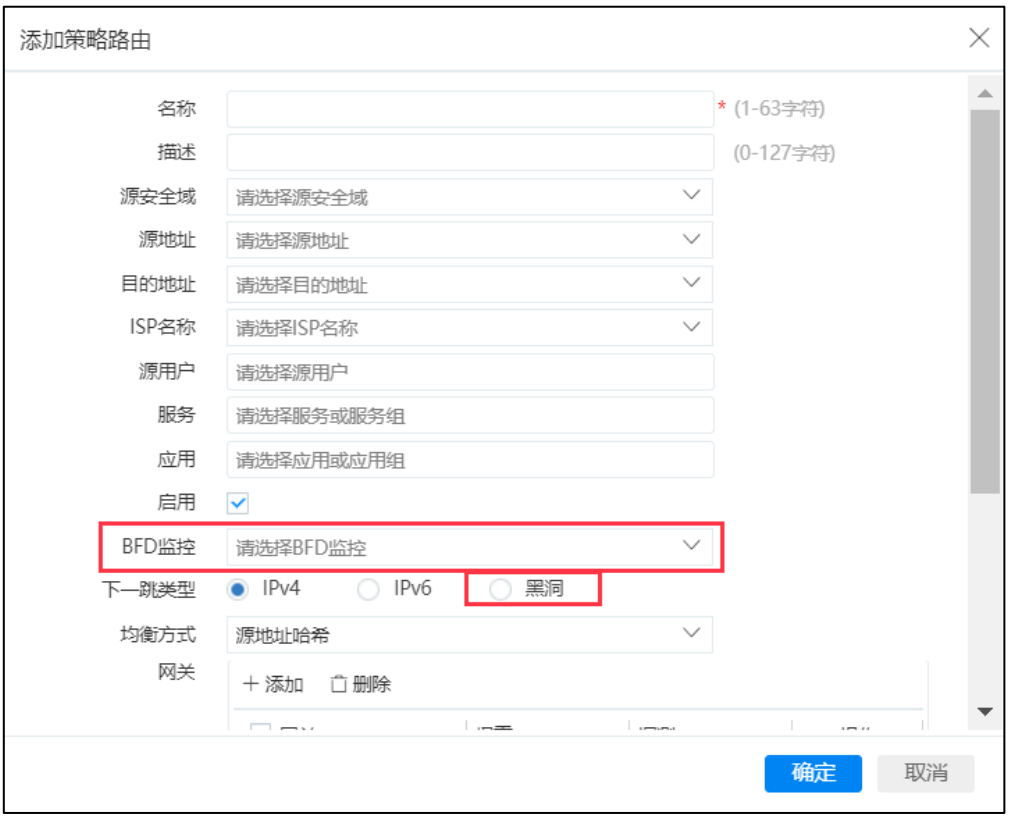
上个版本：



4.11.2 策略路由

选择【网络配置】>【路由】>【策略路由】。

- 新增支持 BFD 监控。
- 下一跳类型新增支持“黑洞”，且【下一跳类型】从原来【均衡方式】下面挪到上面。



4.11.3 RIP

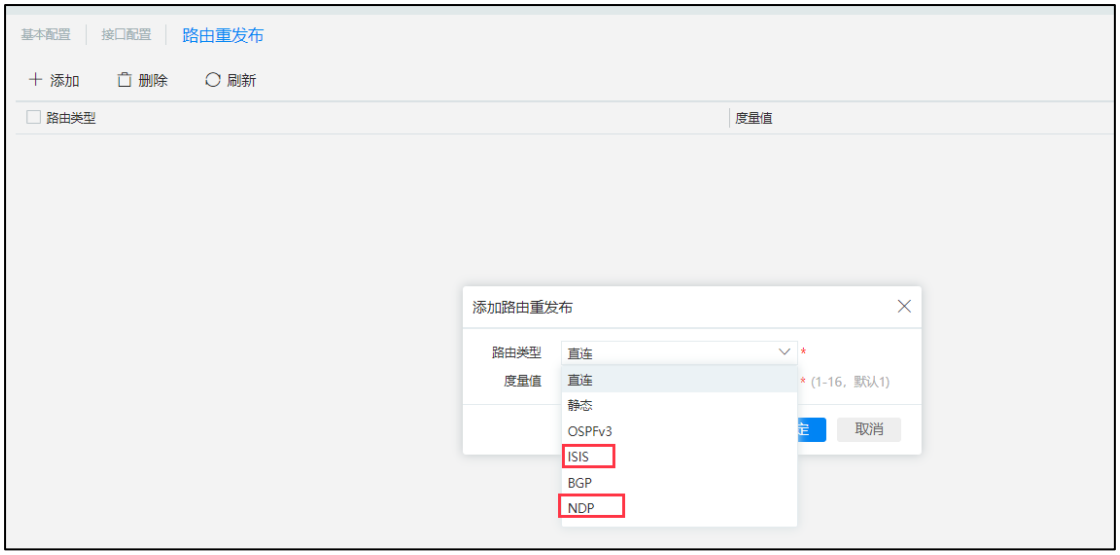
选择【网络配置】>【路由】>【RIP】。

- 基本配置下新增“路由优先级”。
- 路由重发布的路由类型新增“ISIS”和“DHCP”。

4.11.4 RIPng

选择【网络配置】>【路由】>【RIPng】。

- 基本配置下新增“路由优先级”。
- 路由重发布的路由类型新增“ISIS”和“NDP”。

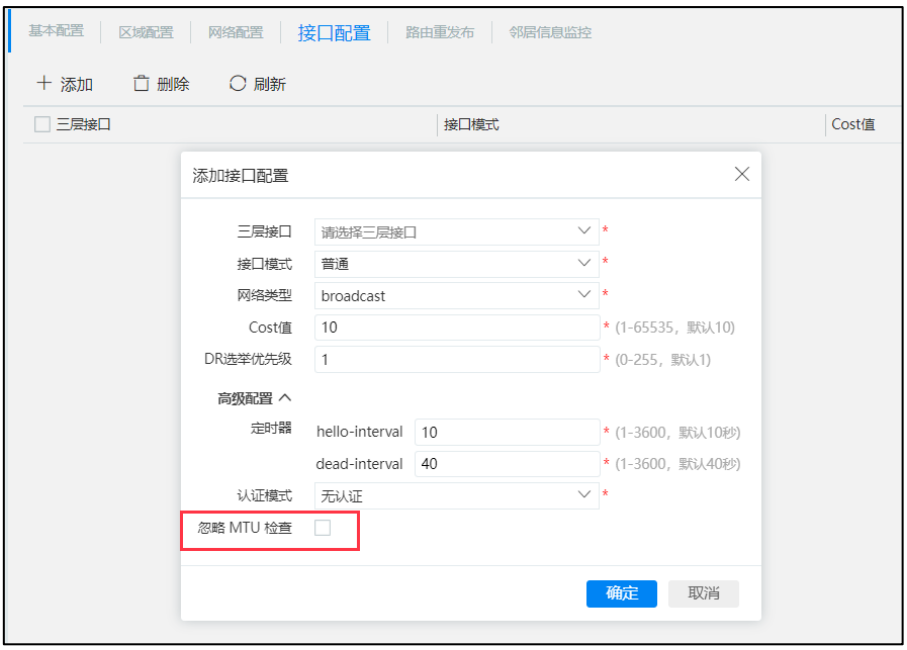


4.11.5 OSPF

选择【网络配置】>【路由】>【OSPF】。

- 基本配置下增加优先级配置。
- 接口配置高级配置下新增“忽略 MTU”功能。
- 路由重发布的路由类型新增“ISIS”、“ENR”和“DHCP”。

基本配置
区域配置
网络配置
接口配置
路由重发布
邻居信息监控
启用OSPF
Router Id
* (IPv4地址形式)
兼容RFC1583
缺省信息发布
域内优先级
100
(1-255 默认100)
域间优先级
110
(1-255 默认110)
ASE优先级
110
(1-255 默认110)
应用
取消

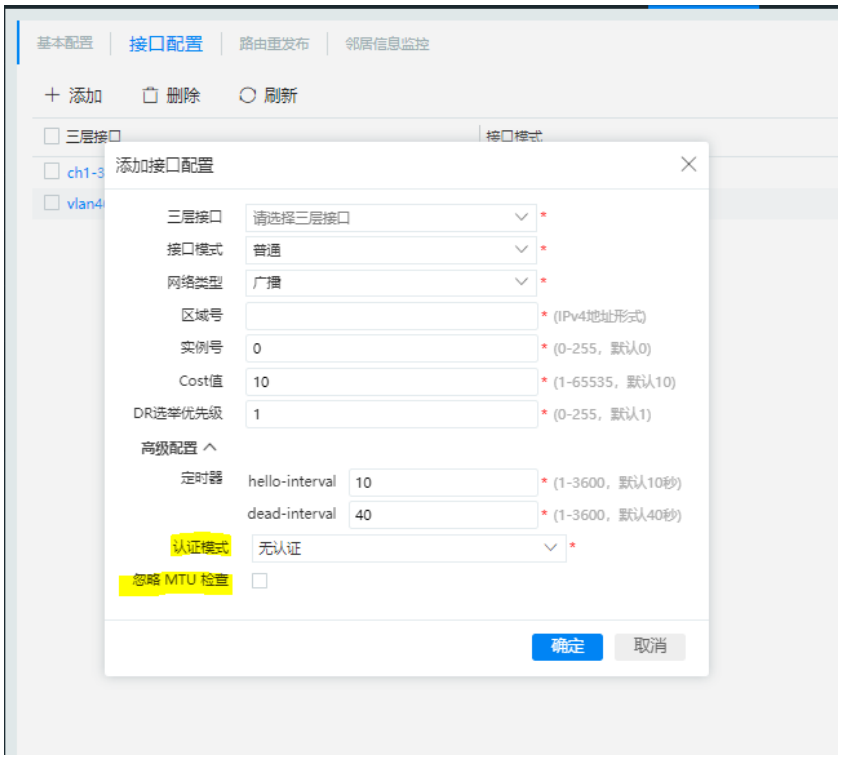

基本配置
区域配置
网络配置
接口配置
路由重发布
邻居信息监控
添加
删除
刷新
三层接口
接口模式
Cost值
添加接口配置
三层接口
请选择三层接口
接口模式
普通
网络类型
broadcast
Cost值
10
(1-65535，默认10)
DR选举优先级
1
(0-255，默认1)
高级配置
定时器
hello-interval
10
(1-3600，默认10秒)
dead-interval
40
(1-3600，默认40秒)
认证模式
无认证
忽略 MTU 检查
确定
取消

基本配置
区域配置
网络配置
接口配置
路由重发布
邻居信息监控
添加
删除
刷新
路由类型
类型
添加路由重发布
路由类型
直连
类型
直连
度量值
静态
(1-1800，默认20)
RIP
BGP
ISIS
ENR
DHCP
确定
取消

4.11.6 OSPFv3

选择【网络配置】>【路由】>【OSPFv3】。本版本变更如下：

- 基本配置新增优先级配置。
- 接口配置高级配置下新增“认证模式”和“忽略 MTU”功能。



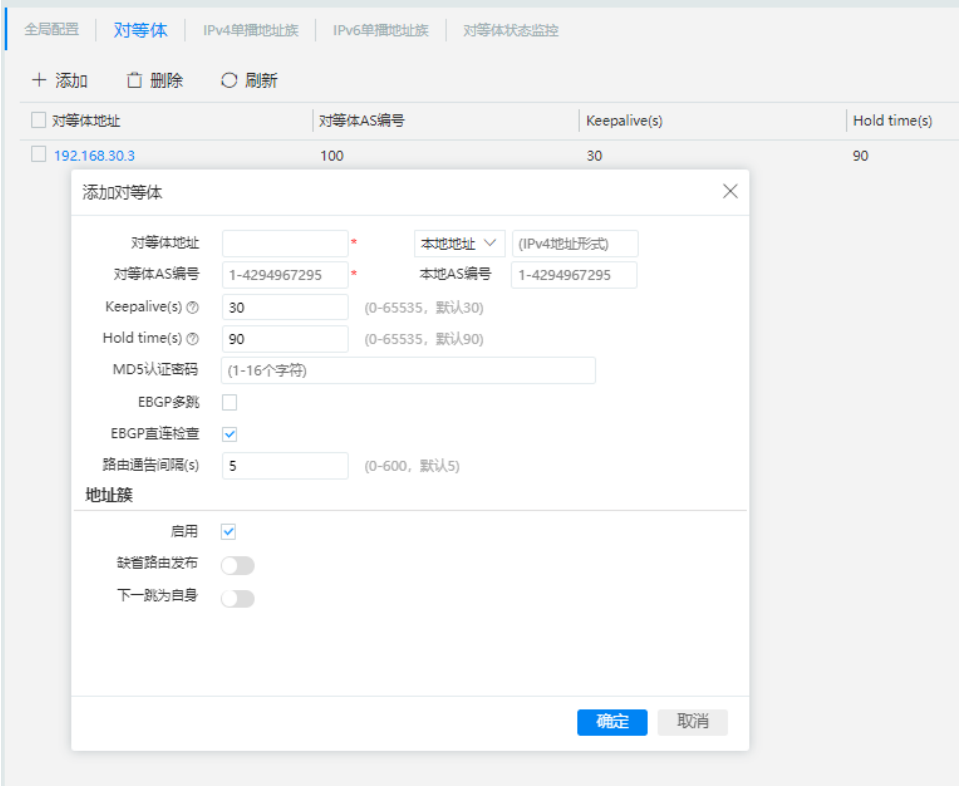
4.11.7 BGP

BGP 功能增强和优化。

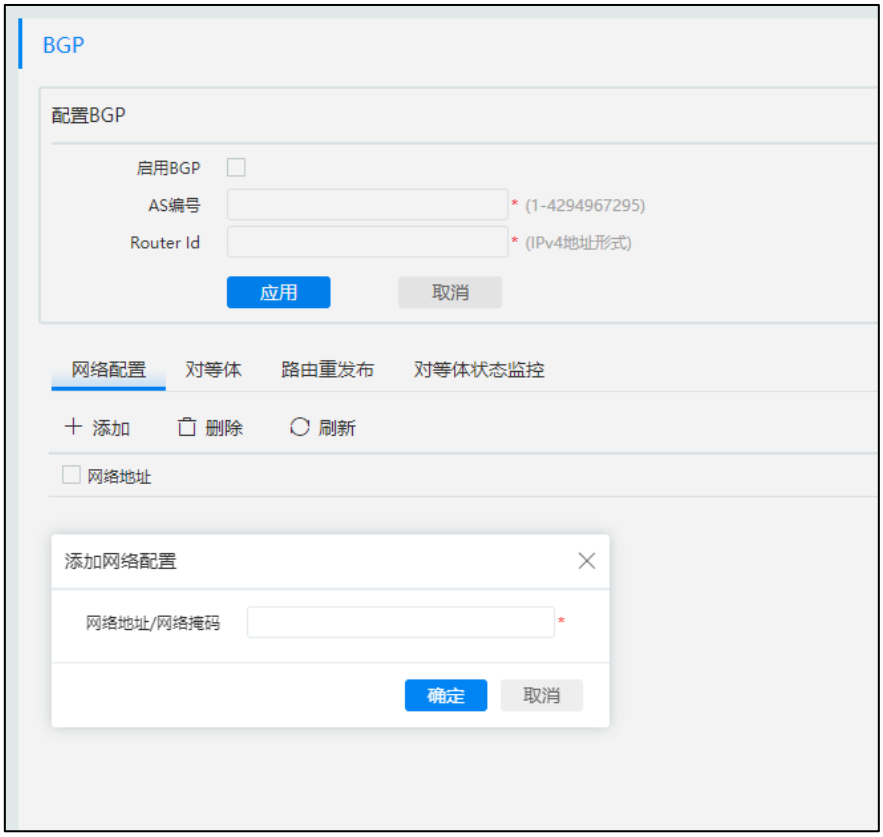
- 全局配置新增支持高级配置支持配置 keepalive 和 holdtime 及本地优先级和路由优先级。
- 对等体配置新增支持 keepalive、holdtime、EBGP 多跳、EBGP 直连检查、路由通告间隔等。
- IPv4 和 IPv6 的网络配置和路由重发布页面分开，分别放入【IPv4 单播地址族】和【IPv6 单播地址族】页面下。
- IPv4 路由重发布新增“DHCP”、“IS-IS”和“ENR”路由类型；IPv6 路由重发布新增“NDP”、“IS-IS”和“ENR”路由类型。

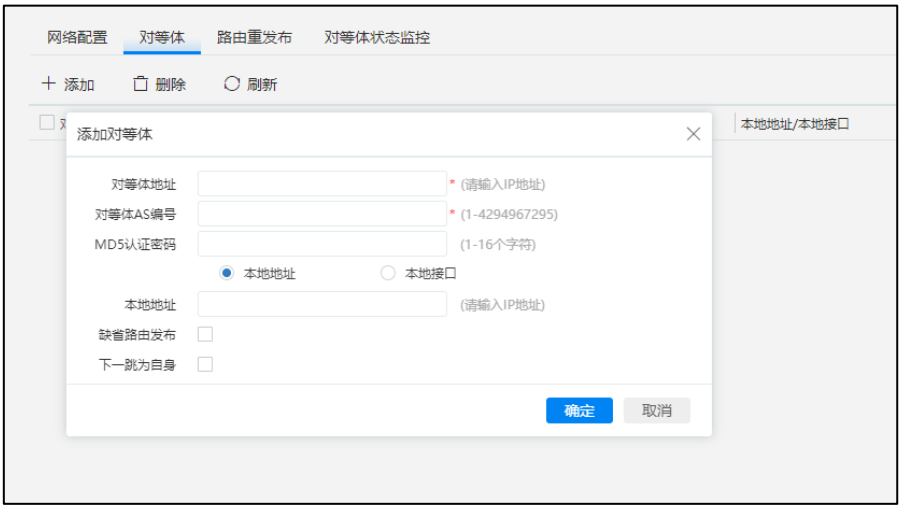
修改后：

全局配置
对等体
IPv4单播地址族
IPv6单播地址族
对等体状态监控
启用BGP
AS编号
200
(1-4294967295)
Router Id
172.24.238.40
(IPv4地址形式)
高级
Keepalive(s)
30
(0-65535，默认30)
Hold time(s)
90
(0-65535，默认90)
本地优先级
100
(0-4294967295，默认100)
MED
路由优先级
EBGP路由
20
(1-255，默认20)
IBGP路由
200
(1-255，默认200)
本地BGP路由
200
(1-255，默认200)
应用
取消


全局配置
对等体
IPv4单播地址族
IPv6单播地址族
对等体状态监控
添加
删除
刷新
对等体地址
对等体AS编号
Keepalive(s)
Hold time(s)
192.168.30.3
100
30
90
添加对等体
对等体地址
本地地址
(IPv4地址形式)
对等体AS编号
1-4294967295
本地AS编号
1-4294967295
Keepalive(s)
30
(0-65535，默认30)
Hold time(s)
90
(0-65535，默认90)
MD5认证密码
(1-16个字符)
EBGP多跳
EBGP直连检查
路由通告间隔(s)
5
(0-600，默认5)
地址簇
启用
缺省路由发布
下一跳为自身
确定
取消

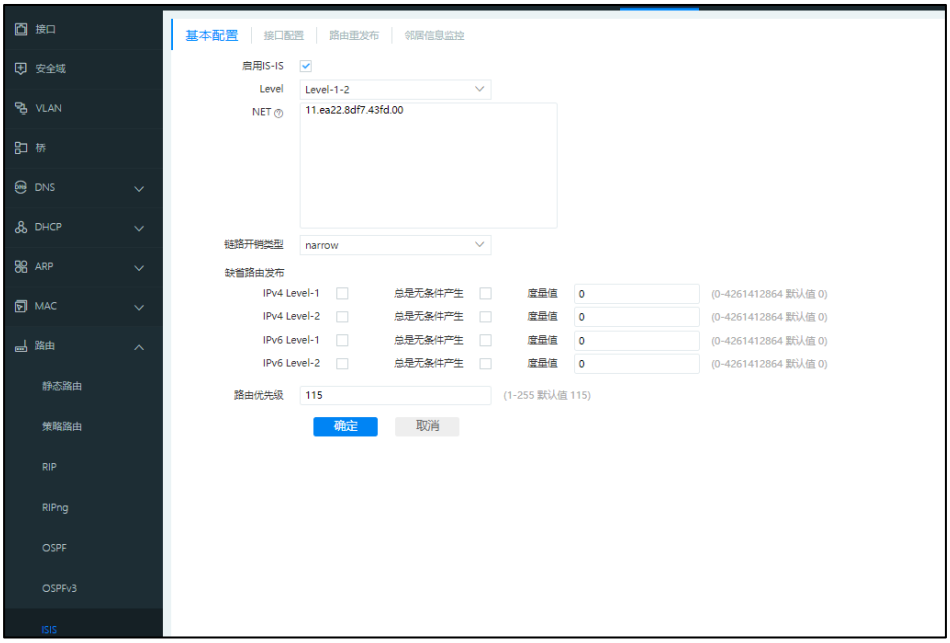
修改前：





4.11.8 IS-IS

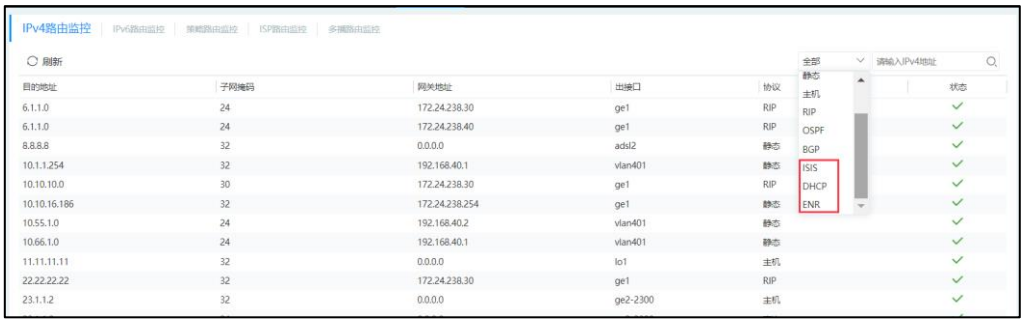
新增 IS-IS 路由。【网络配置】>【路由】下新增 IS-IS 路由。



4.11.9 路由监控

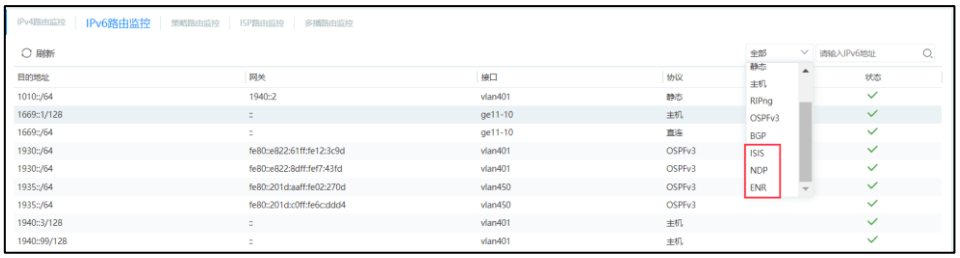
4.11.9.1 IPv4 路由监控

监控的路由新增“ISIS”、“DHCP”和“ENR”。



4.11.9.2 IPv6 路由监控

监控的路由新增“ISIS”、“NDP”和“ENR”。



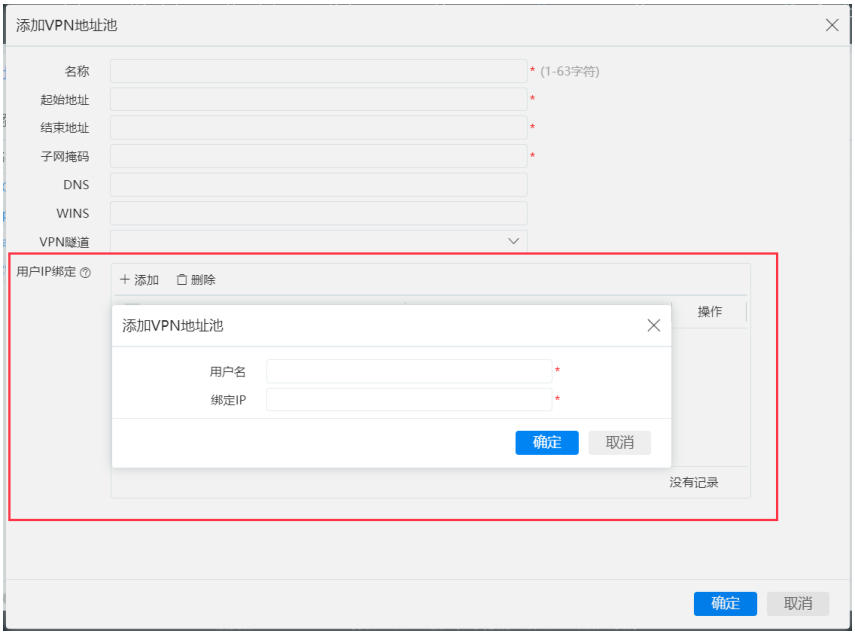
4.11.9.3 策略路由监控

策略路由监控页面新增“BFD 检测”项。

4.12 VPN

4.12.1 VPN 地址池

选择【网络配置】>【VPN】>【VPN 地址池】。添加或编辑 VPN 地址池时新增支持绑定用户功能。



4.12.2 SSL VPN

SSL VPN 客户端新增支持 CentOS 客户端、Ubuntu 客户端和 MACOS 客户端。Window 客户端版本更新。

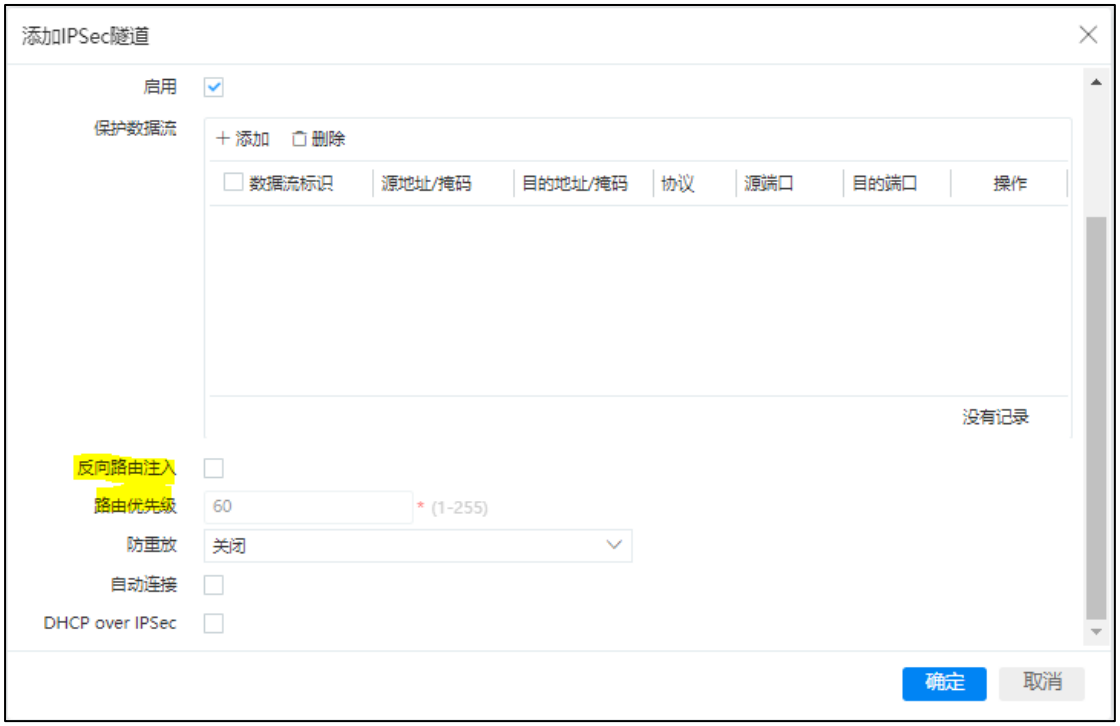
本版本：

R7 版本（上个版本）：

4.12.3 IPSec VPN

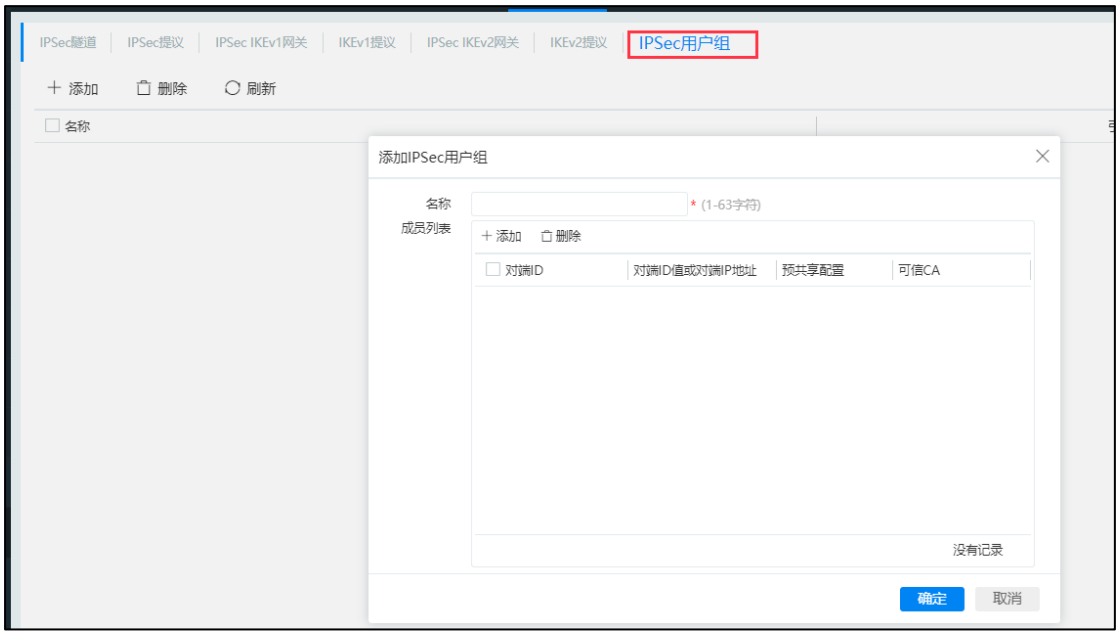
4.12.3.1 IPSec 自动隧道

选择【网络配置】>【VPN】>【IPSec 自动隧道】>【IPSec 隧道】页面，单击【添加】。在【添加 IPSec 隧道】页面新增【反向路由注入】和【路由优先级】。



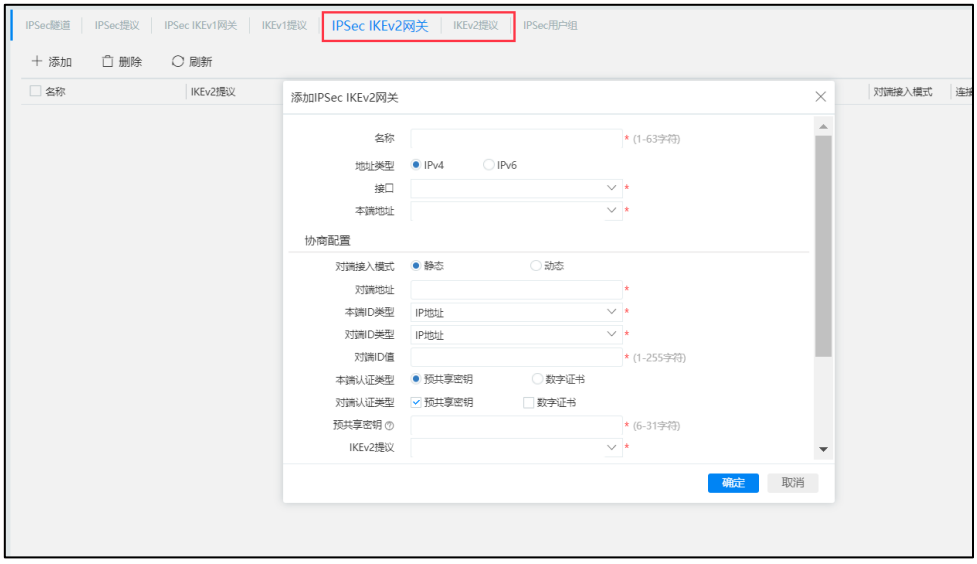
4.12.3.2 IPSec 用户组

1、原【拨号用户组】名称修改为【IPSec 用户组】。涉及修改的包括原【拨号用户组】页面改为【IPSec 用户组】页面。IKE 网关下引用的【拨号用户组】同步修改为【IPSec 用户组】。



4.12.3.3 新增支持 IKEv2

新增 IPSec IKEv2 网关和 IKEv2 提议配置页面。IPSec 隧道配置页面支持选用 IKEv2。



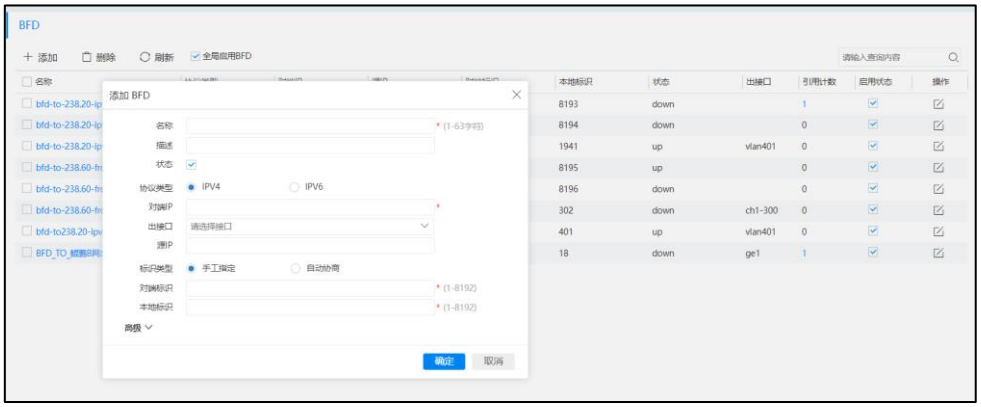
4.13 VXLAN

选择【网络配置】>【VXLAN】，overlay 网络新增支持 IPv6。

4.14 BFD

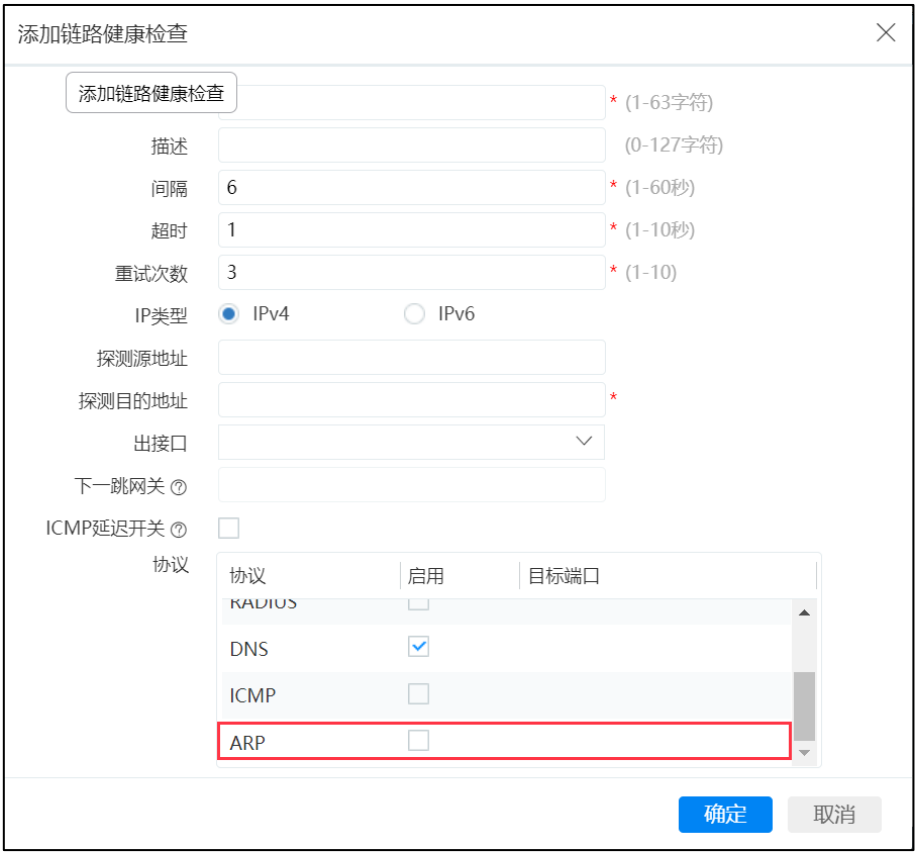
【网络配置】下新增【BFD】。

BFD 支持与静态路由、策略路由以及 HA 等进行联动，可以用来快速检测网络通信故障，以便及时切换路由或主备切换，保证业务不中断，提高系统的可用性。



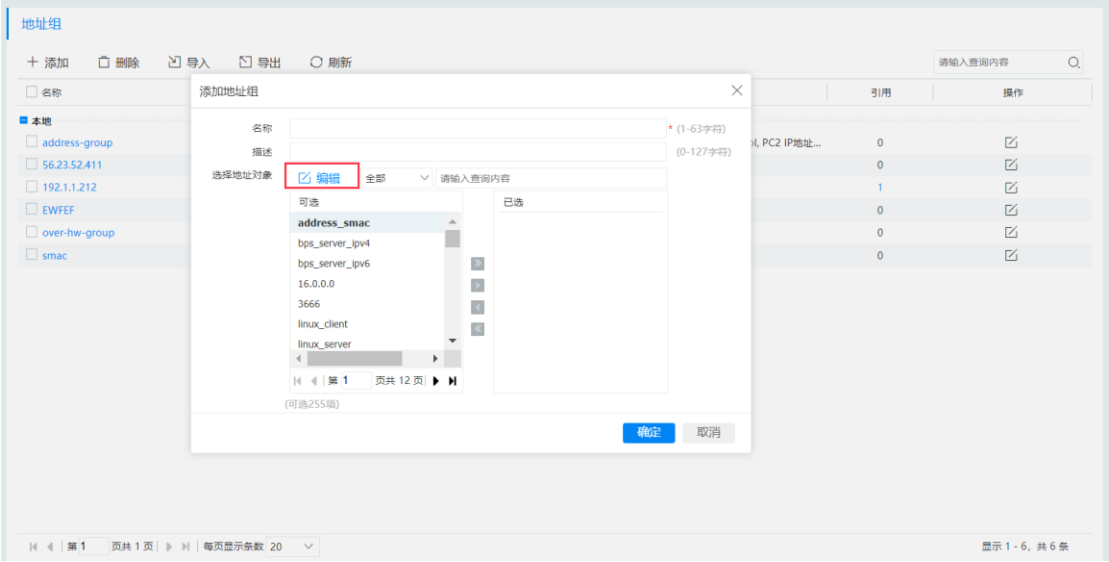
4.15 链路健康检查

选择【网络配置】>【链路健康检查】，添加或编辑链路健康检查页面，协议新增 ARP 协议。



4.16 地址组

选择【对象配置】>【地址】>【地址组】，添加或修改地址组时，新增支持编辑选中的地址对象或地址组。

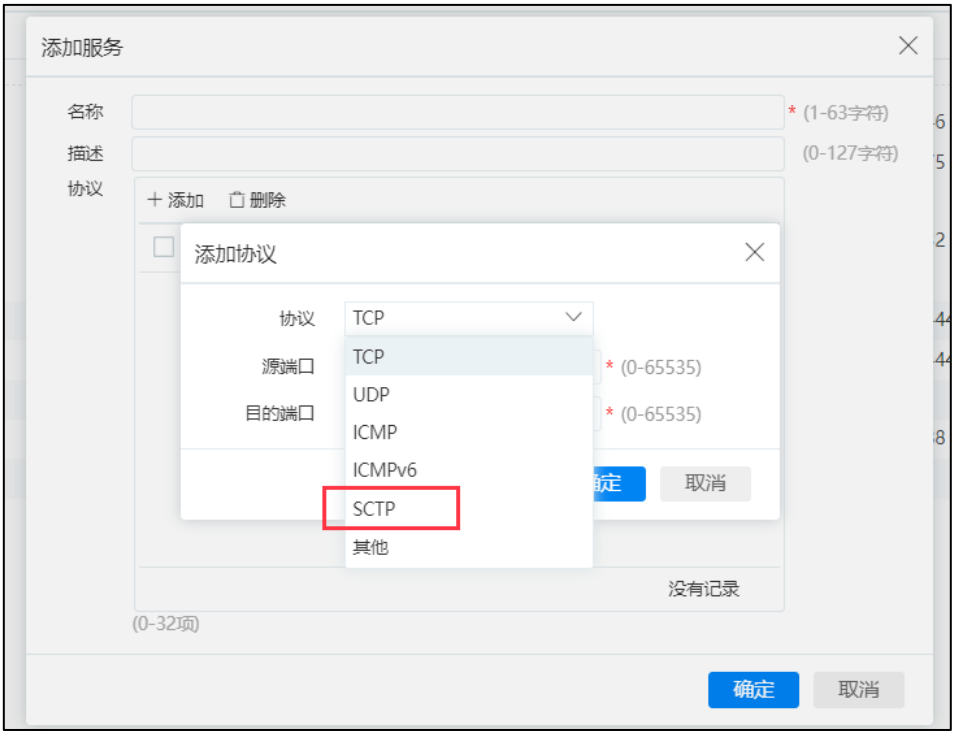


4.17 服务

4.17.1 服务

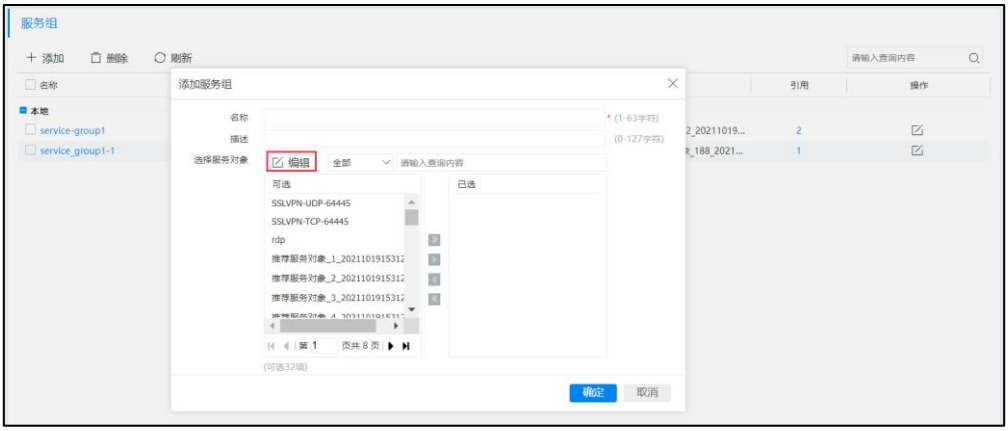
选择【对象配置】>【服务】>【服务】。

- 预定义服务新增一个，由 55 个变为 56 个。
- 自定义服务的协议新增支持“SCTP”。



4.17.2 服务组

选择【对象配置】>【服务】>【服务组】，添加或修改服务组时，新增支持编辑选中的服务对象或服务组。

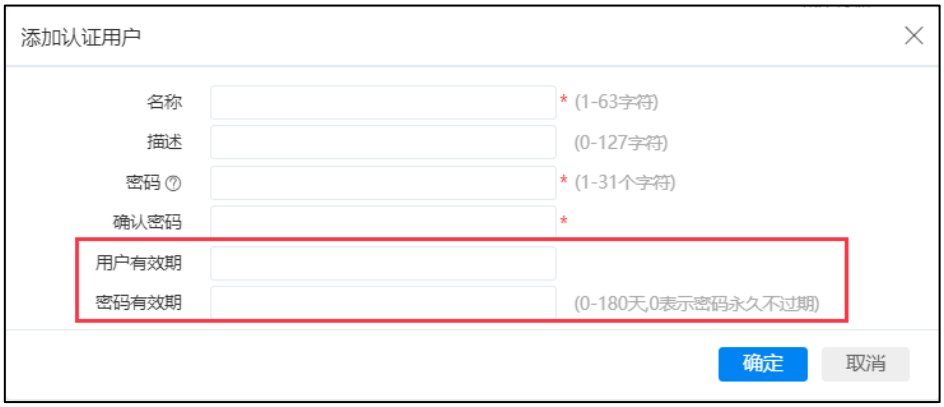


4.18 用户

4.18.1 用户

选择【对象配置】>【用户】>【用户】，添加或编辑用户时，新增“密码有效期”，原有效期改为“用户有效期”。

修改后：



修改前：

4.19 URL

- URL 库中增加云端库中的 URL 规则（5 万条）。
- 自定义 URL 规格从 16 条增加到 64 条。

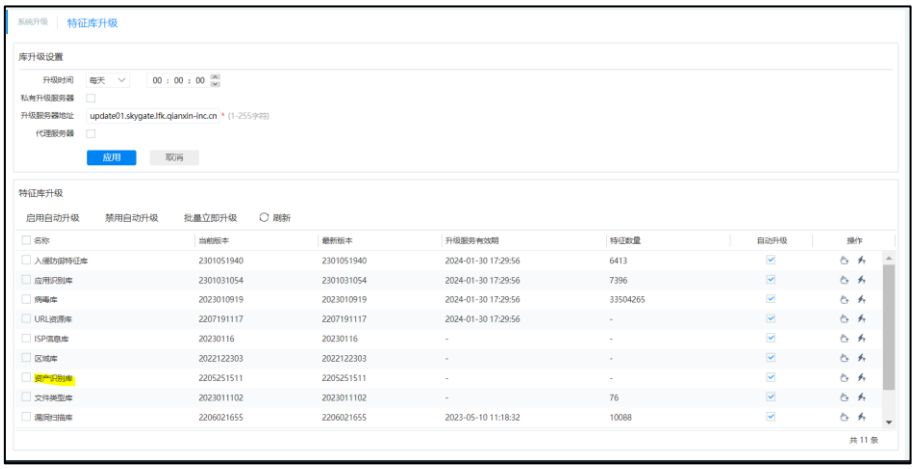
4.20 资产识别

4.20.1 资产指纹库升级

资产指纹库升级的位置由【对象配置】>【资产管理】>【资产指纹库】，调整到【系统】>【升级管理】>【特征库升级】下。

资产指纹库除了支持手工升级，新增支持在线自动升级、在线立即升级。

修改后：



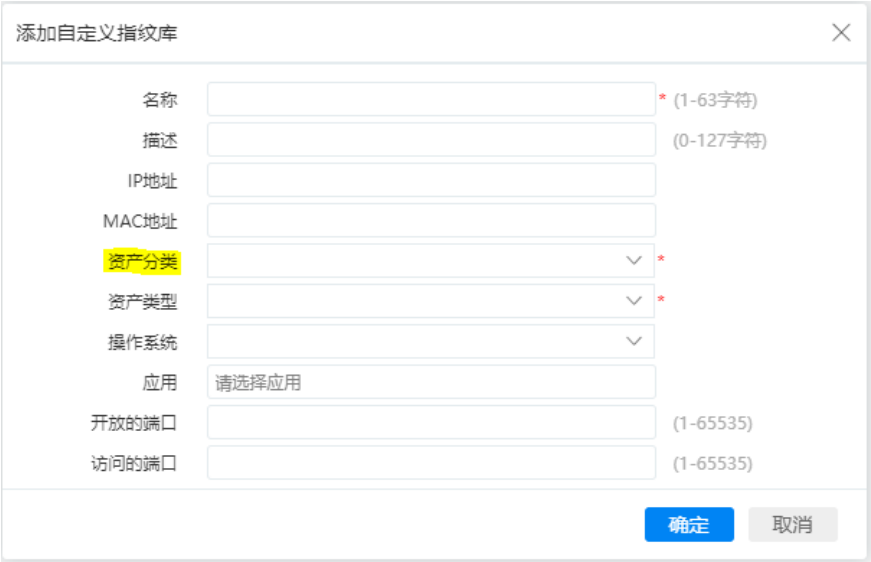
修改前：

4.20.2 自定义资产指纹库

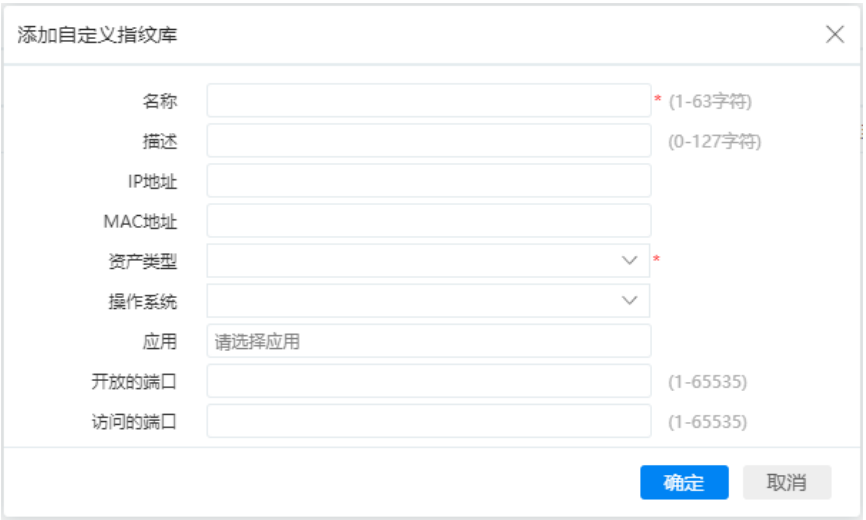
选择【对象配置】>【资产管理】>【资产指纹库】，变更如下：

- 自定义指纹库时新增【资产分类】参数。
- IP 地址新增支持 IPv6。

修改后：



修改前：



4.21 反病毒

4.21.1 新增支持 IPTUX 协议

选择【对象配置】>【安全配置文件】>【反病毒】，在【反病毒】页面单击【添加】。【添加反病毒】页面应用解码的协议新增 IPTUX。通过 IPTUX 上传和下载的文件都可以进行反病毒检测。

4.21.2 新增病毒样本上传

选择【对象配置】>【安全配置文件】>【反病毒】，新增【病毒样本上传】。

支持将检测到的病毒样本上传到 FTP 服务器存储。

4.22 漏洞防护和防间谍软件

4.22.1 IPS 引擎优化

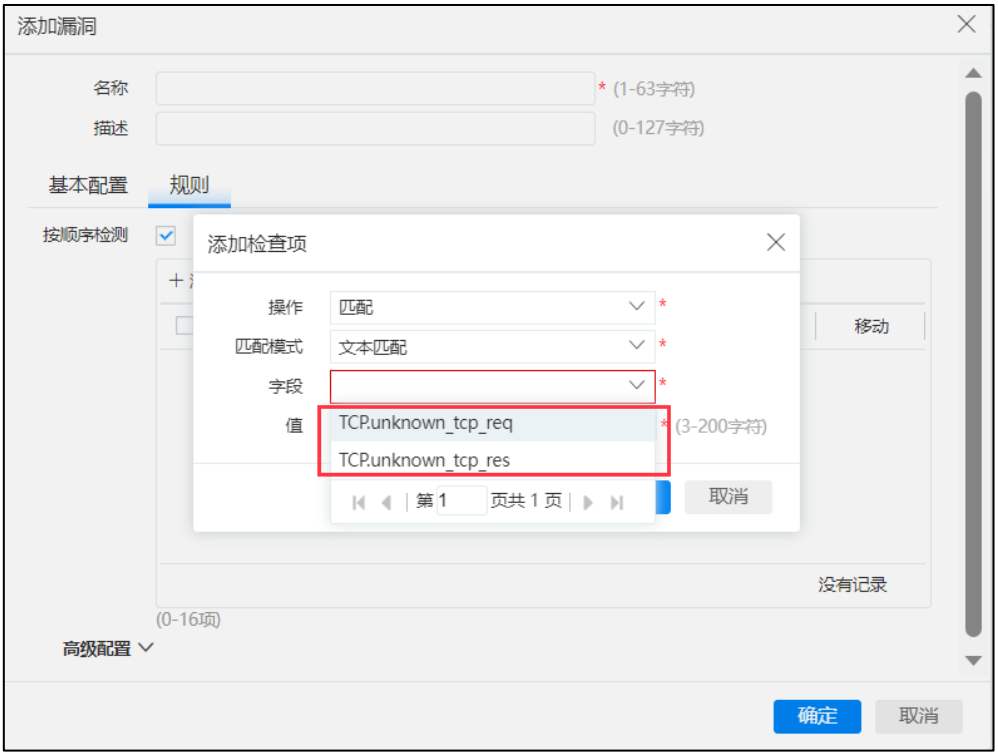
IPS 引擎优化，提高 IPS 引擎检出率。包括：

- 合入 uri 逃逸
- ftp 的 data 超过 4M，只送前 4M 到 ips 扫描；
- 扩大 IPS 引擎报文扫描支持的协议范围，包括新增支持常见邮件协议，HTTP 协议多个单独字段的扫描
- 修改 http req content_length 的判断
- 修改应用最大限制长度
- 控制 url 逃逸判断逻辑
- 增加 ftp 端口异常扫描
- 修改跨包计数逻辑
- 特定下数据不进行 ips、av 处理
- 扩大 MD5 数目范围
- 添加 session 结束与 len 为 0 情况病毒查杀
- 更新固定长度与自学习 bypass
- 报文解压缩功能增强
- 逃逸防御增强
- 优化并发性能
- 新增 IPS 检测增强功能开关
- 合入应用异常方向检测开关，默认关闭。

4.22.2 TCP/UDP 协议检测深度定制

新增针对 TCP/UDP 协议检测深度定制需求。

选择【对象配置】>【自定义签名】>【漏洞】或【对象配置】>【自定义签名】>【间谍软件】，当【基本配置】的协议选择“TCP”或“UDP”时，新增规则时【操作】下拉菜单增加“小于”、“大于”、“等于”，当选择“小于”、“大于”、“等于”任意一个时，配置增加包括“TCP.tcp_req_len”、“TCP.tcp_res_len”或“UDP.udp_req_len”、“UDP.udp_res_len”选项。

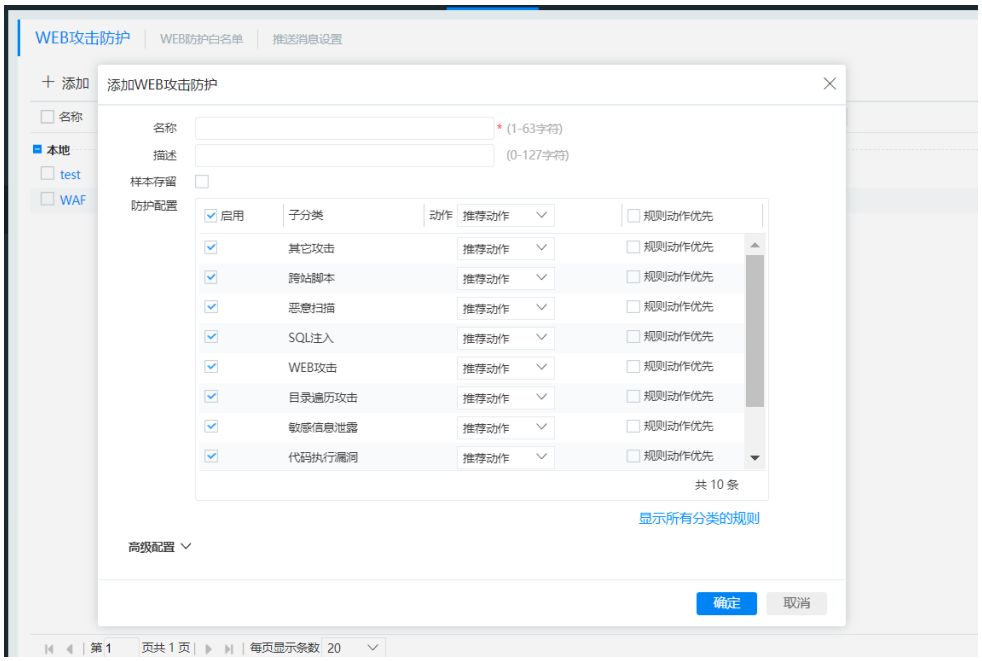


4.23 Web 攻击防护

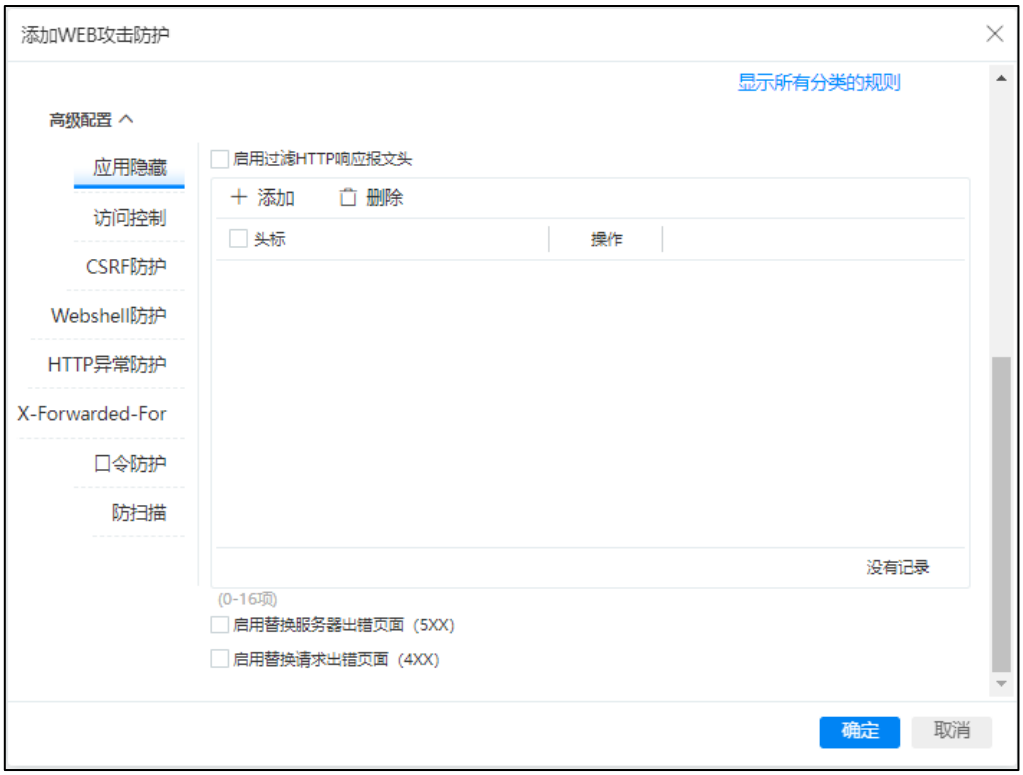
【对象配置】>【安全配置文件】下新增【WEB 攻击防护】菜单。

Web 攻击防护为 WAF（Web Application Firewall）功能。通过执行一系列针对 HTTP/HTTPS 的安全策略来专门为 web 应用提供保护。专门用于解决 Web 应用安全问题，包括 SQL 注入、网页篡改、网页挂码等。Web 攻击防护对来自 Web 应用程序客户端的各种请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站站点进行有效保护。

SecGate 3600 防火墙支持常见的多种 web 防护应用规则，同时支持“隐藏应用”、“URL 访问控制”、“CSRF 防护”、“Webshell 防护”、“HTTP 异常防护”、“X-Forwardde-For”、“口令防护”和“防扫描”。

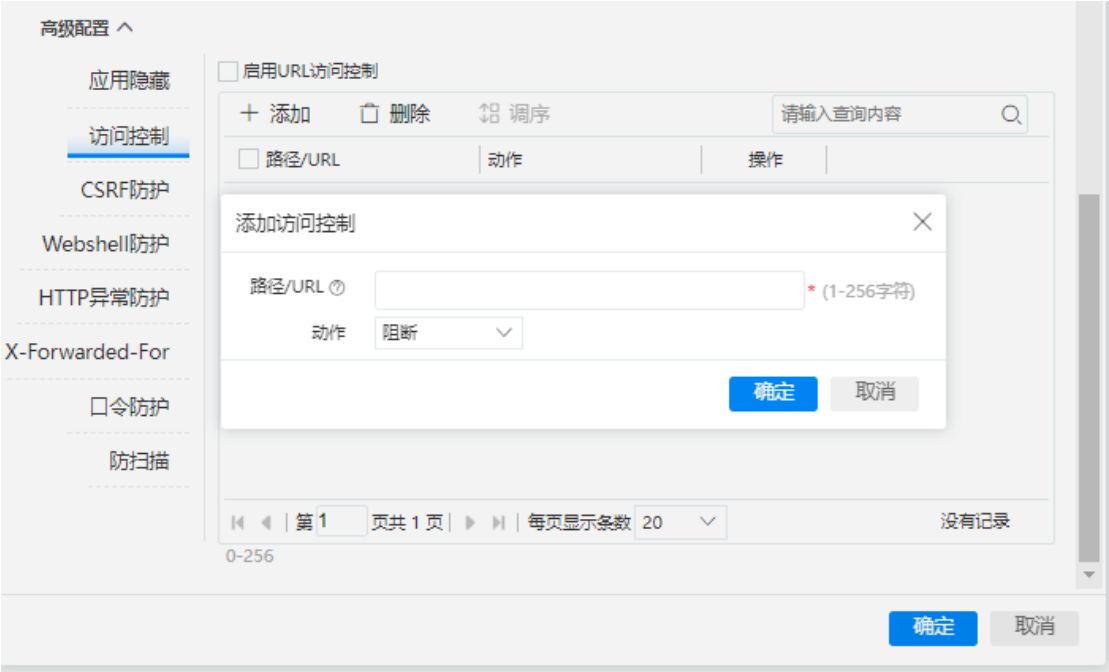


应用隐藏支持屏蔽 HTTP 头部的 Server 字段和 X-powered-By 字段，还支持自定义屏蔽字段。应用隐藏同时还支持对 5XX 和 4XX 错误码的检查和替换。

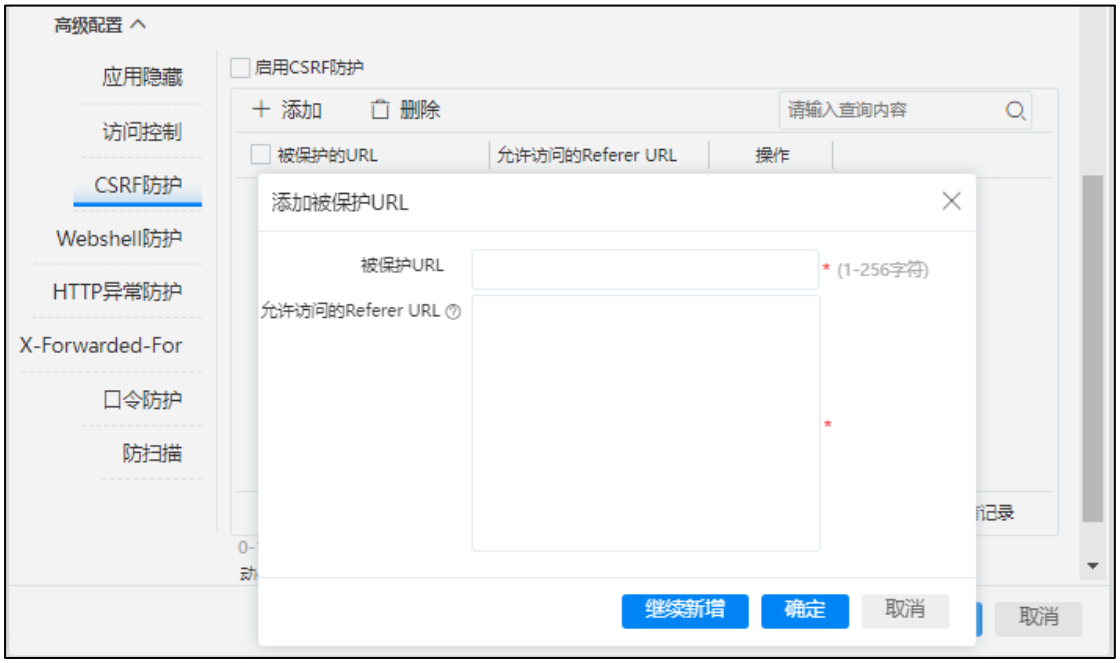


访问控制支持配置放行的 URL 允许访问，配置阻断的 URL 拦截。同时只

会命中优先级最高的一条策略。



防火墙通过设置被保护的 URL 及允许访问的 Referer URL，可以有效防止网站受到 CSRF 攻击。



WebSHell 支持黑名单模式和白名单模式。黑名单模式匹配列表中的文件格式

的数据包执行日志记录或阻断；白名单模式仅允许列表中的文件格式的文件上传，根据动作执行日志记录或阻断。

HTTP 异常防护支持进行 Accept-Charset 重复检测，Content-Type 重复检测、Content-Length 字段值检测、URL 长度异常检测和 HTTP 头部中字段长度异常检测。

XFF 的实现方式变化。新的版本下在 web 攻击防护下实现。原来的 URL 下的开关删除。

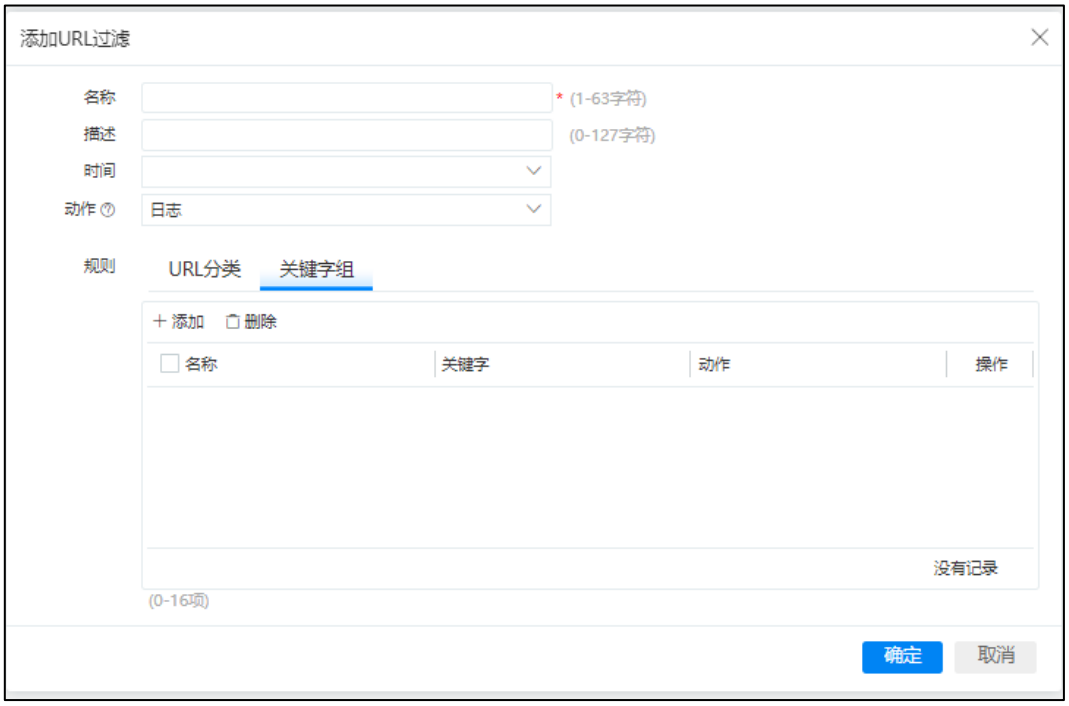
口令防护利用 HTTP 认证失败的报文特征对口令进行防暴力破解。

防扫描支持 302 页面防扫描、404 页面防扫描和目录访问频率检测。

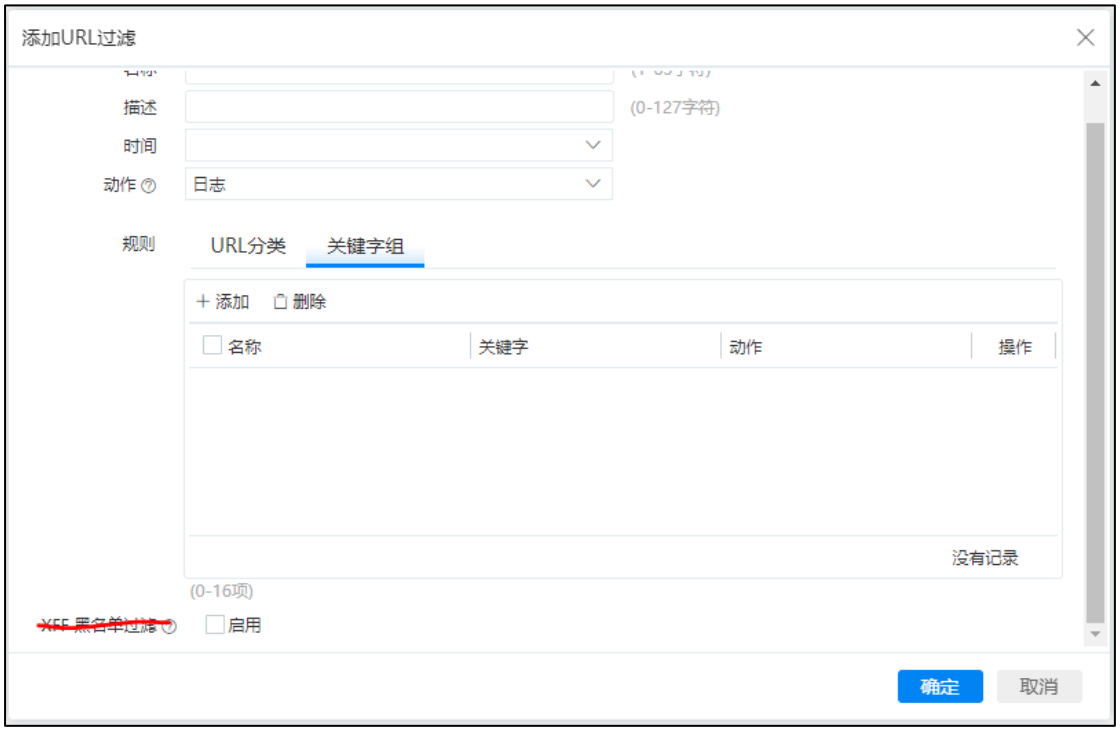
4.24 URL 过滤

选择【对象配置】>【安全配置文件】>【URL 过滤】。URL 过滤下删除 xff，该功能改为在 web 攻击防护下实现。

修改后：



修改前：



4.25 文件过滤

选择【对象配置】>【安全配置文件】>【文件过滤】。

文件过滤支持的应用下删除了“中华论坛网”。

4.26 内容过滤

选择【对象配置】>【安全配置文件】>【内容过滤】。

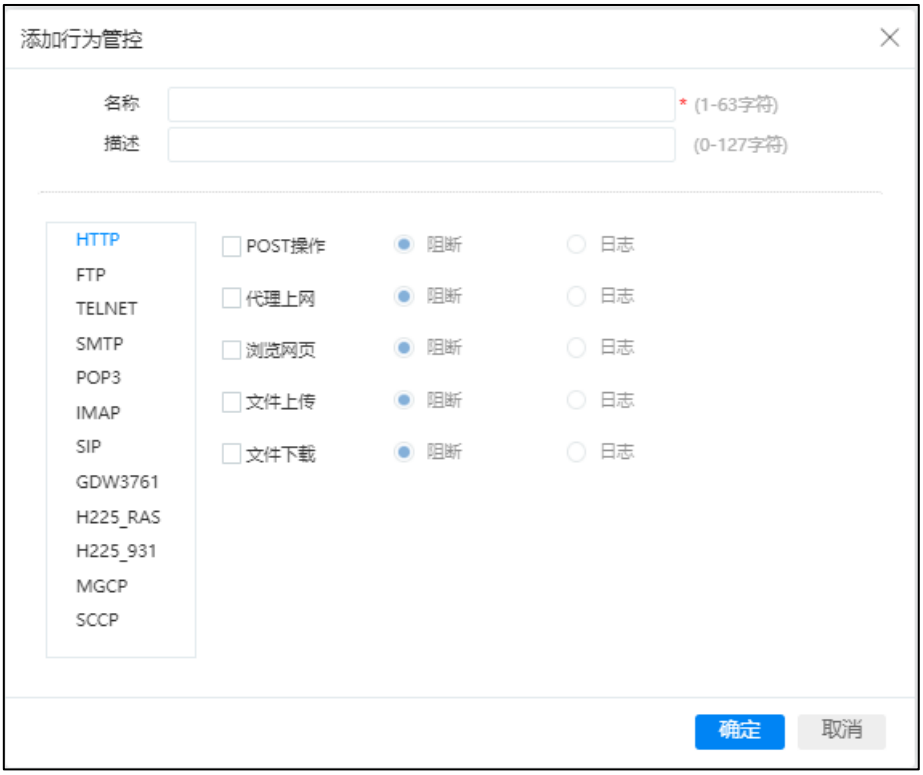
内容过滤支持的应用下删除了“中华论坛网”。

4.27 行为管控

选择【对象配置】>【安全配置文件】>【行为管控】。行为管控页面变化如下：

- 新增 SIP、H225-RAS、H225-931、MGCP、SCCP 协议等 VOIP 行为管控。
- 新增电网 GDW3761 协议行为管控。
- 新增 FTP、TELNET、SMTP、POP3、IMAP 数据库弱口令检测。

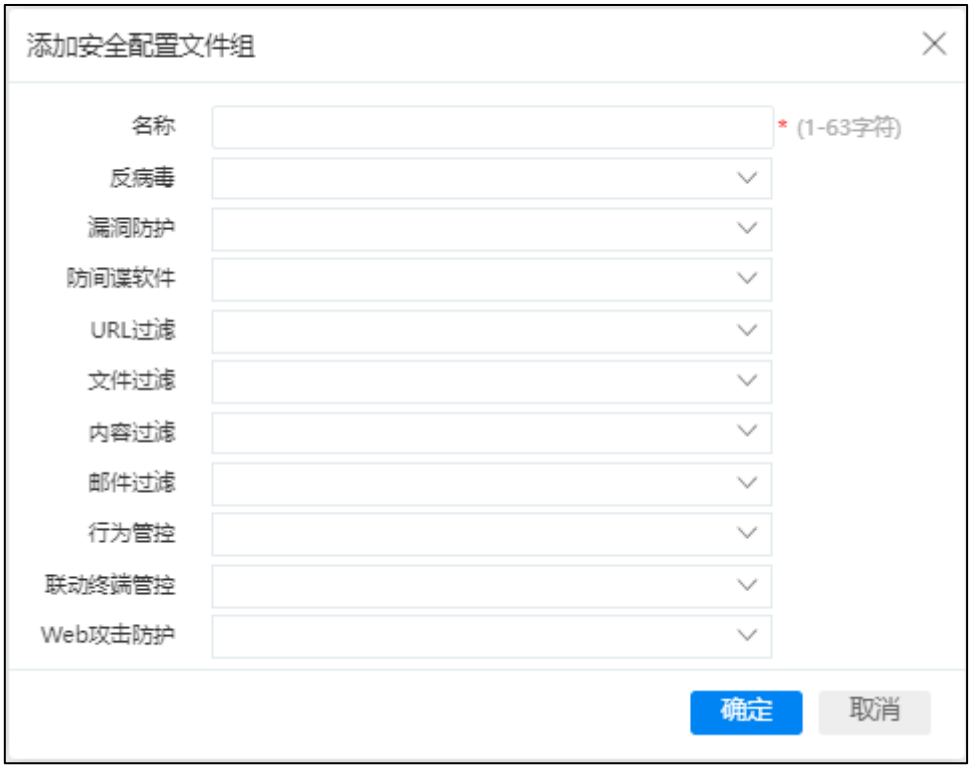
修改后：



修改前：

4.28 安全配置文件组

安全配置文件组新增“web 攻击防护”。

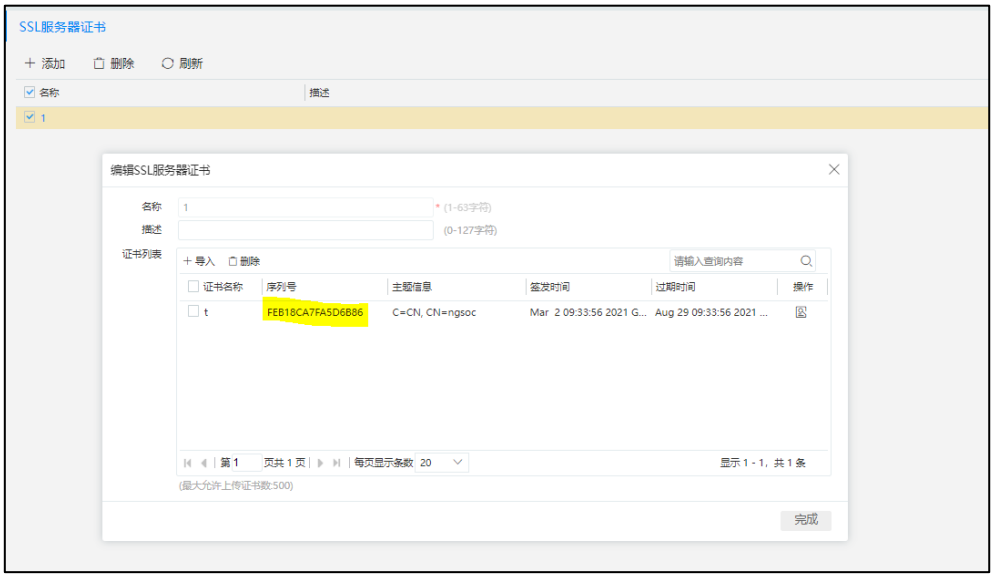


4.29 SSL 解密配置文件

选择【对象配置】>【安全配置文件】>【解密配置文件】。

4.29.1 SSL 服务器证书

SSL 服务器证书功能支持显示导入证书序列号，支持基于序列号查找证书。



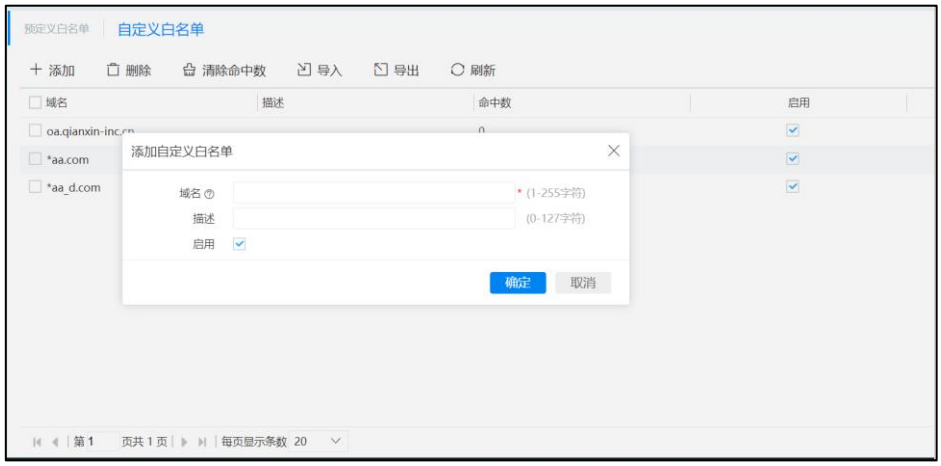
4.29.2 SSL 代理白名单

本版本 SSL 代理白名单支持预定义白名单和自定义白名单。

系统内置了 100 多条确认为正规的金融机构的域名，对这些预定义 SSL 代理白名单，默认不解密。

支持单独启动每条预定义和自定义白名单。

修改后：



修改前：

4.29.3 SSL 解密证书

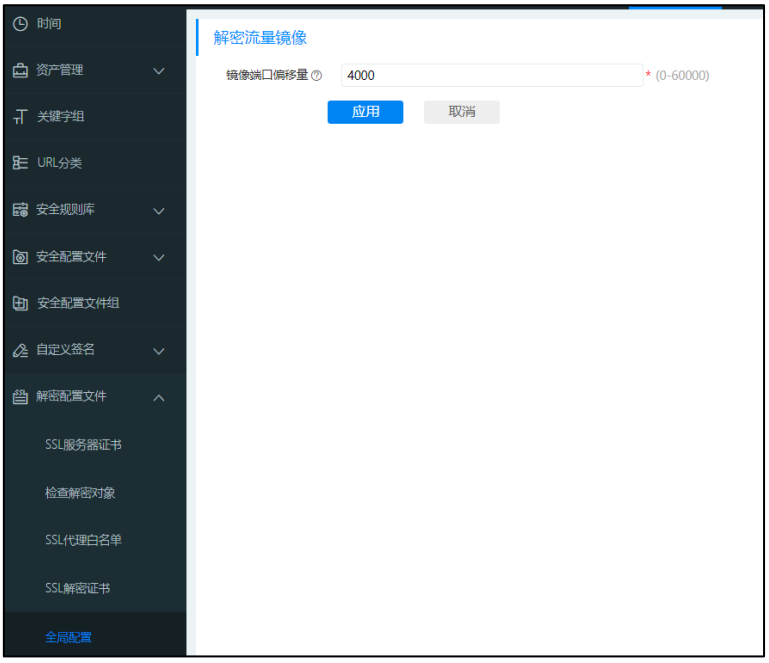
- 新增【恢复转发根证书】按钮，支持恢复默认的转发根证书。
- 转发根证书页面新增【下载 URL】展示区域，支持复制连接。

修改后：

修改前：

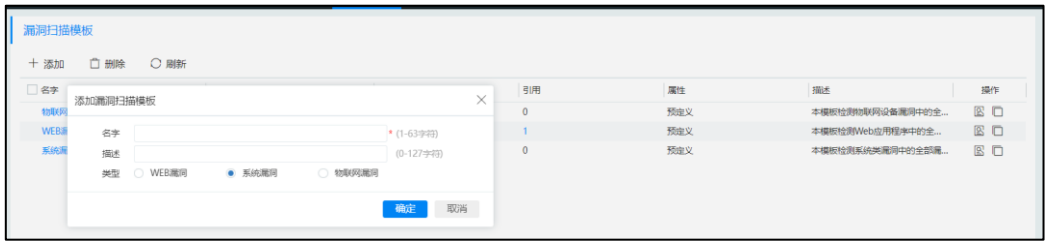
4.29.4 SSL 全局配置

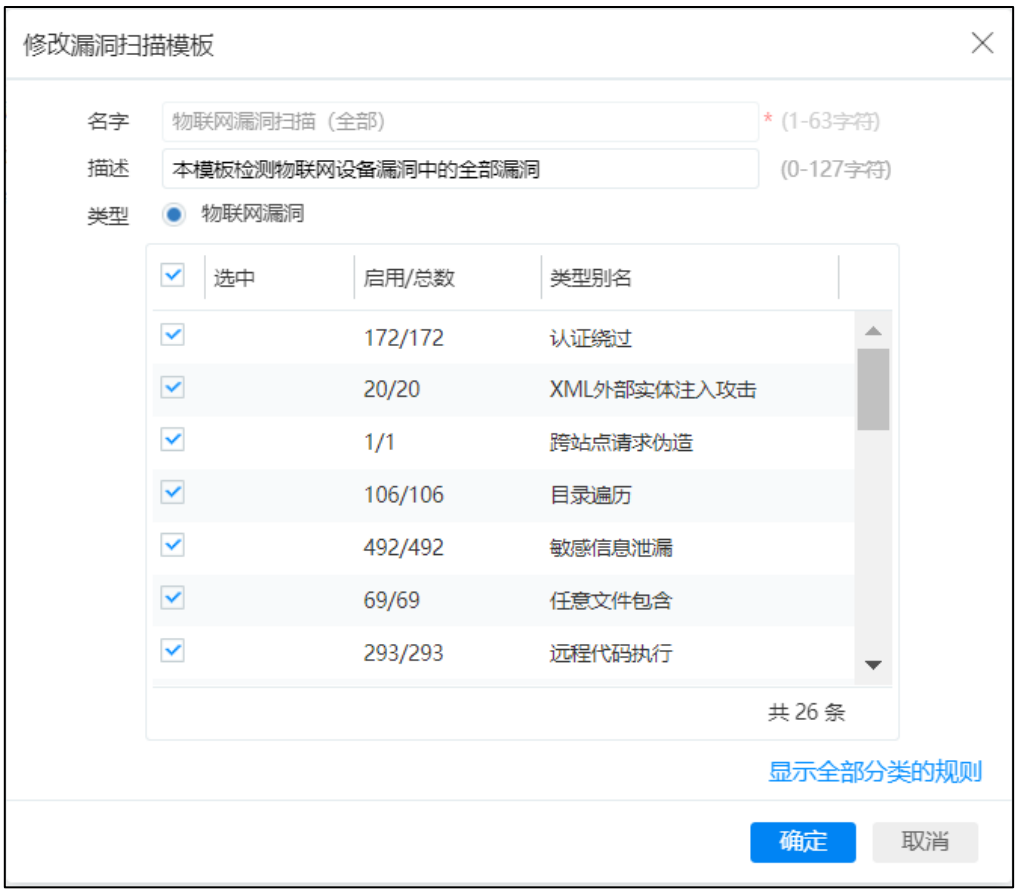
【对象配置】>【解密配置文件】下新增 SSL 解密全局配置，支持配置解密流量镜像的端口偏移量。



4.30 漏洞扫描模板

选择【对象配置】。新增【漏洞扫描模板】，支持三种漏洞扫描模板。

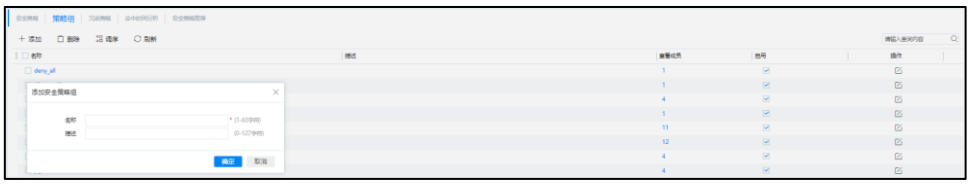




4.31 安全策略

4.31.1 策略组

【策略配置】>【安全策略】下新增【策略组】。策略组支持添加、删除、编辑和调序。



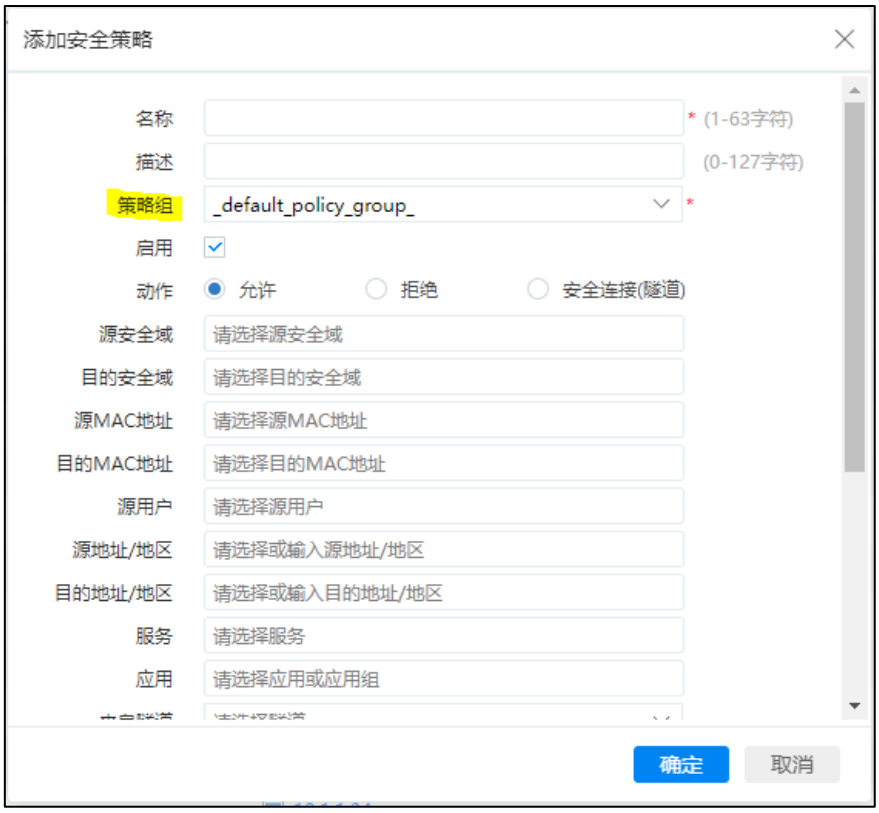
4.31.2 安全策略

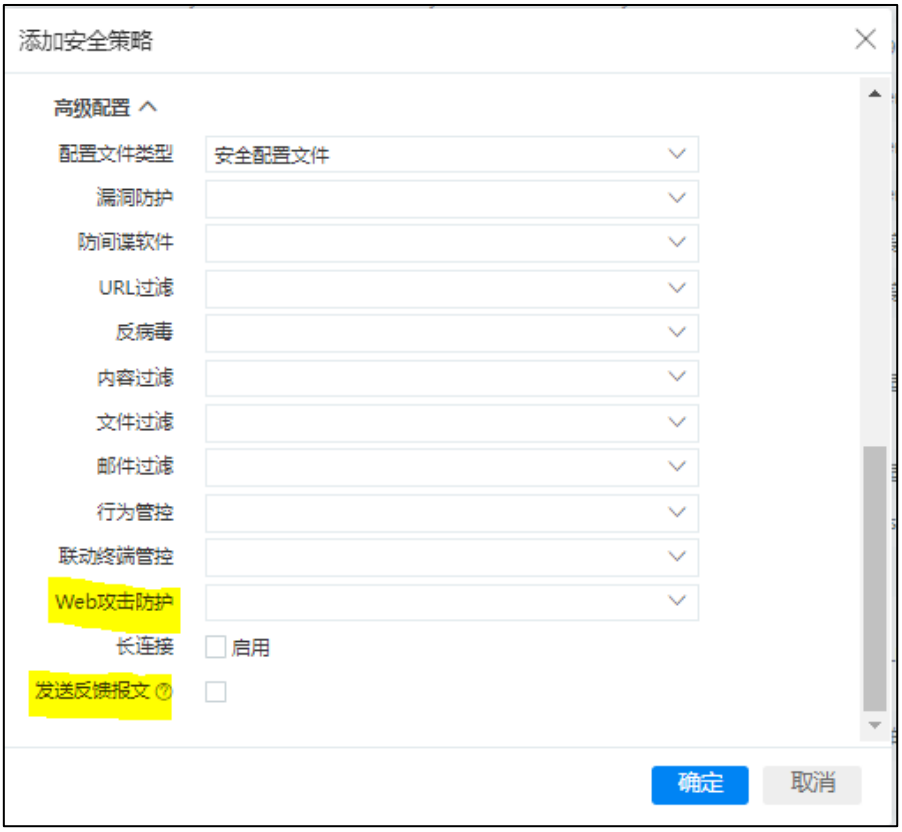
新增支持将安全策略加入策略组进行分组管理。

可选择安全配置文件新增支持 Web 攻击防护。

新增支持发送反馈报文。选中【发送反馈报文】复选框后，启用发送反馈报文功能。当安全策略动作为阻断时，针对不同的报文类型发送对应的反馈报文。针对 TCP 报文反馈 Reset 报文，针对 UDP、ICMP 报文反馈 ICMP 不可达报文。

修改后：





4.31.3 冗余策略

新增 ▷ 完全冗余分析 和 ▷ 部分冗余分析 ，单击相应按钮后会进行相应的分析。

修改后：

修改前：

4.32 NAT 策略

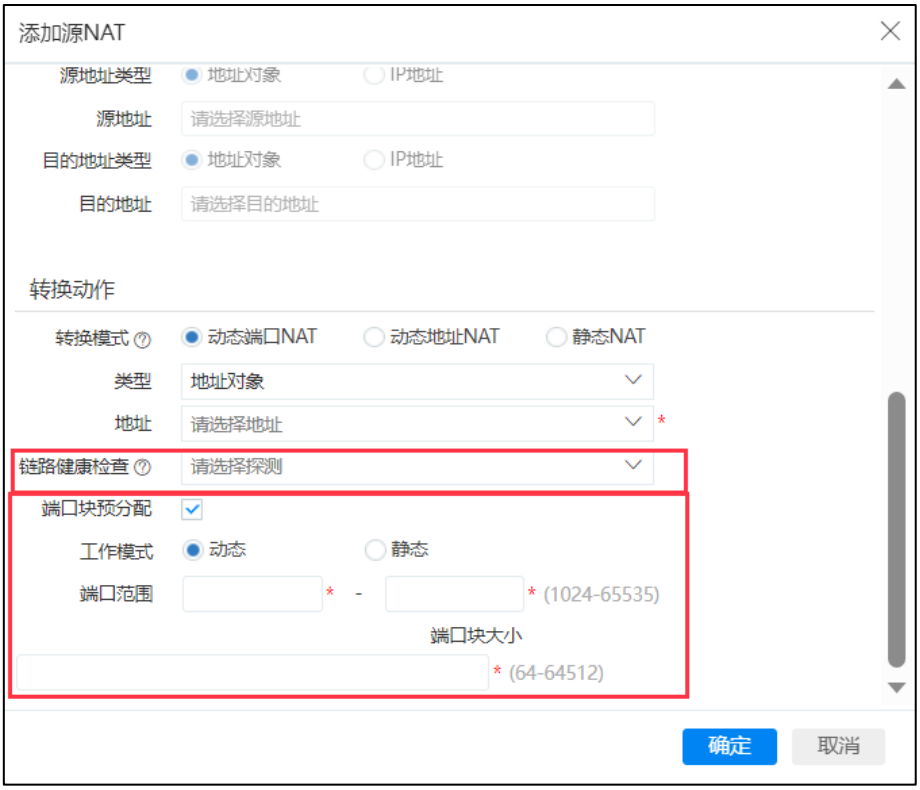
4.32.1 源 NAT

- 源 NAT 新增支持基于时间进行转换前匹配。
- 新增 NAT 防封杀。

  仅转换模式为“动态端口 NAT”，地址类型为 IP 地址或者地址对象时，支持引用“链路健康检查”，对 NAT 地址池地址进行多源地址探测，验证失败的源地址从 NAT 地址池中剔除，验证成功的源地址继续保留在 NAT 地址池中。

- 新增支持 NAT444“端口块预分配”。

  配置探测功能时，不支持地址组。
  仅转换模式为“动态端口 NAT”，地址类型为 IP 地址或者地址对象时，支持端口块预分配。端口块预分配适用于 NAT444 场景下 CGN 配置，工作模式支持“动态”和“静态”。

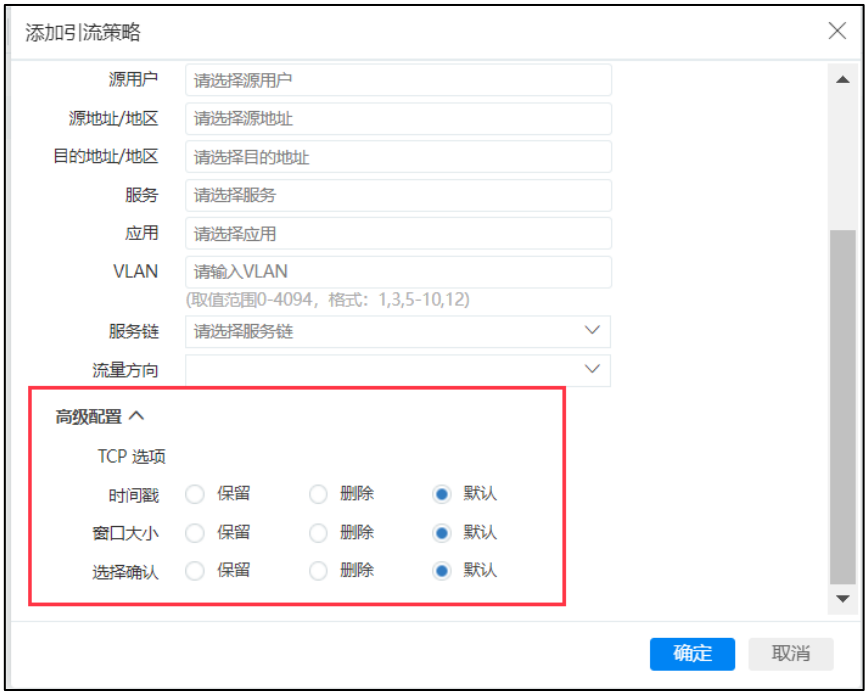


4.32.2 目的 NAT

目的 NAT 新增支持基于时间进行转换前匹配。

4.33 流量编排

选择【策略配置】>【流量编排】>【引流策略】,添加或编辑引流策略时，新增 TCP 选项高级配置。

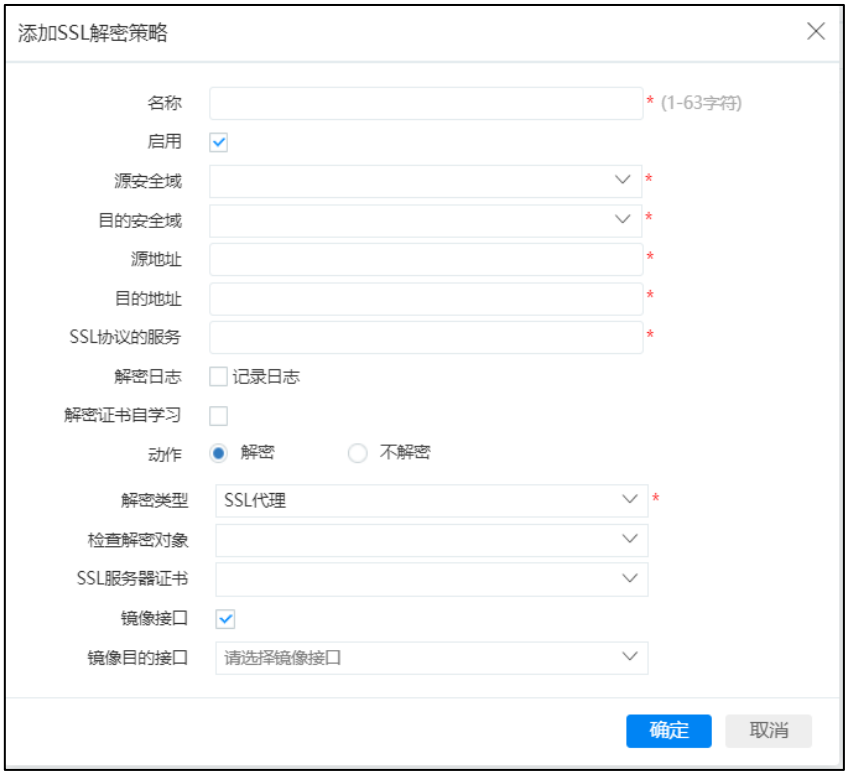


4.34 SSL 解密策略

SSL 解密策略新增“解密证书自学习”开关。开启解密证书自学习后，可以查看自学习结果。

镜像接口开关名称修改，且只有开启开关后才会显示镜像目的接口配置。

修改后：


添加SSL解密策略
名称
* (1-63字符)
启用
源安全域
目的安全域
源地址
目的地址
SSL协议的服务
解密日志
记录日志
解密证书自学习
动作
解密
不解密
解密类型
SSL代理
检查解密对象
SSL服务器证书
镜像接口
镜像目的接口
请选择镜像接口
确定
取消

解密证书自学习
刷新

修改前：

4.35 IP-MAC 绑定

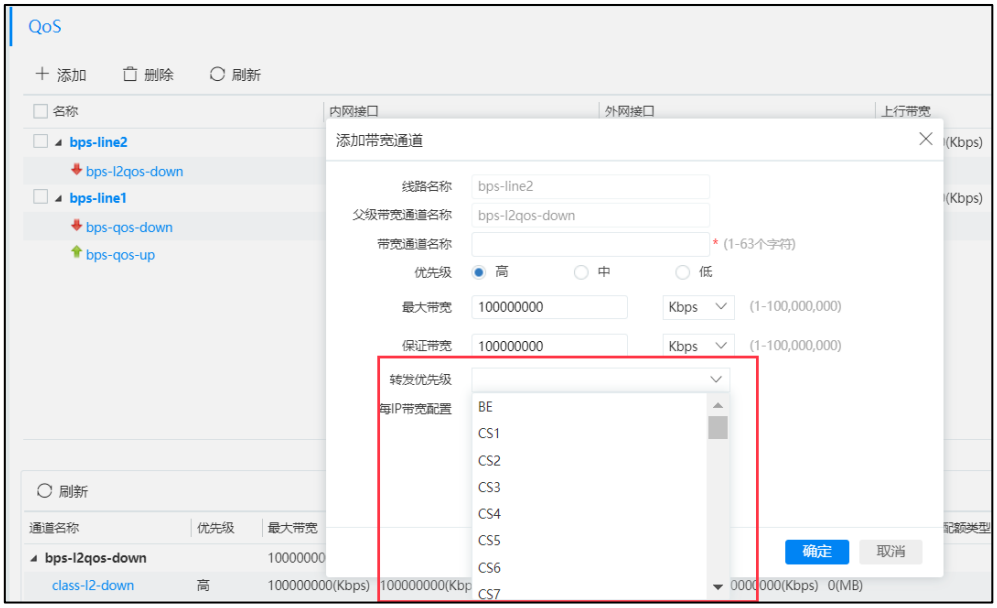
选择【策略配置】>【IP-MAC 绑定】。新增【导入】、【导出】和【批量修改安全域】按钮，支持批量导入、导出 IP-MAC 策略，以及批量修改多条策略的安全域的功能。

4.36 QoS

选择【策略配置】>【QoS】。

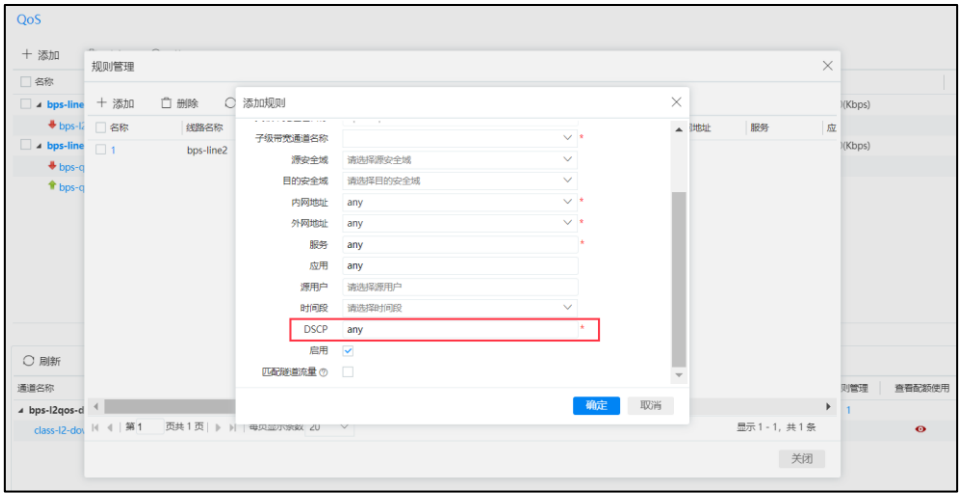
- 添加带宽通道时，转发优先级支持选择 DSCP 的值，修改前为手工输入 0~63 范围内的取值。

修改后：



修改前：

- 添加规则中，规则支持“DSCP”参数，可以根据 dscp 的取值进行 qos 限制。



4.37 黑白名单

4.37.1 域名黑白名单

新增支持带下划线“_”的域名。

4.37.2 IDP 联动黑名单

新增 IDP 联动黑名单展示页面。IDP 联动黑名单展示 IDP 联动生成的黑名单。

4.38 会话限制

【策略配置】>【会话限制】页面，会话限制配置页面新增支持基于源用户和时间维度进行限制。

4.39 安全防护

4.39.1 攻击防护

- 【策略配置】>【安全防护】下的【攻击防护】页面新增“阈值学习”功能，支持设置学习时长。学习完成后，会将三层和四层 Flood 攻击和 IP 地址扫描攻击以及端口扫描攻击的参考值记录下来。

对 Flood 类型的攻击，统计指定时间段内安全域下每秒对应类型 flood 包个数，其最大值自动设置为警戒参考值。

对于恶意扫描类型的攻击，包括 IP 地址扫描攻击、端口扫描，统计指定时间段内安全域下每 10 个包所花费的时间，其最小值自动设置为警戒参考值。

- 新增支持 Frag Flood 攻击防护。

- IP 欺骗白名单逻辑变更。

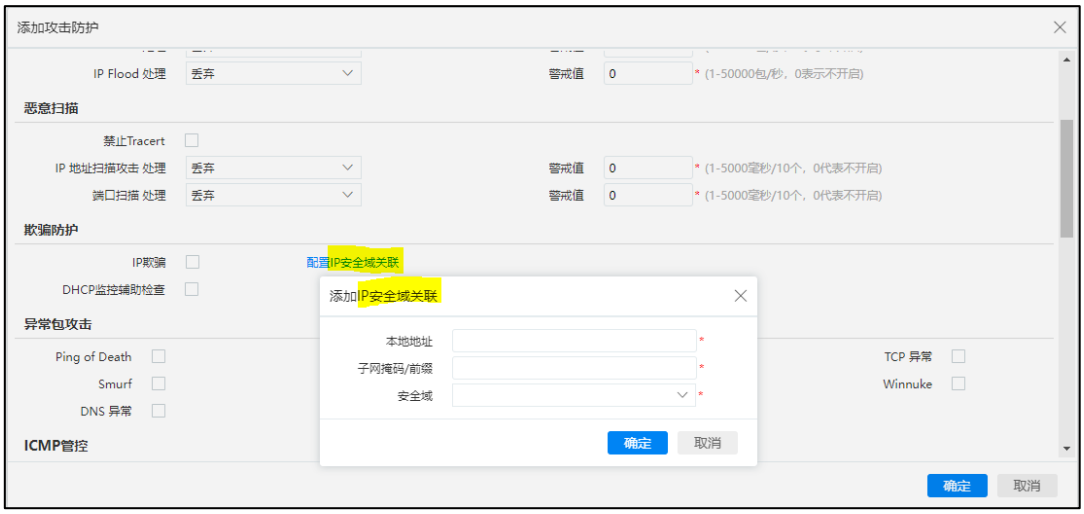
【配置 IP 安全域关联】修改为【IP 欺骗白名单】，IP 欺骗防护的逻辑变

化。

修改后当防火墙接收到的数据包时，先检查数据包的源 IP 地址是否为 IP 欺骗白名单中的 IP，若命中白名单（安全域也必须一致），则直接允许数据包进入下一个模块；若数据包未命中白名单，则对数据包的源 IP 进行欺骗防护检查，检查该 IP 的入接口与返回报文的出接口是否一致，若接口一致则通过 IP 欺骗防护检查，否则认定为 IP 欺骗，直接丢弃报文。

修改后：

修改前：



- 异常包攻击防护新增圣诞树攻击防护

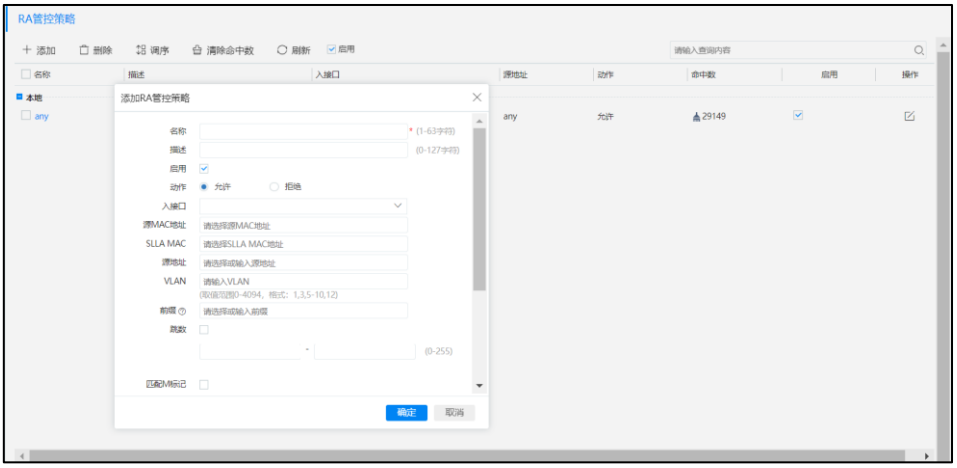
- 新增 DNS Reply Flood，原来的 DNS Flood 改为 DNS Request Flood。

修改后：

修改前：

4.39.2 RA 管控策略

【策略配置】>【安全防护】下新增 RA 管控策略，通过 IPv6 RA Guard 防止中间人 RA 攻击。



RA 管控策略是通过 IPv6 RA Guard 防止中间人 RA 攻击。

当防火墙以不同模式进行部署时，保护的对象并不同。

- 防火墙部署在网络出口，以路由模式部署，负责为 IPv6 用户配置地址，对防火墙自身进行 RA 攻击防护。
- 防火墙部署在企业内部，以交换模式部署，对企业内网主机进行 RA 攻击防护。

4.39.3 弱口令检测

【策略配置】>【安全防护】下新增弱口令检测功能。支持“主动检测”和“被动检测”。

说明：弱口令字典类型为“用户名”，则为用户库；弱口令字典类型为“密码”，则为弱口令字典。

- 主动检测

  主动检测任务主动对指定网段指定协议进行弱口令暴力破解测试，测试用户名口令是否为预置用户库/弱口令字典和自定义用户库/弱口令字典中包含的常见用户名、口令。

防火墙支持对 SSH、SMB、RDP、FTP、POP3、SMTP、MYSQL、POSTGRES、REDIS、SNMP 协议进行主动弱口令检测。

- 被动检测

  被动检测对获取的用户名密码进行弱口令规则匹配，当检测到命中弱口令规则的用户名或密码时，记录威胁日志。

  协议要进行弱口令被动检测，必须打开“对象配置 > 安全配置文件 > 行为管控”页面，在添加行为管控时，开启对应协议下的“弱口令检测”开关。

  防火墙支持对 SMTP、POP3、IMAP、FTP、TELNET 协议进行被动弱口令检测。

4.40 共享接入

原来的共享接入只支持共享接入出口 IP 确认，本版本新增内网终端数和类型识别。

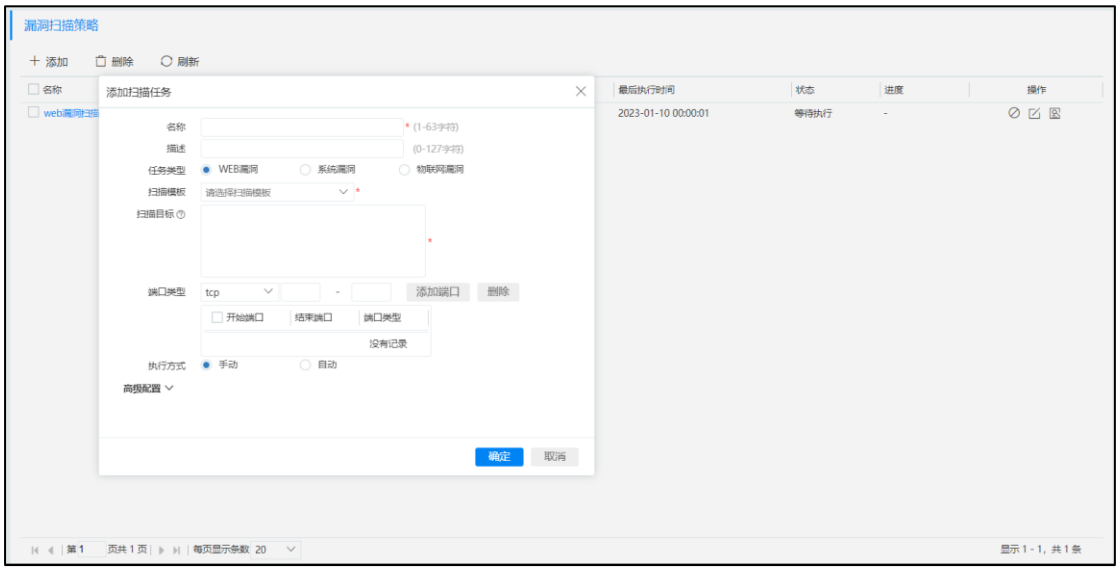
选择【策略配置】>【共享接入管理】,【共享接入检测】页面中新增【内网详情检测】开关和【锁定时间】参数的设置。

内网详情检测用于检测共享接入终端数量。通过对常见的应用协议进行特征识别，并与资产识别特征库（其中一部分是共享接入识别特征）中特征进行匹配，识别出流量中的设备信息，从而确定出 NAT 后终端数量和类型。

锁定时间即对设备流量执行阻断的时长。

4.41 漏洞扫描策略

选择【策略配置】。新增【漏洞扫描策略】，支持进行 Web 漏洞、系统漏洞和物联网漏洞扫描，支持进行 Web 漏洞、系统漏洞和物联网漏洞扫描。



4.42 处置中心

【处置中心】下新增【漏洞主机】。漏洞扫描功能扫描到的漏洞主机可以在【处置中心】>【漏洞主机】页面查看。

4.43 数据中心

4.43.1 日志

4.43.1.1 日志存储

防火墙日志存储空间说明如下：

- 带硬盘的防火墙设备所有日志都存储在硬盘中。
- 不带硬盘的防火墙设备操作日志、系统日志和沙箱日志存储在 CF 卡中，其他的所有日志存储在内存中。

防火墙总体日志空间划分给根系统和每个虚拟系统分别存储日志。根系统的日志空间系统默认指定 25%，虚拟系统的日志空间可以在创建虚拟系统时配置。

本版本日志系统进行了重构，采用了新的存储架构。新的存储架构日志存储效率变高，日志存储时间增长（最多为原来 10 倍，才会触发日志回滚）。

触发日志回滚的条件和日志空间清空方式有所变化，说明如下：

- 重构前当单个虚拟系统或根防火墙系统的日志达到日志空间的 70%时，最早生成的日志（占总空间 1/30 的单元）除威胁日志之外将被删除，清空的空间用来存放新的日志。最老威胁日志将被存储在专门的空间，直至威胁日志大小到达一定大小触发回滚后，再清除这些威胁日志。
- 重构后虚系统所分配的磁盘空间按照日志类型再次划分存储空间，当某种日志类型将耗尽所分配的磁盘空间时，将按天为单位，删除最旧的日志。

以下数据可用于估算日志存储时间

日志类型	日志空间（老版本）	日志空间（新版本）
操作日志	90M（硬盘）/9M（CF 卡）	30M（硬盘）/9M(CF 卡)
系统日志	90M（硬盘）/9M（CF 卡）	30M（硬盘）/9M(CF 卡)
沙箱日志	90M（硬盘）/9M（CF 卡）	30M（硬盘）/9M(CF 卡)
其他日志	日志空间大小*70%*vsys 占比-3*90M（硬盘）/30M(内存)	MAX（30M，日志空间大小*vsys 占比-3*30Mb）（硬盘）/30M（内存） 存在硬盘的情况下威胁日志固定为 200Mb

注：

- 无硬盘的设备日志存储在 CF 卡和内存中。
- 带硬盘的设备日志空间大小为日志磁盘分区大小-Min（日志磁盘分区大小*15%，10Gb）
- 原来存储架构下平均每条日志占用 338 字节，新的存储架构下每条日志占用 30 字节。

4.43.1.2 流量日志

流量日志中增加服务链信息。

4.43.1.3 NAT444 日志

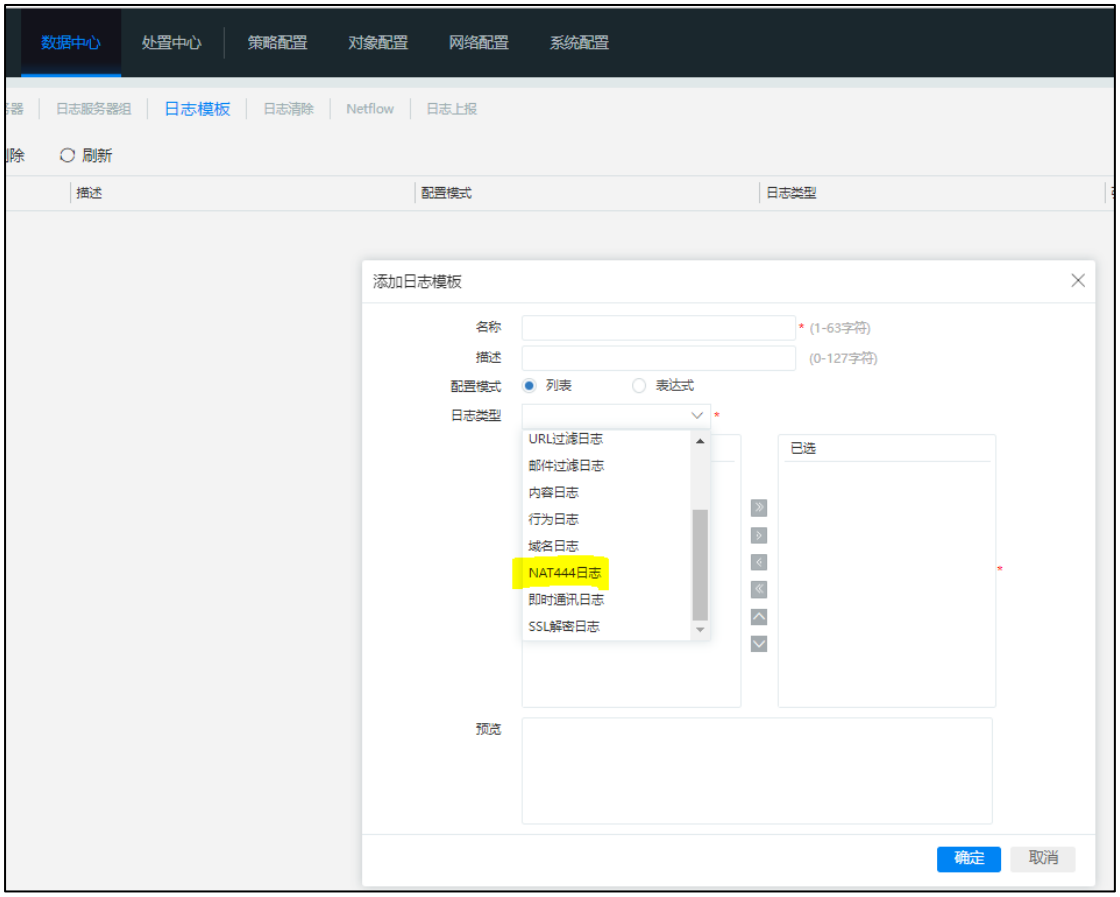
【数据中心】>【日志】下新增 NAT444 日志。

4.43.1.4 日志外发

新增 NAT444 日志的外发设置。

4.43.1.5 日志模板

日志模板日志类型新增 NAT444 日志。

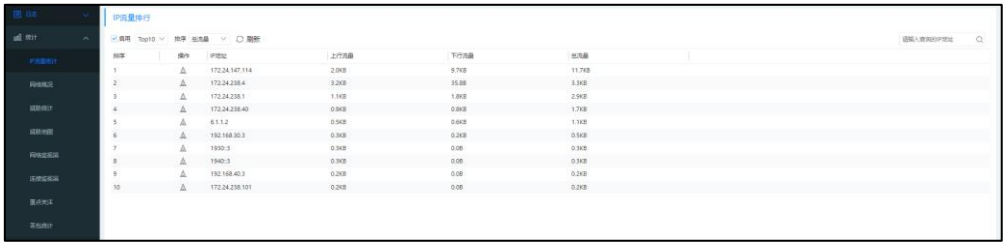


4.43.1.6 日志上报

【数据中心】>【日志】>【日志设置】下新增【日志上报】功能，支持通过 FTP 将日志自动备份至其他设备存储。

4.43.2 统计

【数据中心】>【统计】下新增【IP 流量统计】页签。IP 流量统计默认展示总流量 TOP10 的流量统计情况。



4.43.3 监控

4.43.3.1 隧道监控

选择【数据中心】>【监控】,【隧道监控】下新增【IKEv2 自动隧道】。

4.43.3.2 用户监控

选择【数据中心】>【监控】,【用户监控】下每个类型的用户监控页面显示的信息都新增“描述”项。

4.43.3.3 联动终端监控

选择【数据中心】>【监控】，原【资产监控】下的【联动终端列表】单独拆分出来，放到【监控】下。

5 硬件更新说明

5.1.1 新增产品型号及配套板卡

新增产品	说明	配套板卡
NSG5900-TQ35	板载 MGT+HA 接口 16 电+16 千兆光+12 万兆+4 扩展槽	NSG5900-TQ-4T-QW NSG5900-TQ-4TP-QW NSG5900-TQ-4S-QW NSG5900-TQ-4SP-SM-QW NSG5900-TQ-4SP-MM-QW NSG5900-TQ-4T4S-QW NSG5900-TQ-8T-QW NSG5900-TQ-8TP-QW NSG5900-TQ-8S-QW NSG5900-TQ-2X-QW NSG5900-TQ-2XP-SM-QW NSG5900-TQ-2XP-MM-QW NSG5900-TQ-4X-QW NSG5900-TQ-4XP-MM-QW NSG5900-TQ-4XP-SM-QW NSG5900-TQ-2QX-QW NSG5900-TQ-4TP4S-QW
NSG5900-TX25	板载 MGT+HA 接口 16 电+16 千兆光+12 万兆+4 扩展槽	NSG5900-TX-2T-QW NSG5900-TX-2S-QW NSG5900-TX-4T-QW NSG5900-TX-4TP-QW NSG5900-TX-4S-QW NSG5900-TX-4SP-SM-QW NSG5900-TX-4SP-MM-QW NSG5900-TX-2T2S-QW NSG5900-TX-4T4S-

新增产品	说明	配套板卡
		QW NSG5900-TX-8T-QW NSG5900-TX-8TP-QW NSG5900-TX-8S-QW NSG5900-TX-2X-QW NSG5900-TX-2XP-SM-QW NSG5900-TX-2XP-MM-QW NSG5900-TX-4X-QW NSG5900-TX-4XP-MM-QW NSG5900-TX-4XP-SM-QW NSG5900-TX-2QX-QW NSG5900-TX-4TP4S-QW
NSG5900-TQ15	板载 MGT+HA 接口 18 电+16 千兆光+8 万兆+4 扩展槽	NSG5900-TQ-4T-QW NSG5900-TQ-4TP-QW NSG5900-TQ-4S-QW NSG5900-TQ-4SP-SM-QW NSG5900-TQ-4SP-MM-QW NSG5900-TQ-4T4S-QW NSG5900-TQ-8T-QW NSG5900-TQ-8TP-QW NSG5900-TQ-8S-QW NSG5900-TQ-2X-QW NSG5900-TQ-2XP-SM-QW NSG5900-TQ-2XP-MM-QW NSG5900-TQ-4X-QW NSG5900-TQ-4XP-MM-QW NSG5900-TQ-4XP-SM-QW NSG5900-TQ-2QX-QW

新增产品	说明	配套板卡
		NSG5900-TQ-4TP4S-QW
NSG8000-TX25	板载 MGT+HA 接口 16 电+16 千兆光+12 万兆+4 扩展槽	NSG8000-TX-2T-QW NSG8000-TX-2S-QW NSG8000-TX-4T-QW NSG8000-TX-4TP-QW NSG8000-TX-4S-QW NSG8000-TX-4SP-SM-QW NSG8000-TX-4SP-MM-QW NSG8000-TX-2T2S-QW NSG8000-TX-4T4S-QW NSG8000-TX-8T-QW NSG8000-TX-8TP-QW NSG8000-TX-8S-QW NSG8000-TX-2X-QW NSG8000-TX-2XP-SM-QW NSG8000-TX-2XP-MM-QW NSG8000-TX-4X-QW NSG8000-TX-4XP-MM-QW NSG8000-TX-4XP-SM-QW NSG8000-TX-2QX-QW NSG8000-TX-4TP4S-QW
NSG8000-TX15	板载 MGT+HA 接口 16 电+16 千兆光+12 万兆+4 扩展槽	

5.1.2 新增单板及配套产品

新增板卡	说明	配套产品
NSG2000-TC-4T-QW	4 口 10/100/1000Base-T 板卡	NSG2000-TE25 NSG2000-TE35 NSG2000-TE45
NSG2000-TC-4TP-QW	4 口 10/100/1000Base-T 板卡，支持 2 对硬件 bypass	

新增板卡	说明	配套产品
NSG2000-TC-4S-QW	4 口千兆 SFP 板卡	
NSG2000-TC-2X-QW	2 口万兆光口板卡，2 个 SFP+插槽（GEN2.0 固件）	
NSG3000-BT-4T-2U-QW	4 口 10/100/1000Base-T 板卡	NSG3000-TE45
NSG3000-BT-4TP-2U-QW	4 口 10/100/1000Base-T 板卡,支持 2 对硬件 bypass	
NSG3000-BT-8T-2U-QW	8 口 10/100/1000Base-T 板卡	
NSG3000-BT-4S-2U-QW	4 口千兆 SFP 板卡	
NSG3000-BT-4T-QW	4 口 10/100/1000Base-T 板卡	NSG3000-TE35 NSG3000-TE25 NSG3000-TE15
NSG3000-BT-4TP-QW	4 口 10/100/1000Base-T 板卡,支持 2 对硬件 bypass	
NSG3000-BT-4S-QW	4 口千兆 SFP 板卡	
NSG4000-TC-2X-QW	2 口万兆光口板卡，2 个 SFP+插槽（GEN2.0 固件）	NSG4000-TG15 NSG4000-TG25 NSG4000-TG35 NSG4000-TG45
NSG4000-TC-4S-QW	4 口千兆 SFP 板卡	
NSG4000-TC-2XP-MM-QW	2 口万兆多模 SFP 板卡，支持 1 对硬件 bypass	
NSG4000-TC-2XP-SM-QW	2 口万兆单模 SFP 板卡，支持 1 对硬件 bypass	
NSG5000-TC-4SP-MM-QW	4 口千兆多模 SFP 板卡，支持 2 对千兆光口硬件 bypass	NSG5000-TG15 NSG5000-TG25 NSG5000-TG35 NSG5000-TG45 NSG5000-TG55 NSG5000-TG65
NSG5000-TC-4SP-SM-QW	4 口千兆单模 SFP 板卡，支持 2 对千兆光口硬件 bypass	
NSG5000-TC-4T-QW	4 口 10/100/1000Base-T 板卡	
NSG5000-TC-4TP-QW	4 口 10/100/1000Base-T 板卡，支持 2 对硬件 bypass	
NSG5000-TC-8T-QW	8 口 10/100/1000Base-T 板卡	
NSG5000-TC-8TP-QW	8 口 10/100/1000Base-T 板卡,支持 4 对硬件 bypass	
NSG5000-TC-4S-QW	4 口千兆 SFP 板卡	
NSG5000-TC-8S-QW	8 口千兆 SFP 板卡	
NSG5000-TC-4T4S-QW	4 口 10/100/1000Base-T 和 4 口千兆 SFP 板卡	
NSG5000-TC-4X-QW	4 口万兆光口板卡，4 个 SFP+插槽（GEN2.0 固件）	

新增板卡	说明	配套产品
NSG5000-TC-2X-QW	2 口万兆光口板卡，2 个 SFP+插槽（GEN3.0 固件）	
NSG5000-TC-2XP-MM-QW	2 口万兆多模 SFP 板卡，支持 1 对硬件 bypass	
NSG5000-TC-2XP-SM-QW	2 口万兆单模 SFP 板卡，支持 1 对硬件 bypass	
NSG5900-TQ-4T-QW	4 口 10/100/1000Base-T 板卡	NSG5900-TQ35
NSG5900-TQ-4TP-QW	4 口 10/100/1000Base-T 板卡，支持 2 对硬件 bypass	
NSG5900-TQ-4S-QW	4 口千兆 SFP 板卡	
NSG5900-TQ-4SP-SM-QW	4 口千兆单模 SFP 板卡，支持 2 对硬件 bypass	
NSG5900-TQ-4SP-MM-QW	4 口千兆多模 SFP 板卡，支持 2 对硬件 bypass	
NSG5900-TQ-4T4S-QW	4 口 10/100/1000Base-T 和 4 口千兆 SFP 板卡	
NSG5900-TQ-8T-QW	8 口 10/100/1000Base-T 板卡	
NSG5900-TQ-8TP-QW	8 口 10/100/1000Base-T 板卡,支持 4 对硬件 bypass	
NSG5900-TQ-8S-QW	8 口千兆 SFP 板卡	
NSG5900-TQ-2X-QW	2 口万兆光口板卡	
NSG5900-TQ-2XP-SM-QW	2 口万兆单模 SFP 板卡，支持 1 对硬件 bypass	
NSG5900-TQ-2XP-MM-QW	2 口万兆多模 SFP 板卡，支持 1 对硬件 bypass	
NSG5900-TQ-4X-QW	4 口万兆光口板卡	
NSG5900-TQ-4XP-MM-QW	4 口万兆多模 SFP 板卡,支持 2 对硬件 bypass	
NSG5900-TQ-4XP-SM-QW	4 口万兆单模 SFP 板卡,支持 2 对硬件 bypass	
NSG5900-TQ-2QX-QW	2 口 40G QSFP 板卡，2 个 QSFP 插槽；	
NSG5900-TQ-4TP4S-QW	4 口 10/100/1000Base-T 和 4 口千兆 SFP 板卡，支持 2 对电口 bypass	
NSG5900-TX-2T-QW	2 口 10/100/1000Base-T 板卡	NSG5900-TX25
NSG5900-TX-2S-QW	2 口千兆 SFP 板卡	
NSG5900-TX-4T-QW	4 口 10/100/1000Base-T 板卡	

新增板卡	说明	配套产品
NSG5900-TX-4TP-QW	4 口 10/100/1000Base-T 板卡，支持 2 对硬件 bypass	
NSG5900-TX-4S-QW	4 口千兆 SFP 板卡	
NSG5900-TX-4SP-SM-QW	4 口千兆单模 SFP 板卡，支持 2 对硬件 bypass	
NSG5900-TX-4SP-MM-QW	4 口千兆多模 SFP 板卡，支持 2 对硬件 bypass	
NSG5900-TX-2T2S-QW	2 口 10/100/1000Base-T 和 2 口千兆 SFP 板卡	
NSG5900-TX-4T4S-QW	4 口 10/100/1000Base-T 和 4 口千兆 SFP 板卡	
NSG5900-TX-8T-QW	8 口 10/100/1000Base-T 板卡	
NSG5900-TX-8TP-QW	8 口 10/100/1000Base-T 板卡，支持 4 对硬件 bypass	
NSG5900-TX-8S-QW	8 口千兆 SFP 板卡	
NSG5900-TX-2X-QW	2 口万兆光口板卡	
NSG5900-TX-2XP-SM-QW	2 口万兆单模 SFP 板卡，支持 1 对硬件 bypass	
NSG5900-TX-2XP-MM-QW	2 口万兆多模 SFP 板卡，支持 1 对硬件 bypass	
NSG5900-TX-4X-QW	4 口万兆光口板卡	
NSG5900-TX-4XP-MM-QW	4 口万兆多模 SFP 板卡，支持 2 对硬件 bypass	
NSG5900-TX-4XP-SM-QW	4 口万兆单模 SFP 板卡，支持 2 对硬件 bypass	
NSG5900-TX-2QX-QW	2 口 40G QSFP 板卡，支持 2 个 QSFP 插槽；	
NSG5900-TX-4TP4S-QW	4 口 10/100/1000Base-T 和 4 口千兆 SFP 板卡，支持 2 对电口 bypass	
NSG5900-TQ-4T-QW	4 口 10/100/1000Base-T 板卡	NSG5900-TQ15
NSG5900-TQ-4TP-QW	4 口 10/100/1000Base-T 板卡，支持 2 对硬件 bypass	
NSG5900-TQ-4S-QW	4 口千兆 SFP 板卡	
NSG5900-TQ-4SP-SM-QW	4 口千兆单模 SFP 板卡，支持 2 对硬件 bypass	
NSG5900-TQ-4SP-MM-QW	4 口千兆多模 SFP 板卡，支持 2 对硬件 bypass	

新增板卡	说明	配套产品
NSG5900-TQ-4T4S-QW	4 口 10/100/1000Base-T 和 4 口千兆 SFP 板卡	
NSG5900-TQ-8T-QW	8 口 10/100/1000Base-T 板卡	
NSG5900-TQ-8TP-QW	8 口 10/100/1000Base-T 板卡，支持 4 对硬件 bypass	
NSG5900-TQ-8S-QW	8 口千兆 SFP 板卡	
NSG5900-TQ-2X-QW	2 口万兆光口板卡	
NSG5900-TQ-2XP-SM-QW	2 口万兆单模 SFP 板卡，支持 1 对硬件 bypass	
NSG5900-TQ-2XP-MM-QW	2 口万兆多模 SFP 板卡，支持 1 对硬件 bypass	
NSG5900-TQ-4X-QW	4 口万兆光口板卡	
NSG5900-TQ-4XP-MM-QW	4 口万兆多模 SFP 板卡，支持 2 对硬件 bypass	
NSG5900-TQ-4XP-SM-QW	4 口万兆单模 SFP 板卡，支持 2 对硬件 bypass	
NSG5900-TQ-2QX-QW	2 口 40G QSFP 板卡	
NSG5900-TQ-4TP4S-QW	4 口 10/100/1000Base-T 和 4 口千兆 SFP 板卡，支持 2 对电口 bypass	
NSG7000-TX-2QXP-SM-QW	2 口 40G 单模 QSFP 板卡，2 个 QSFP 插槽，支持 1 对硬件 bypass	NSG7000-TX15 NSG7000-TX25 NSG7000-TX35 NSG7000-TX45 NSG7000-TX55 NSG7000-TX65
NSG7000-TX-2QXP-MM-QW	2 口 40G 多模 QSFP 板卡，2 个 QSFP 插槽，支持 1 对硬件 bypass	
NSG8000-TX-2T-QW	2 口 10/100/1000Base-T 板卡	NSG8000-TX15 NSG8000-TX25
NSG8000-TX-2S-QW	2 口千兆 SFP 板卡	
NSG8000-TX-4T-QW	4 口 10/100/1000Base-T 板卡	
NSG8000-TX-4TP-QW	4 口 10/100/1000Base-T 板卡，支持 2 对硬件 bypass	
NSG8000-TX-4S-QW	4 口千兆 SFP 板卡	
NSG8000-TX-4SP-SM-QW	4 口千兆单模 SFP 板卡,支持 2 对硬件 bypass	
NSG8000-TX-4SP-MM-QW	4 口千兆多模 SFP 板卡,支持 2 对硬件 bypass	
NSG8000-TX-2T2S-QW	2 口 10/100/1000Base-T 和 2 口千兆 SFP 板卡	

新增板卡	说明	配套产品
NSG8000-TX-4T4S-QW	4 口 10/100/1000Base-T 和 4 口千兆 SFP 板卡	
NSG8000-TX-8T-QW	8 口 10/100/1000Base-T 板卡	
NSG8000-TX-8TP-QW	8 口 10/100/1000Base-T 板卡,支持 4 对硬件 bypass	
NSG8000-TX-8S-QW	8 口千兆 SFP 板卡	
NSG8000-TX-2X-QW	2 口万兆光口板卡	
NSG8000-TX-2XP-SM-QW	2 口万兆单模 SFP 板卡，支持 1 对硬件 bypass	
NSG8000-TX-2XP-MM-QW	2 口万兆多模 SFP 板卡，支持 1 对硬件 bypass	
NSG8000-TX-4X-QW	4 口万兆光口板卡	
NSG8000-TX-4XP-MM-QW	4 口万兆多模 SFP 板卡,支持 2 对硬件 bypass	
NSG8000-TX-4XP-SM-QW	4 口万兆单模 SFP 板卡,支持 2 对硬件 bypass	
NSG8000-TX-2QX-QW	2 口 40G QSFP 板卡	
NSG8000-TX-4TP4S-QW	4 口 10/100/1000Base-T 和 4 口千兆 SFP 板卡，支持 2 对电口 bypass	
NSG9000-QX-2QXP-SM-QW	2 口 40G 单模 QSFP 板卡，支持 1 对硬件 bypass	NSG9000-TZ15 NSG9000-TZ25 NSG9000-TZ35 NSG9000-TZ55 NSG9000-TZ65 NSG9000-TZ75
NSG9000-QX-2QXP-MM-QW	2 口 40G 多模 QSFP 板卡，支持 1 对硬件 bypass	
NSG9000-QX-8X-QW	8 口万兆光口板卡	

5.1.3 其他硬件变更

无

6 修正 Bug 清单

表 6-1 修正 Bug 清单说明

编号	功能模块	描述	Bug 号
1	IPSec VPN	IPSec VPN 使用 SM4 算法与 H3C 对接，页面隧道监控一阶段不显示加密算法	TDSUSTASK-863
2	虚拟系统	虚拟系统中 AD 丢包，在主系统中无丢包统计显示	WLPT-9169
3	黑名单	地址黑名单校验错误，MAC 地址中有小写字母导入失败	WLPT-7325
5	威胁日志	反病毒类型威胁日志中威胁 ID 都为 0	WLPT-7816
6	登录密码	console 重置 admin 密码时应同时开启 admin 账号的 console 登录方式	WLPT-6019
7	认证服务器	AD 服务器用户目录包含反斜杠会概率性导致改目录下用户无法读出	WLPT-10468
8	MTU	从 web 上查看接口 MTU 最大值为 9186，x86 设备应该为 9216	WLPT-7567
9	流量编排	出口墙运行一个多月后，SSL 解密与高级功能失效。存在 SKB 泄漏	WLPT-10713

7 发布文件列表

表 7-1 6.1.14.164546 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	hw6.1.14.164546.86.sign hw6.1.14.164546.86.enc.sign
2	版本号	6.1.14.164546
3	文件大小	243.86MB (非 enc 版本) 244.11MB（enc 版本）
4	MD5	70981c0594eeb1a36b0a255d4129ba84 (非 enc 版本) 5ac9b93fae50aded313e97ca000875b5（enc 版本）
5	SHA-1	22306fcbd7aced3d7a4597f4f3493a23ff5a3ec4 (非 enc 版本) 9d5dafb3016dd49cea1c4b319d5f21ed61c80e85（enc 版本）
6	SHA-256	181c6a8a16835496a483182511424ec0edf25287c41b920e880a8e35e21abc1f (非 enc 版本) 67e823b6ef6a30c7a63ceedee01f7957d36c38553a3bc7ed1a7e892158941062（enc 版本）

表 7-2 6.91.14.164546 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	hw6.91.14.164546.91.sign
2	版本号	6.91.14.164546
3	文件大小	292.80MB
4	MD5	a2aae7df0460fff9437e9b249d2a8a86
5	SHA-1	c1adfb7e373f6419dc2448ffb4f2c1d3013b8fa0
6	SHA-256	febe22607f185b0b53b5a54ee5ec1e62e408e9006956e95b40d00d472dec0bc4

表 7-3 6.90.14.164546 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	hw6.90.14.164546.96.sign
2	版本号	6.90.14.164546
3	文件大小	307.08MB
4	MD5	b2fc40d3d9c8a979cc1b02e75f53af6d
5	SHA-1	59579d0c299e47553855cab1684138284e848693
6	SHA-256	84befdf76ef8a386283512e61001402b3d1730e82513d5962d9ce9edf87e9ef8

8 资料获取

表 8-1 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	https://docs.qianxin-inc.cn/dms/file?folder=360994&type=load
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。	https://docs.qianxin-inc.cn/dms/file?folder=360994&type=load
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。	https://docs.qianxin-inc.cn/dms/file?folder=360994&type=load
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。	https://docs.qianxin-inc.cn/dms/file?folder=360994&type=load