RG-WALL 1600-Z-S 系列

云管防火墙

NTOS1.0R3 用户手册

文档版本 V1.0

归档日期 2022-10-28

copyright © 2022 锐捷网络

版权声明

copyright © 2022 锐捷网络

保留对本文档及本声明的一切权利。

未得到锐捷网络的书面许可，任何单位和个人不得以任何方式或形式对本文档的部分或全部内容进行复制、摘录、备份、修改、传播、翻译成其他语言、将其部分或全部用于商业用途。

和其他锐捷网络商标均为锐捷网络的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

免责声明

您所购买的产品、服务或特性等应受商业合同和条款的约束，本文档中描述的部分或全部产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，锐捷网络对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。锐捷网络保留在没有任何通知或者提示的情况下对文档内容进行修改的权利。

本手册仅作为使用指导。锐捷网络在编写本手册时已尽力保证其内容准确可靠，但并不确保手册内容完全没有错误或遗漏，本手册中的所有信息也不构成任何明示或暗示的担保。

前　言

读者对象

本书适合下列人员阅读

- 网络工程师
- 技术推广人员
- 网络管理员

技术支持

- 锐捷睿易官方网站：https://www.ruijiery.com/
- 锐捷睿易在线客服：https://ocs.ruijie.com.cn/?p=smb
- 锐捷网络官方网站服务与支持版块：https://www.ruijie.com.cn/service.aspx
- 7天无休技术服务热线：4001-000-078
- 锐捷睿易技术论坛：http://bbs.ruijiery.com/
- 常见问题搜索：https://www.ruijie.com.cn/service/know.aspx
- 锐捷睿易技术支持与反馈信箱：4001000078@ruijie.com.cn
- 锐捷网络文档支持与反馈信箱：doc@ruijie.com.cn
- 锐捷网络服务公众号：【锐捷服务】扫码关注

本书约定

1. 图形界面格式约定

界面图标	解释	举例
<>	按钮	<确定>
[]	菜单项，弹窗名称，页面名称，标签页的名称	菜单项“系统设置”可简化[系统设置]
>>	分级页面，子菜单项	选择[系统设置]>>[系统管理员]
“”	配置项，提示信息，链接	如提示框提示“保存配置成功” 点击“开启”选项 点击“忘记密码”链接

2. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

警告

表示用户必须严格遵守的规则。如果忽视此类信息，可能导致数据丢失或设备损坏。

注意

表示用户必须了解的重要信息。如果忽视此类信息，可能导致功能失效或性能降低。

说明

用于提供补充、申明、提示等。如果忽视此类信息，不会导致严重后果。

产品/版本支持情况

用于提供产品或版本支持情况的说明。

3. 说明

本手册重在介绍产品的特点以及使用方法，指导用户对设备进行配置和试用。

文档修订记录

修订日期	修订版本号	修订描述	修订人
2022-10-27	1.0	在R2的基础上更新 1、更新界面截图和参数解释：安全策略、NAT策略、DoS/DDoS防护、本机防护、特征库升级、配置备份、配置Syslog服务器、Ping诊断、系统日志、安全日志、Web管理界面布局、设置服务参数 2、新增以下功能：临时黑名单、病毒防护、策略路由、链路探测、诊断中心、设备自检、补丁升级、会话日志、流量监控、睿易一体化配置	郭若

目 录

前 言 I

1 产品简介 1

2 Web界面快速入门 2

2.1 登录Web界面 2

2.2 了解Web管理界面布局 3

2.3 Web管理界面通用操作 4

2.3.1 修改当前登录用户密码 4

2.3.2 注销登录 5

3 快速部署 6

3.1 部署规划 6

3.1.1 规划部署位置及IP地址 6

3.1.2 规划部署网络模式 6

3.1.3 梳理业务流量访问关系 7

3.2 部署操作 7

3.2.1 快速上线 7

3.2.2 使用向导配置安全策略 17

4 睿易一体化开局配置 23

4.1 防火墙设备开局（路由模式） 23

4.2 NBR设备开局（透明模式） 29

4.3 睿易APP开局（路由模式） 33

4.4 睿易APP开局（透明模式） 44

5 策略配置管理 57

5.1 安全策略 57

5.1.1 简介 57

5.1.2 手动配置安全策略 57

5.1.3 模拟运行策略 59

5.1.4 导入配置文件配置安全策略 61

5.1.5 调整安全策略顺序 62

5.1.6 优化安全策略 63

5.1.7 查看策略生命周期 64
5.2 开启基础协议报文控制功能 65
5.3 开启端口扫描 66
5.4 开启流量学习 70
5.5 NAT策略 73
5.5.1 简介 73
5.5.2 手动配置NAT策略 74
5.5.3 导入配置文件配置NAT转换 83
5.5.4 配置ALG功能 84
5.5.5 配置地址池 85
5.6 安全防护管理 86
5.6.1 配置DoS/DDoS防护 87
5.6.2 配置ARP防护 90
5.6.3 配置本机防护 93
5.7 黑白名单管理 96
5.7.1 简介 96
5.7.2 创建白名单 97
5.7.3 创建黑名单 98
5.7.4 创建临时黑名单 100
6 对象配置管理 102
6.1 地址对象 102
6.1.1 简介 102
6.1.2 创建地址对象 102
6.1.3 创建地址组对象 104
6.2 应用 105
6.2.1 简介 105
6.2.2 创建自定义应用组 105
6.2.3 查看特征库应用信息 107
6.2.4 升级应用识别特征库 108
6.3 服务 108
6.3.1 简介 108

6.3.2 自定义服务 109
6.3.3 创建服务组 111
6.4 时间计划 113
6.4.1 简介 113
6.4.2 创建循环时间计划 113
6.4.3 创建单次时间计划 114
6.5 内容模板 116
6.5.1 病毒防护 116
6.5.2 入侵防御 120
6.6 安全规则库管理 126
7 网络配置 128
7.1 接口 128
7.1.1 设置物理接口 128
7.1.2 设置子接口 131
7.1.3 设置桥接口 133
7.2 安全区域 136
7.2.1 简介 136
7.2.2 创建安全区域 136
7.3 路由管理 138
7.3.1 简介 138
7.3.2 创建静态路由 138
7.3.3 创建策略路由 140
7.3.4 查看路由表 142
7.4 DNS服务器 143
7.4.1 简介 143
7.4.2 创建DNS服务器 143
7.5 DHCP管理 144
7.5.1 简介 144
7.5.2 配置DHCP服务器 144
7.5.3 地址管理列表 147
7.6 链路探测 147

7.6.1 链路探测 147
7.6.2 探测日志 148
8 系统管理 149
8.1 管理员 149
8.1.1 简介 149
8.1.2 启用默认账号 149
8.1.3 自定义创建管理员 150
8.1.4 修改管理员密码安全策略 154
8.1.5 修改管理员密码 155
8.2 系统配置 156
8.2.1 设置系统时间 156
8.2.2 设置服务参数 158
8.3 激活授权 160
8.4 故障诊断 163
8.4.1 诊断中心 163
8.4.2 设备自检 165
8.4.3 Ping诊断 168
8.4.4 Tracert诊断 169
8.4.5 使用抓包工具 170
8.4.6 一键收集故障信息 171
8.5 特征库升级 172
8.6 系统维护 174
8.6.1 查看设备信息 174
8.6.2 配置备份管理 175
8.6.3 系统升级 176
8.6.4 补丁升级 178
8.6.5 重启设备 180
8.6.6 恢复出厂设置 180
9 安全监控管理 181
9.1 安全驾驶舱 181
9.2 日志监控管理 182

9.2.1 了解日志 182
9.2.2 查询日志 182
9.2.3 配置Syslog服务器 186
9.3 流量监控 188
9.3.1 接口流量统计 188
9.3.2 源IP流量统计 189
9.3.3 应用流量统计 190
9.4 会话监控 191
9.4.1 简介 191
9.4.2 实时会话信息 191
9.4.3 会话统计 193
9.5 设备硬件监控 194
10 对接诺客云 196
10.1 简介 196
10.2 接入诺客云管 196
10.2.1 开启诺客云管 196
10.2.2 绑定设备 196
10.3 诺客云管相关操作 198
10.3.1 查看设备信息 198
10.3.2 隧道管理 200
10.3.3 升级设备软件/固件 201
10.3.4 查看网络拓扑 202
11 典型配置案例 204
11.1 配置外网用户访问内网服务器 204
11.2 配置内网用户通过公网地址访问内部服务器 207
11.3 配置DDoS攻击防护 212
12 常见问题 215
12.1 无法登录Web页面 215
12.2 无法登录SSH页面 215

1 产品简介

锐捷网络新一代防火墙RG-WALL 1600-Z-S系列云管防火墙（以下简称为Z-S系列防火墙）包括Z5100-S和Z3200-S两个产品型号，是面向全行业用户的新一代防火墙，能够通过云网联动不断提升新一代防火墙的安全检测能力，从被动防御向快速检测、积极处置的主动安全发展。

Z-S系列防火墙产品具有主动扫描、流量学习、策略模拟及智能梳理、可视化管理等多种特色功能；广泛支持路由、VLAN、DHCP等各种协议；能够提供稳定可靠的硬件平台、强有力的网络适应能力。可广泛应用于网络结构较简单、应用丰富的中小学、县医院、中小企业及SMB等中低端行业网络环境。

2 Web 界面快速入门

Z-S系列防火墙提供了图形化的Web管理界面，可实现高效的配置和管理。

2.1 登录 Web 界面

【应用场景】

管理员允许通过HTTPS方式登录Web，用户通过Web管理界面即可对防火墙设备进行配置管理操作。

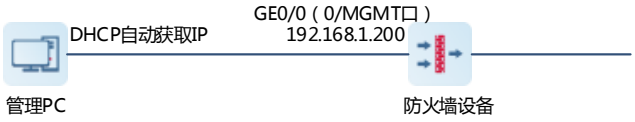
【前置条件】

- Z-S系列防火墙提供了如表2-1所示的Web缺省配置，使用默认值即可登录管理界面。

表2-1 缺省 Web 配置

功能配置	缺省值
Web服务	开启
管理接口IP	192.168.1.200（0/MGMT口）
用户/密码	admin/firewall
默认用户权限	超级管理员，拥有所有权限

- 管理PC与防火墙设备已经连接成功，且设备间能够互通。
  - 通过网线，将防火墙设备的0/MGMT口与管理PC连接。



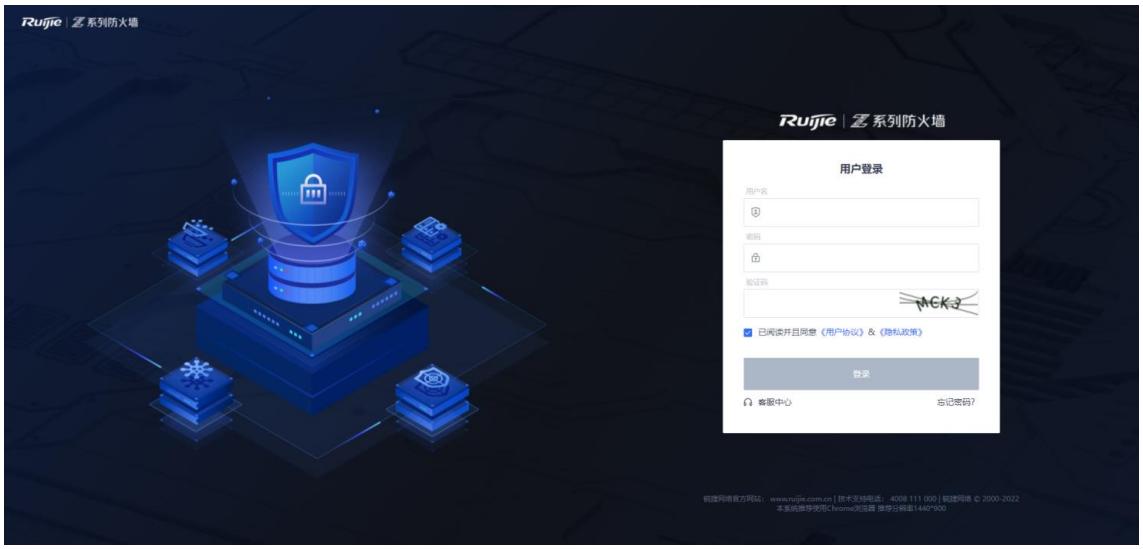
  - 0/MGMT口默认开启DHCP Server功能，管理PC本地网卡可自动从防火墙获取IP地址，能够与防火墙设备互通。无需手动配置管理PC本地网卡IP地址。
- 管理PC需要满足浏览器及分辨率相关要求。
  - 浏览器支持IE11.0、Google chrome、Firefox以及部分基于IE内核的浏览器（如360安全浏览器）。使用其它浏览器登录WEB管理时，可能出现乱码或格式错误等异常。
  - 分辨率：建议分辨率设置为920*1080或1440*900，在其它分辨率下，页面可能出现滚动条，影响使用体验。

【操作步骤】

(1) 在管理PC中打开浏览器。

(2) 在浏览器中输入https://192.168.1.200，并按<Enter>键。

系统弹出登录界面。



(3) 输入用户名、密码及校验码，阅读声明并勾选"已阅读并且同意《免责声明&知识产权声明》"后，点击<登录>。

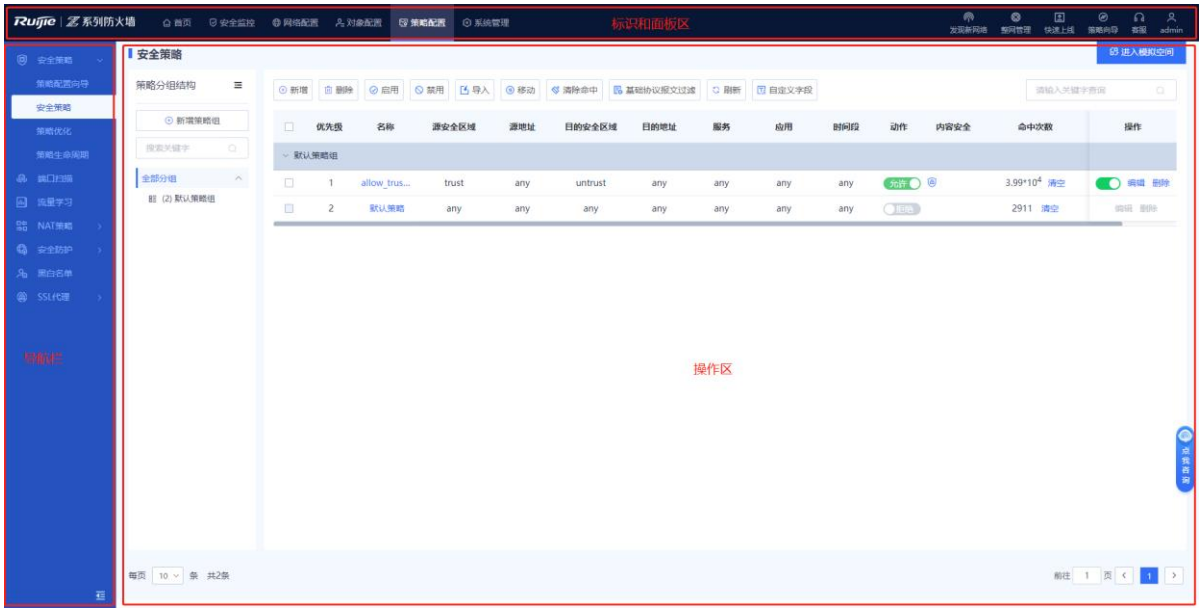
说明

Web服务默认开启校验码功能。如果关闭校验码功能，登录Web管理界面时无需输入校验码。

2.2 了解 Web 管理界面布局

登录Web管理界面后，管理界面的整体布局如图2-1所示。

图2-1 Web 管理界面布局



区域	说明
标识和面板区	● 该区域用来显示公司Logo、设备名称、功能面板。 ● 提供发现新网络、整网管理、快速上线、策略配置向导、客服，帮助用户快速完成部署操作。 ● 显示当前登录用户，提供修改密码及注销登录功能。
导航栏	以树的形式组织设备的Web功能菜单。用户在导航栏中可以方便的选择功能菜单，选择结果显示在操作区中。
操作区	进行配置操作、信息查看、操作结果显示的区域。

2.3 Web 管理界面通用操作

2.3.1 修改当前登录用户密码

【应用场景】

使用默认账户登录Web管理界面后，为确保账户安全性，请及时修改密码。

【操作步骤】

(1) 在标识和面板区，点击登录用户的名称，在弹出的快捷菜单中点击<修改密码>。

(2) 在[修改密码]页面，输入当前密码、新密码、确认密码。

配置项	说明	配置方法
当前密码	登录用户的旧密码。	请提前获取当前登录用户的密码。
新密码	修改后的密码。	密码格式要求如下： ● 至少包含大写字母、小写字母、数字或特殊字符中的任意三种。 ● 不能包含中文、空格和全角字符。 ● 长度范围为8~15个字符。 ● 不能与用户名或用户名的倒序相同。
确认密码	再次输入修改后的密码。	确认密码需要与新密码保持一致。

(3) 点击<确认>。

2.3.2 注销登录

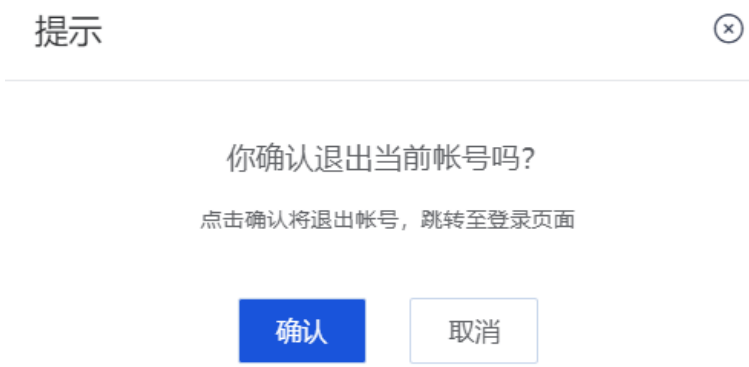
【应用场景】

当管理员一段时间不操作Web界面时，为确保账号安全，请及时注销登录。

【操作步骤】

(1) 在标题和面板区，点击登录用户的名称，在弹出的快捷菜单中点击<退出>。

系统弹出“提示”信息。



(2) 点击<确认>。

系统返回登录页面。

3 快速部署

3.1 部署规划

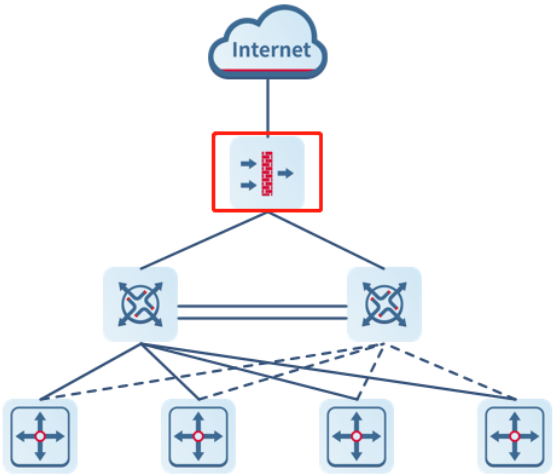
3.1.1 规划部署位置及 IP 地址

根据网络规划，确认防火墙部署位置，例如：内网DMZ服务器区、核心汇聚/出口等。

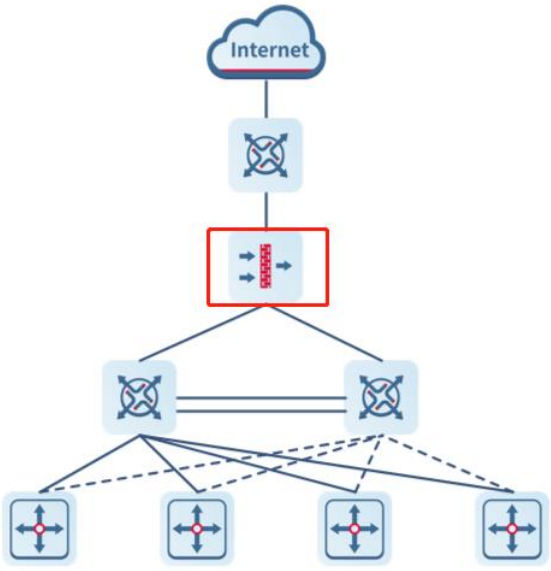
3.1.2 规划部署网络模式

确认防火墙部署位置后，选择对应的模式。

- 部署在网络出口：防火墙选择路由模式，可在安全防护的同时完成部分路由器的功能，如NAT和多运营商访问等。路由模式需确认外网上网方式，若没有根据当地运营商的要求配置，可能将导致无法上网。



- 部署在核心交换机与出口路由之间：防火墙选择透明模式，实现安全防护功能。



3.1.3 梳理业务流量访问关系

网络中的流量错综复杂，安全策略的部署也应该随着业务流量访问关系不断进行优化。

通常情况下，安全策略中不指定应用、时间段是可以接受的。但是源/目的IP地址、源/目的安全区域、服务应指定具体的范围。

通常配置安全策略时，可以从以下几个维度进行考虑：

(1) 确定防火墙在网络中的部署位置，并使用安全区域划分网络。通过对照组网图，了解当前网络资源的分布情况，识别关键信息资产、服务及其安全等级。

(2) 了解当前网络中的运行的合法业务，建立白名单。

(3) 结合企业信息安全政策（Information security policy）、用户组结构和业务白名单，确定通信矩阵和业务访问规则。

(4) 了解需要禁止的高风险应用和非法业务（企业信息安全政策禁止的服务），建立黑名单，确定业务禁止规则。

(5) 建立一条any到any的全通策略，通过开启端口扫描、流量学习功能，记录策略命中日志。对安全策略进行优化。

3.2 部署操作

3.2.1 快速上线

通过Web管理界面提供的快速上线向导，使设备能快速接入互联网。

1. 快速上线（路由模式）

【应用场景】

当规划使用路由模式时，通过执行以下操作使设备快速上线。

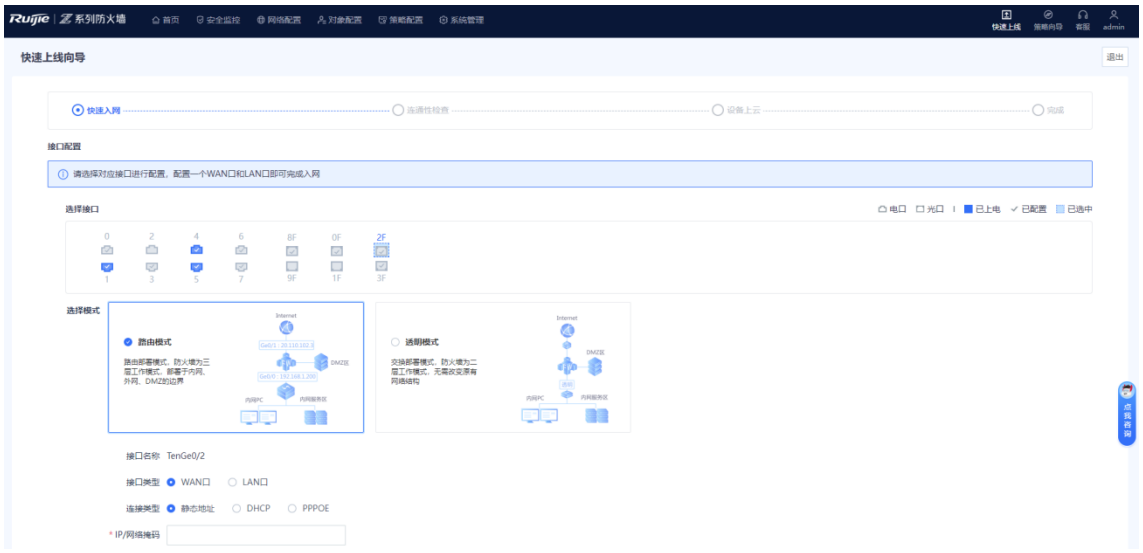
【前置条件】

配置一个LAN口和一个WAN口即可实现快速上网，请提前规划使用的物理接口。

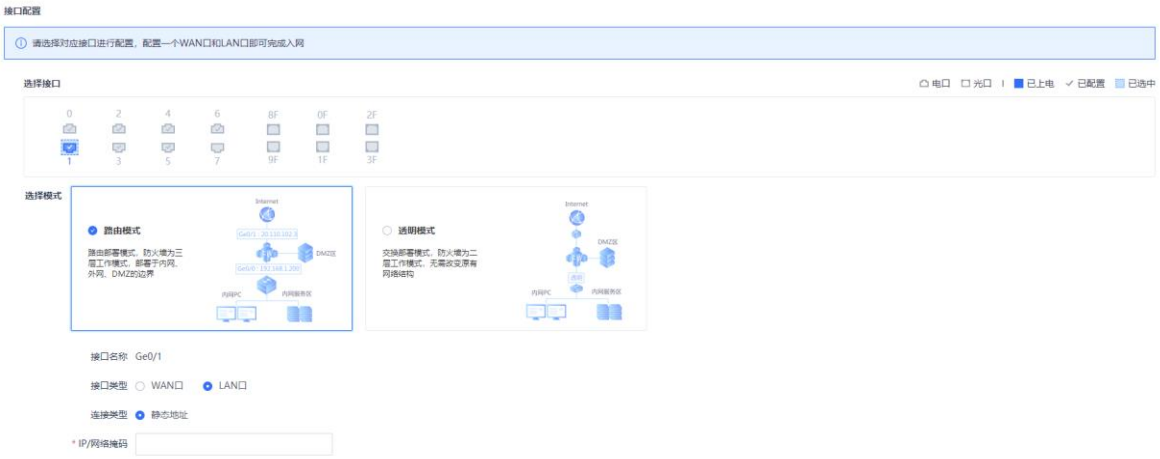
【操作步骤】

(1) 在操作及面板区右侧，点击<快速上线>。

系统弹出[快速上线向导]页面。



(2) 配置LAN口。



a 在“选择接口”区域，选择作为LAN口的接口。

b 在“选择模式”区域，选择路由模式。

c 设置LAN口相关的配置项。

配置项	说明	配置方法
接口名称	选择配置的接口名称。	系统自动显示接口的名称。 [示例] Ge0/6
接口类型	LAN口 :适用于连接内网中的设备场景 ,主要是用来连接电脑、交换机、打印机等设备。	[示例] LAN口

配置项	说明	配置方法
连接类型	接口的连接类型，包括： ● 静态地址 :适用于网络管理员根据预先定义好的IP地址规划来分配给设备的场景 ,要求网络管理员拥有一定的网络知识。需要配置IP/网络掩码和下一跳地址。	[示例] 静态地址
IP/网络掩码	接口的IP地址及网络掩码。	当“连接类型”设置为“静态地址”时，需要配置该参数。 [示例] 192.168.20.1/24
帐号/密码	拨号上网时，使用的用户名和密码。 一般由运营商分配。	当“连接类型”设置为“PPPOE”时，需要配置该参数。 [示例] Admin/Ruijie@123

(3) 配置WAN口。

a 在“选择接口”区域选择作为WAN口的接口。

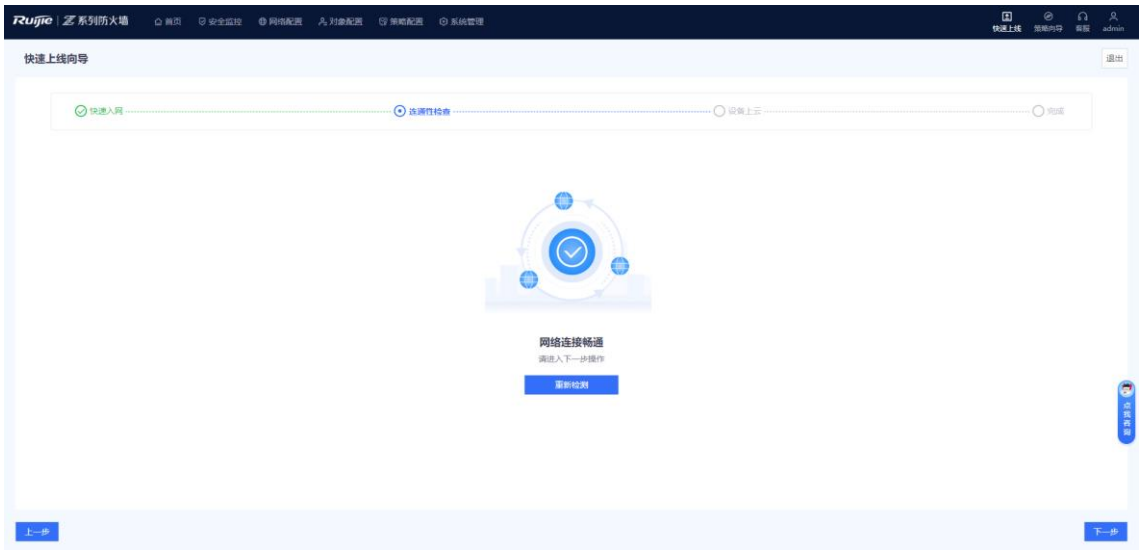
b 在“选择模式”区域，选择路由模式。

c 设置WAN口相关的配置项。

配置项	说明	配置方法
接口名称	选择配置的接口名称。	系统自动显示接口的名称。 [示例] Ge0/7
接口类型	WAN口：适用于连接外网，用于将防火墙接入Internet，它一般和运营商的入户光猫直连。	[示例] WAN口
连接类型	接口的连接类型，包括： ● 静态地址：适用于网络管理员根据预先定义好的IP地址规划来分配给设备的场景，要求网络管理员拥有一定的网络知识。需要配置IP/网络掩码和下一跳地址。 ● DHCP：适用于非专业的网络管理人员，用户通过连接防火墙就可以自动获取上网IP的场景。 ● PPPOE：适用于连接运营商网络需要拨号上网的场景。需要配置用户名和密码。	[示例] 静态地址
IP/网络掩码	接口的IP地址及网络掩码。	当“连接类型”设置为“静态地址”时，需要配置该参数。 [示例] 192.168.20.1/24
下一跳地址	要到达目的地址路由器所通过的下一个路由器地址。	当“连接类型”设置为“静态地址”时，需要配置该参数。 [示例] 192.168.20.2/24
帐号/密码	拨号上网时，使用的用户名和密码。 一般由运营商分配。	当“连接类型”设置为“PPPOE”时，需要配置该参数。 [示例] Admin/ Ruijie@123

d 配置完成后，点击<下一步>。

(4) 系统自动检测防火墙设备是否已经与Internet连通。如果与Internet连通，点击<下一步>。



说明

如果与Internet未连通，点击<上一步>修改接口配置。

(5) 在[设备上云]页面根据页面提示，开启相关的云管平台功能并进行设备绑定。

说明

如果设备未连接互联网，可以参见10 对接诺客云执行对接云管操作。

(6) 点击<完成>，快速上线配置完成。

【效果验证】

将设备的Ge0/1口连接光调制解调器（也称光猫），通过管理口登录设备，点击[系统管理]>>[故障诊断]>>[Ping诊断]菜单项，如图3-1所示设置相关诊断参数并点击<开始诊断>。

图3-1 Ping 诊断示例

如果"诊断结果"区域，显示设备能正常访问外网，表示快速上线功能配置成功。

2. 快速上线（透明模式）

【应用场景】

当规划使用透明模式时，通过执行以下操作使设备快速上线。

【前置条件】

配置一个LAN口和一个WAN口即可实现快速上网，请提前规划对应的物理接口。

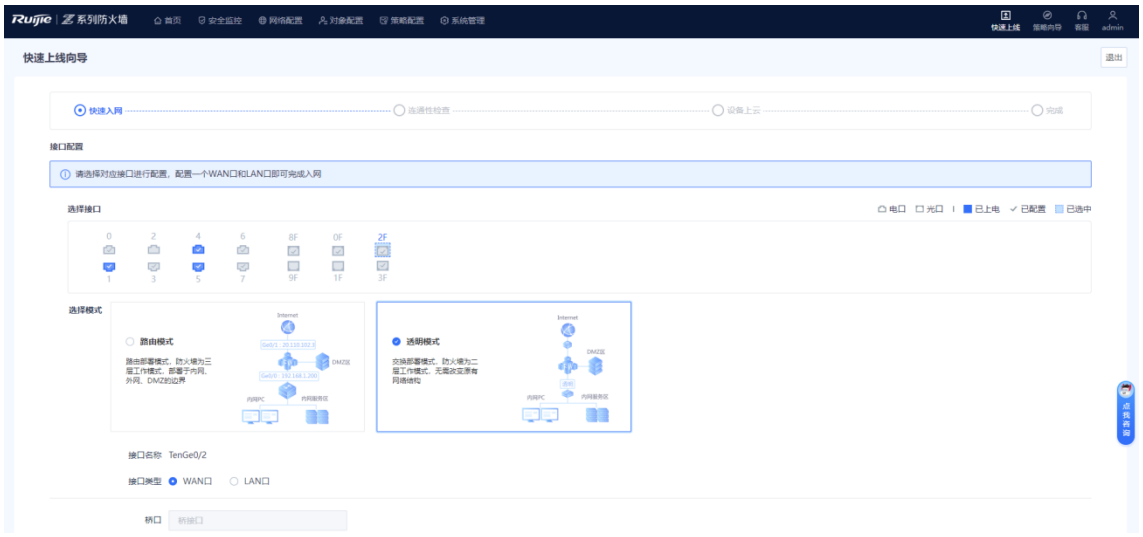
说明

管理口不支持设置为透明模式。

【操作步骤】

(1) 在操作及面板区右侧点击<快速上线>。

系统弹出[快速上线向导]页面。



(2) 配置WAN口。

a 在“选择接口”区域，选择作为WAN口的接口。

b 在“选择模式”区域，选择透明模式。

系统自动显示接口名称。

c 将“接口类型”设置为“WAN口”。

(3) 配置LAN口。

a 在“选择接口”区域，选择作为LAN口的接口。

b 在“选择模式”区域，选择透明模式。

系统自动显示接口名称。

c 将“接口类型”设置为“LAN口”。

(4) 设置桥口。

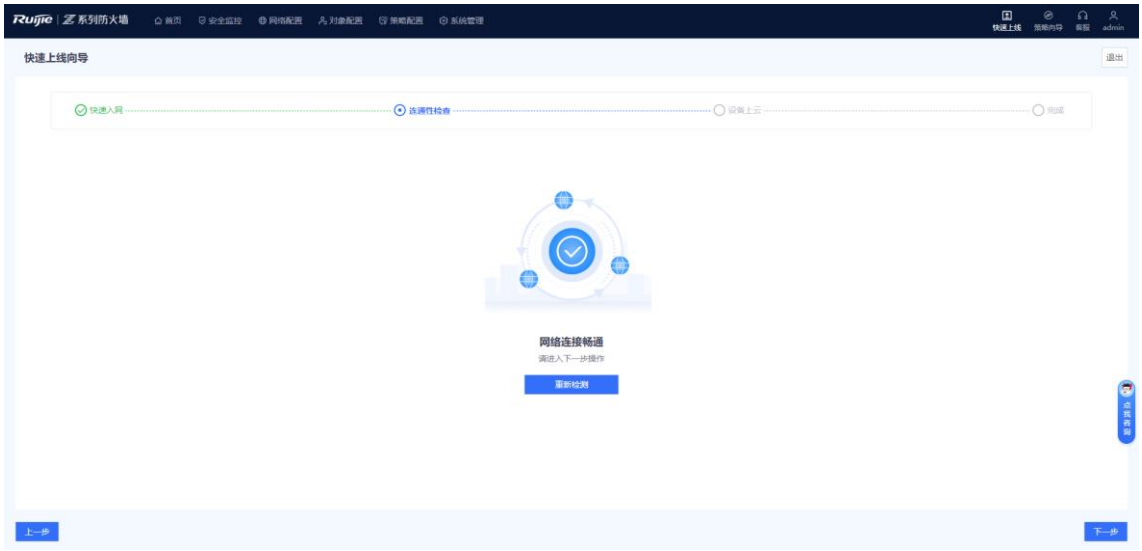
a 设置桥口相关配置项。

配置项	说明	配置方法
桥口	桥口名称。	系统默认将配置为透明模式的接口设置为桥口，且不支持修改。 [示例] 桥接口
接口成员	桥接口中的成员接口。	系统默认将配置为透明模式的接口设置为桥口的接口成员。 [示例] Ge0/8,Ge0/9
连接类型	接口的连接类型，包括： ● 静态地址：适用于网络管理员根据预先定义好的IP地址规划来分配给设备的场景，要求网络管理员拥有一定的网络知识。需要配置IP/网络掩码和下一跳地址。 ● DHCP：适用于非专业的网络管理人员，用户通过连接防火墙就可以自动获取上网IP的场景。	[示例] 静态地址

配置项	说明	配置方法
IP/网络掩码	接口的IP地址及网络掩码。	当“连接类型”设置为“静态地址”时需要配置该参数。 [示例] 192.168.20.1/24
下一跳地址	要到达目的地址路由器所通过的下一个路由器地址。	“连接类型”设置为“静态地址”时需要配置该参数。 [示例] 192.168.20.2/24

b 配置完成后，点击<下一步>。

(5) 系统自动检测防火墙设备是否已经与Internet连通。如果与Internet连通，点击<下一步>。



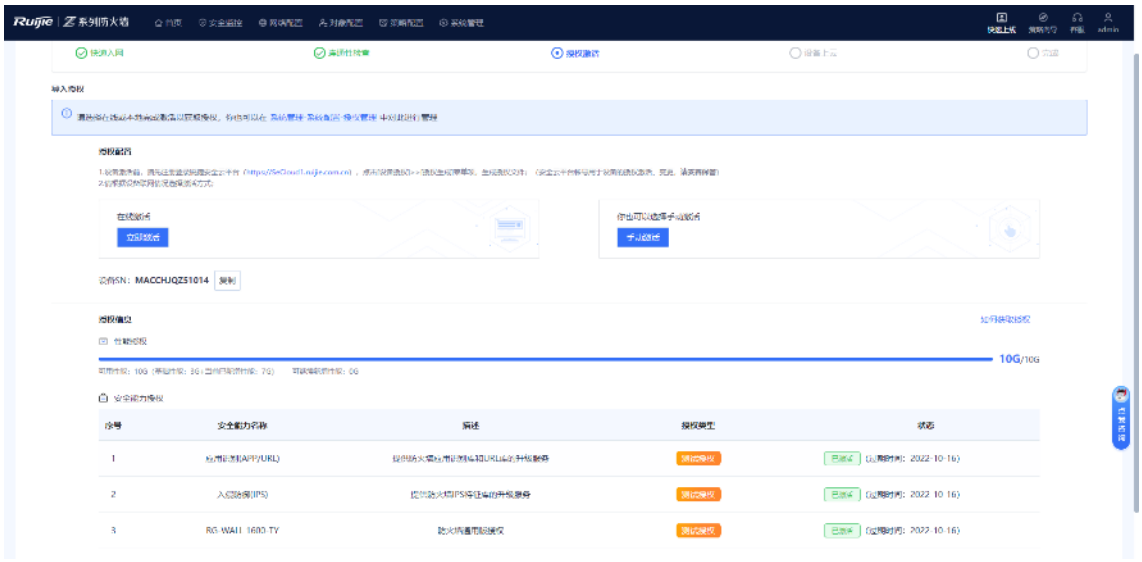
说明

如果与Internet未连通，点击<上一步>，重新配置相关参数后再进行检查。

(6) （可选）出现[授权激活]页面，设备自动向安全云平台发起授权激活。完成对应操作后，点击<下一步>。

根据设备的联网及行业基础授权激活情况，系统可能出现以下提示信息：

- 当设备未联网时，系统提示“设备授权未激活”。快速上线完成后，可手动进行授权激活，具体操作请参见8.3 激活授权。
- 当设备正常联网且未激活行业基础授权时，系统会弹出[授权激活]页面自动向安全云平台发起授权激活，请求激活行业属性授权。



(7) （可选）如果设备能访问互联网，且激活了通用版授权，则系统显示MACC上云界面。请根据界面提示，开启相关的云管平台功能并进行设备绑定。

说明

如果设备未连接互联网，可以参见10 对接诺客云执行对接云管操作。

(8) 点击<完成>，快速上线配置完成。

【效果验证】

将设备的Ge0/1口连接光调制解调器（也称光猫），通过管理口登录设备，选择[系统管理]>>[故障诊断]>>[Ping诊断]菜单项，如图3-2所示设置相关诊断参数并点击<开始诊断>。

图3-2 Ping 诊断示例

如果"诊断结果"区域，显示设备能正常访问外网，表示快速上线功能配置成功。

3.2.2 使用向导配置安全策略

Z-S系列防火墙的Web界面提供的策略配置向导，可以高效完成配置部署。

执行以下操作，进入"策略配置"向导：

(1) 在标识和面板区右侧，点击<策略向导>。

(2) 点击<开始策略配置>，进入[策略配置向导]页面，按照向导完成对应的操作。

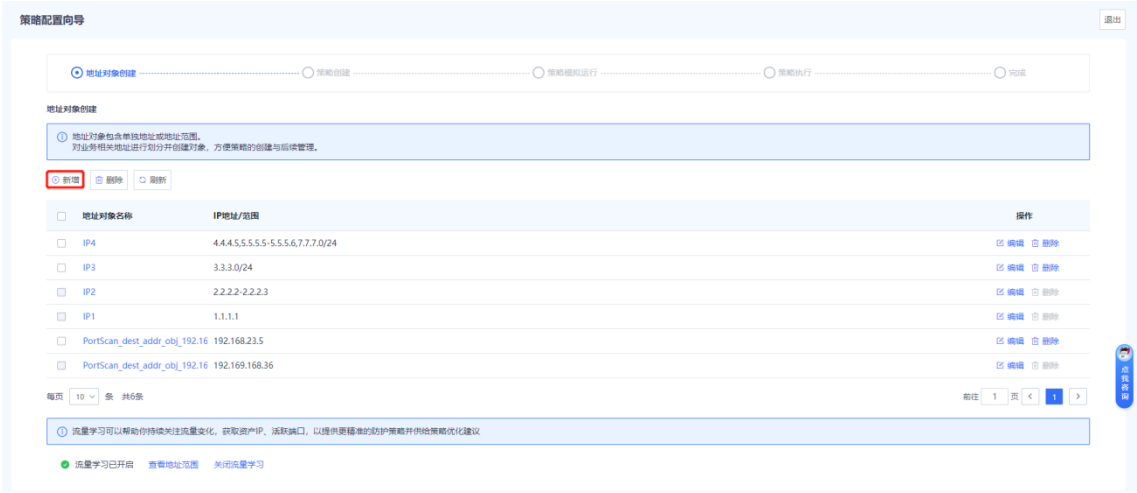
1. 创建地址对象

【应用场景】

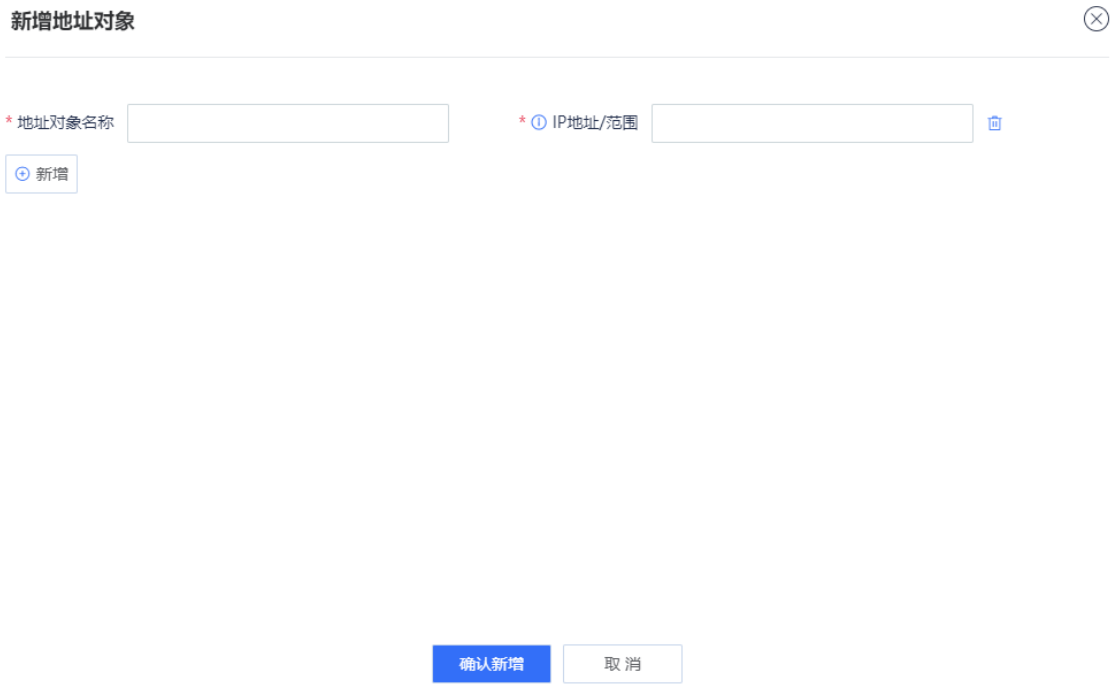
通过地址对象可以对业务相关的IP地址（包括内部网络或者外部网络的IP地址）进行划分，方便后续管理指定IP范围的流量。

【操作步骤】

(1) 在[地址对象创建]页面，点击<新增>。



(2) 在[新增地址对象]页面，填写名称和IP地址/范围等信息。



配置项	说明	配置方法
地址对象名称	IP地址对象的名称。	[示例] Addr1
IP地址/范围	IP地址或范围。	支持如下三种配置方式： ● IP地址：一个或多个IP地址。每行输入一个IP地址，如果输入多个IP地址时，使用回车键空行。例如：192.168.20.3 ● IP范围：同一个地址段中的范围，用-进行连接。例如：192.168.20.1~192.168.20.3。 ● 网段：IP网段。例如：192.168.1.0/24或192.168.1.0/255.255.255.0。

说明

如果需要新增多个地址对象，点击<新增>。

(3) 点击<确认新增>。

(4) 选择地址对象，点击<下一步>。

【后续处理】

- 管理员还可以通过[对象配置]>>[地址]菜单查看、新增、编辑和删除地址对象。
- 管理员只能删除引用情况为0的地址。

2. 配置安全策略

【应用场景】

根据界面向导，完成配置安全策略。

安全策略可以对通过防火墙的数据流进行校验，符合安全策略的合法流量才能通过防火墙进行转发。通过安全策略提供安全防护，例如：防火墙处于内外部网络连接处，通过安全策略建立内外网络之间的指定通道，从而过滤敏感的数据访问。

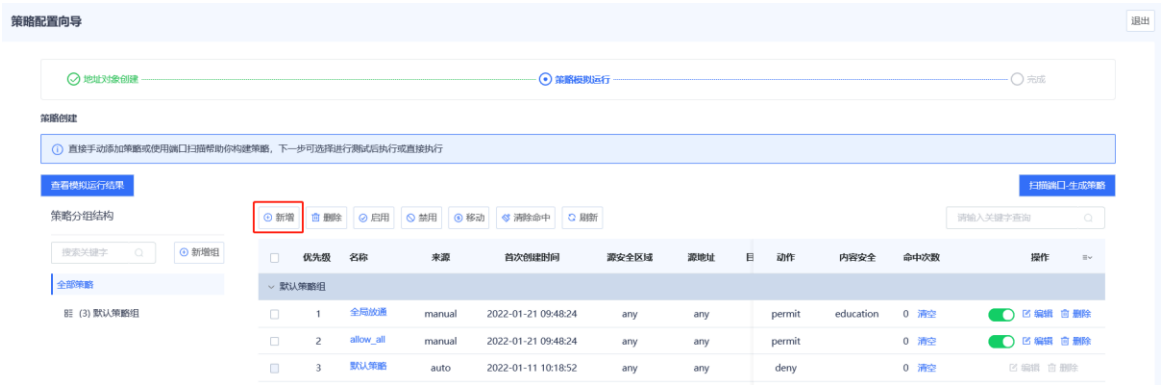
【前置条件】

根据业务需要，已经提前创建安全区域、服务、服务组、应用组、时间计划、入侵防御策略。

- 创建安全区域的具体操作，请参见7.2 安全区域。
- 创建服务的具体操作，请参见6.3.2 自定义服务。
- 创建服务组的具体操作，请参见6.3.3 创建服务组。
- 创建应用组的具体操作，请参见6.2 应用。
- 创建时间计划的具体操作，请参见6.4 时间计划。
- 创建入侵防御策略的具体操作，请参见6.5.2 入侵防御。

【操作步骤】

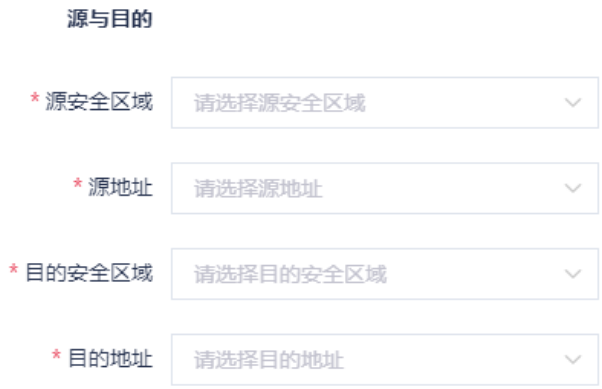
(1) 在[策略创建]页面，点击<新增>。



(2) 设置安全策略相关参数。

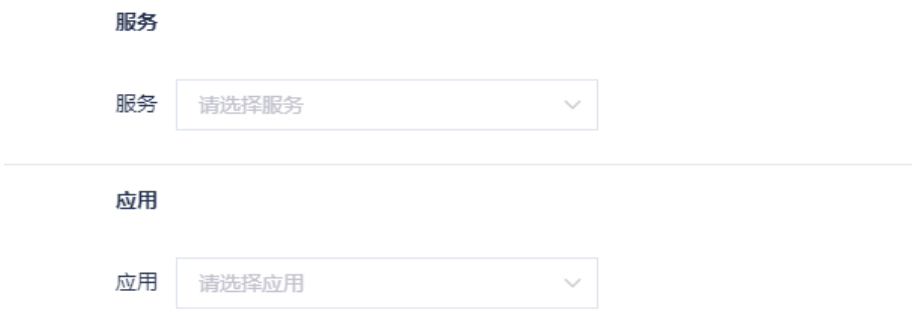
a 配置安全策略基础信息。

b 设置目标数据连接的源及目的安全区域及地址。



配置项	说明	配置方法
源安全区域	目标数据连接发起的安全区域。	下拉选择。 [示例] untrust
源地址	目标数据连接的发起源地址。	在"待选"区域选择源地址，自动添加到"已选"区域。 [示例] Any
目的安全区域	目标数据连接的目的安全区域。	下拉选择。 [示例] trust
目的地址	目标数据连接的目的地址。	在"待选"区域选择源地址，自动添加到"已选"区域。 [示例] Any

c （可选）选择目标数据连接请求的服务、应用。



d （可选）选择当前策略的生效时间段。

e 设置安全策略的执行动作，允许或拒绝目标数据连接。

动作选项	说明
允许	如果设置为“允许”，根据是否启用内容安全检查进行处理： 不启用其内容安全检查：流量通过。 启用安全内容检查：根据安全内容检查策略对流量进行处理。
拒绝	禁止流量通过。

f 设置目标数据连接是否启用内容安全检查。

g 在“高级”区域点击<设置>，设置长连接属性并点击<确认>。

h 点击<保存>。

3. 模拟运行策略

【应用场景】

创建安全策略后可以进行模拟运行，提前发现策略的漏洞或问题，避免正式执行时对业务形成风险。

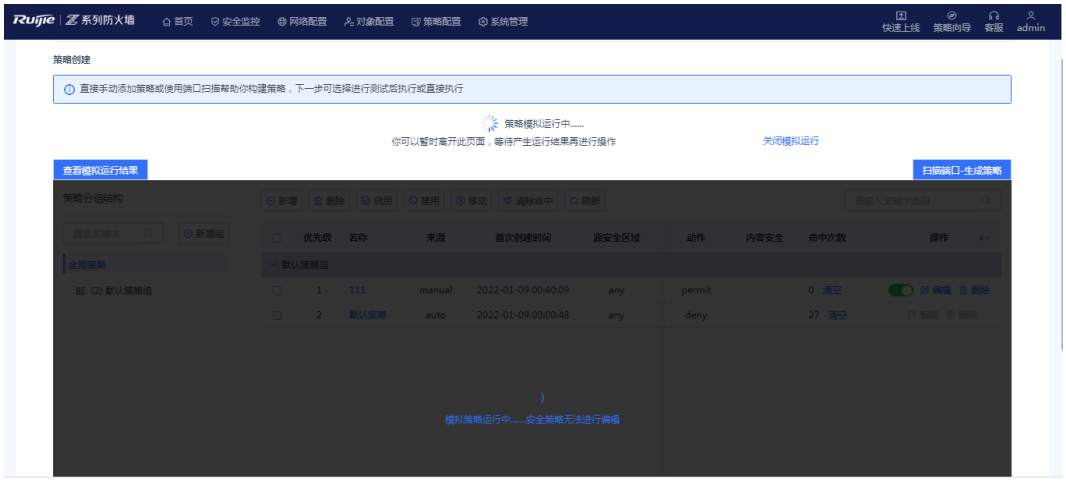
【操作步骤】

(1) 在[策略创建]页面，选择需要模拟运行的策略，点击 开始模拟运行 的图标。

(2) 在[设置模拟运行时长]页面，设置模拟运行时长。

(3) 点击<确认>。

系统自动对所选策略进行模拟分析。

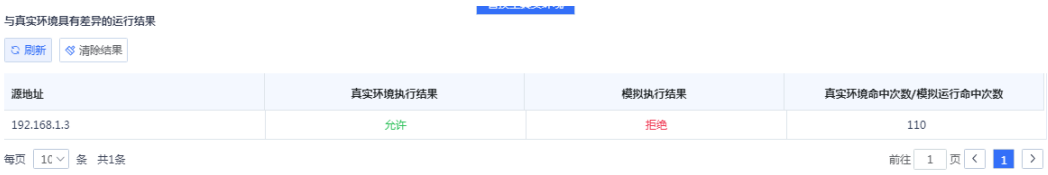


(4) 等待运行完成后，在[策略创建]页面，点击<查看模拟运行结果>。

模拟运行结果以源IP为单位，展示：

- 流量在真实策略中放行但在模拟策略中阻断的次数。
- 流量在模拟策略中放行但在真实策略中阻断的次数。

(5) 根据结果分析当前是否存在非期望差异。



(6) 当策略模拟效果符合预期，点击 替换至真实策略 图标，使当前创建的策略生效。

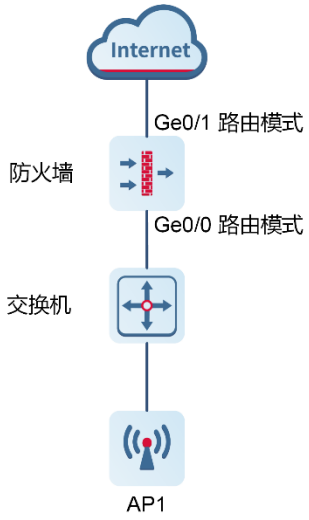
4 睿易一体化开局配置

由于防火墙设备功能比较复杂，在实际网络开局时，技术人员可能会遇到某些功能不会配置或配置失败的情况。因此，设备提供了急速开局功能（即发现新网络、整网管理和云管功能），可通过发现新网络功能将防火墙将入当前组网中，帮助用户快速完成设备的现场上线部署。遇到复杂业务无法配置时，也可以联系锐捷工程师通过诺客云平台进行远程配置。

4.1 防火墙设备开局（路由模式）

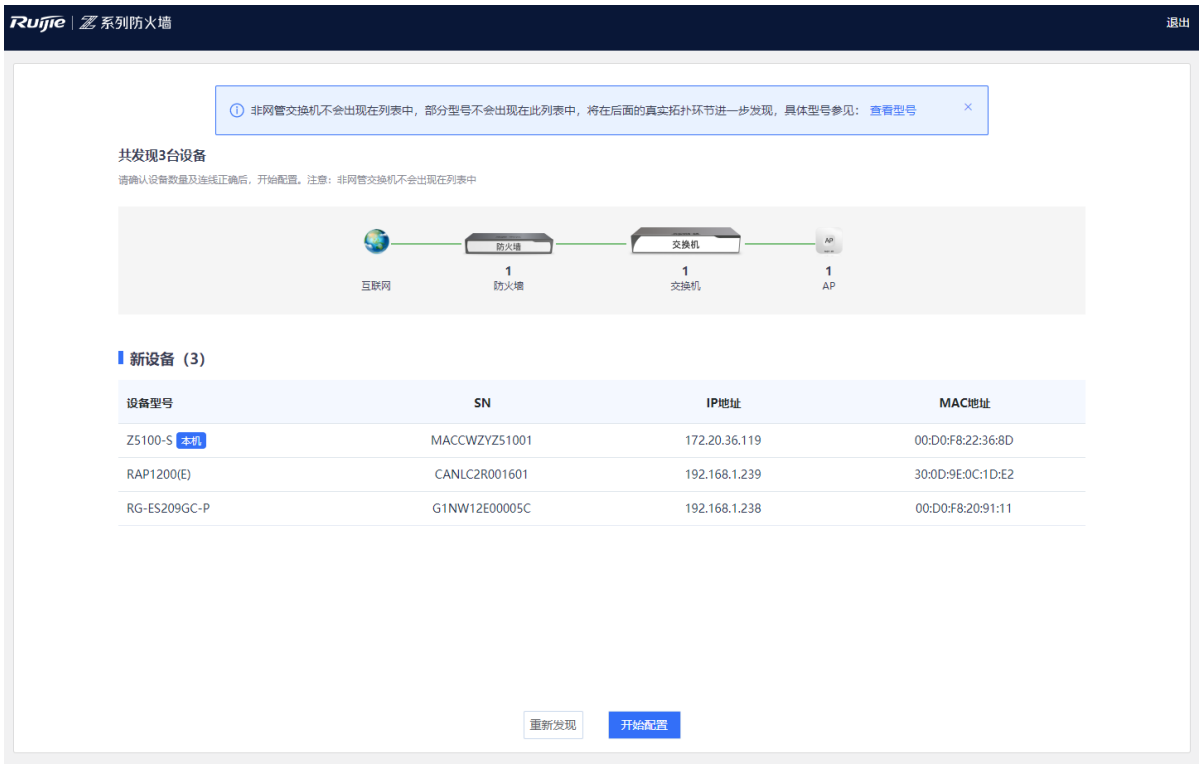
1. 应用场景

防火墙作为出口网关，上联互联网，下联交换机时，建议配置为路由模式。上行口配置为路由模式设置上网，下行口配置为路由模式。



2. 配置步骤

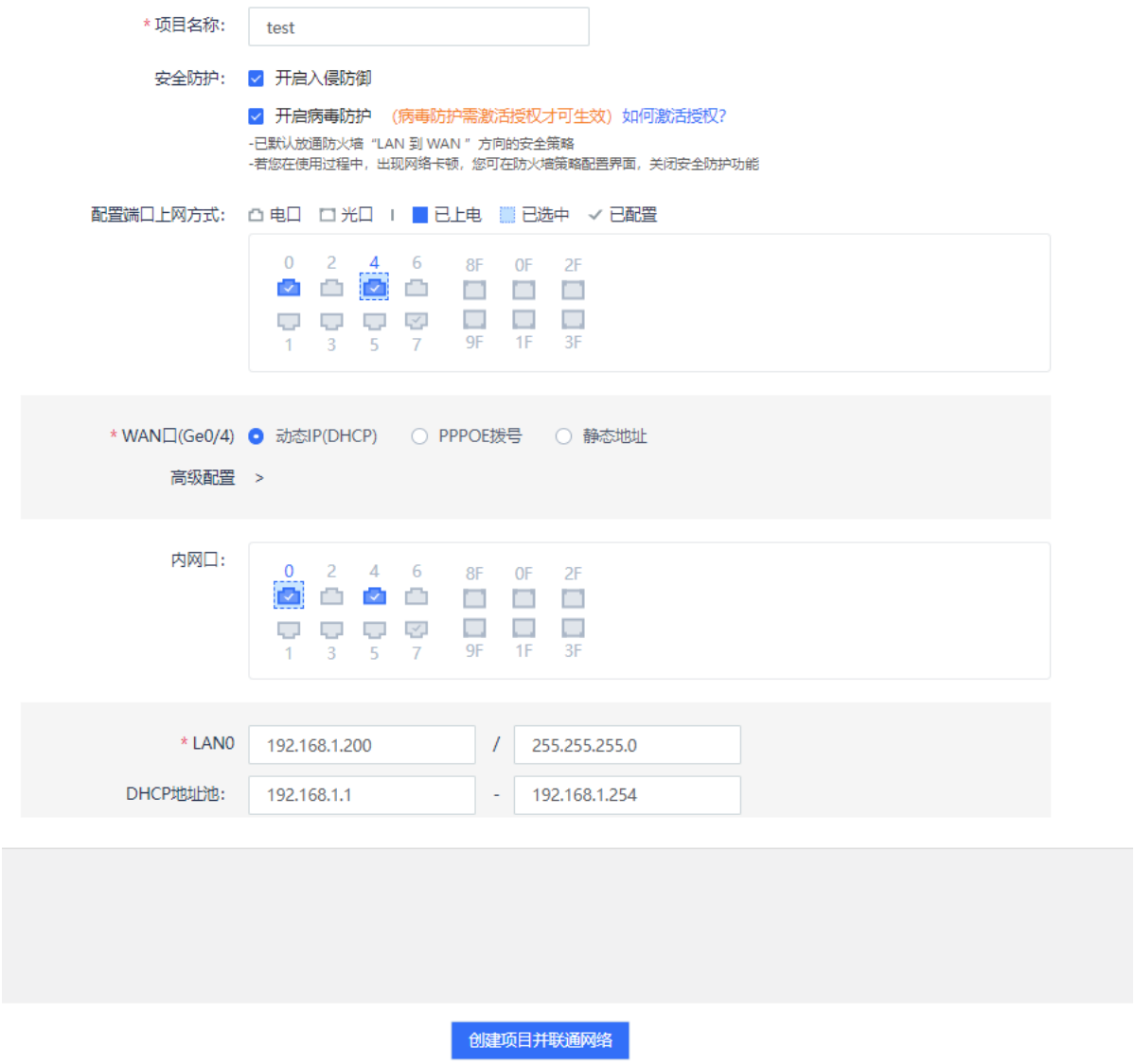
(1) 点击[发现新网络]菜单项，系统弹出界面显示当前组网信息。



(2) 点击<开始配置>，按照界面提示输入网络项目名称并配置端口IP。

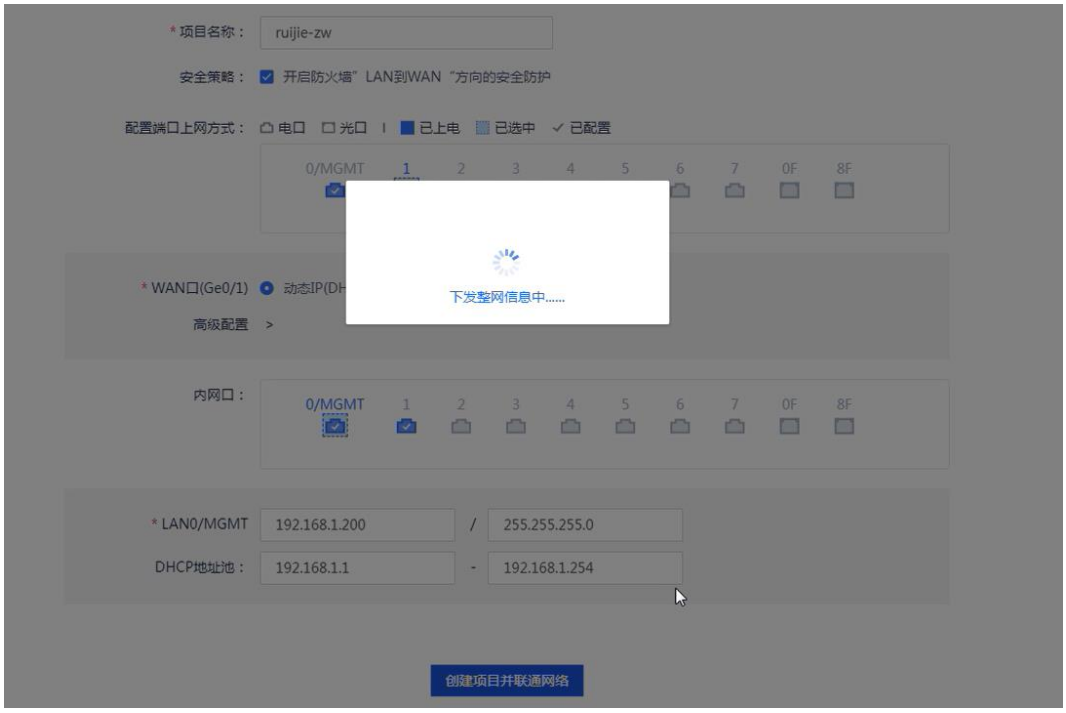
说明

- 设备默认开启了DHCP服务器功能，并在管理口下配置了默认的DHCP地址池。
- 设备默认开启入侵防御和病毒防护功能，您可以根据实际需求关闭该功能。其中，病毒防护功能需要安装授权才能生效，有关授权激活的详细介绍请点击“如何激活授权”，扫码查看授权激活视频。



配置项	说明	配置方法
WAN口	连接外网，用于将防火墙接入Internet，它一般和运营商的入户光猫直连。 WAN口的IP地址获取方式有三种： ● 动态IP（DHCP）：适用于非专业的网络管理人员，用户通过连接防火墙就可以自动获取上网IP的场景。 ● PPPOE：适用于连接运营商网络需要拨号上网的场景。需要配置用户名和密码。 ● 静态地址：适用于网络管理员根据预先定义好的IP地址规划来分配给设备的场景，要求网络管理员拥有一定的网络知识。需要配置IP/网络掩码和下一跳地址。	[示例] Ge0/4 动态IP（DHCP）
内网口	连接内网，根据预先定义好的IP地址规划设置内网口IP地址。	[示例] 192.168.1.1/24

(3) 点击<创建项目并连通网络>，系统下发配置信息。



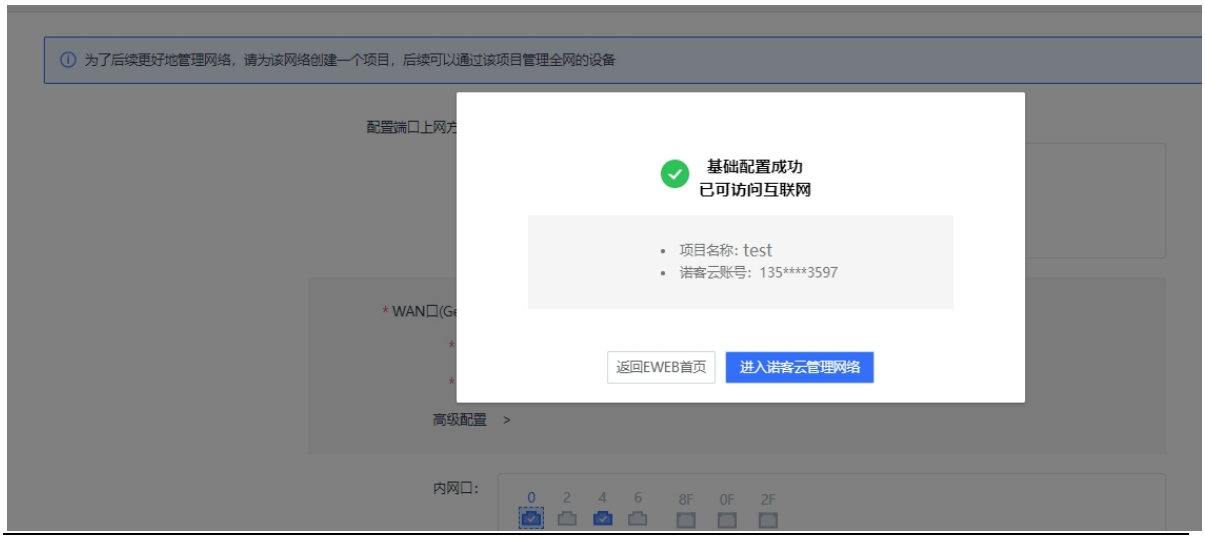
(4) 配置完成后，系统提示配置成功。可以扫码或手机号登录诺客云，完成设备上云操作。

说明

配置成功后，防火墙设备自动将组网中DHCP Server设备的IP地址加入白名单，并自动生成一条安全策略（策略名称为trust-untrust，且启用了入侵防御。）

说明

若设备已经绑定过诺客云平台，设备将会弹出如下页面。点击<进入诺客云管理网络>可直接进入诺客云平台进行设备管理，点击<返回EWEB首页>将会回到防火墙设备首页。



(5) 登录成功后，根据实际组网场景选择项目类型，点击<下一步>。不同类型的项目下发的初始配置不同，请根据实际业务场景选择。

(6) 等待配置前准备完成，进行下一步配置业务网。

(7) 等待所有设备上线后，点击<前往云平台>，进入诺客云平台进行业务配置。

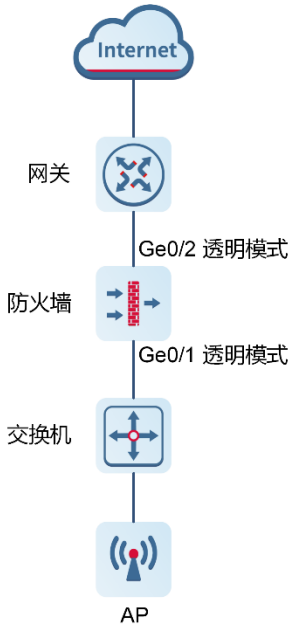
(8) （可选）业务配置完成后，在防火墙设备上点击[整网管理]菜单项，页面跳转到Master设备Web管理页面，用户可以在Master设备上查看当前组网拓扑及组网中的设备信息，并对全网设备进行管理。

Master设备[整网概览]页面如下图所示。

4.2 NBR 设备开局（透明模式）

1. 应用场景

防火墙上联网关，下联交换机时，建议配置为透明模式，防火墙上下行端口配置为透明模式。本例中的网关设备指代RG-NBR6210-E（以下简称NBR设备），实际业务场景中可以根据需求选择其他型号的网关设备。



2. 配置步骤

(1) 按图搭建组网环境后，将PC连接到NBR设备管理口，并设置PC网段与NBR设备管理口在同一网段，确保PC可以访问NBR设备Web页面。

说明

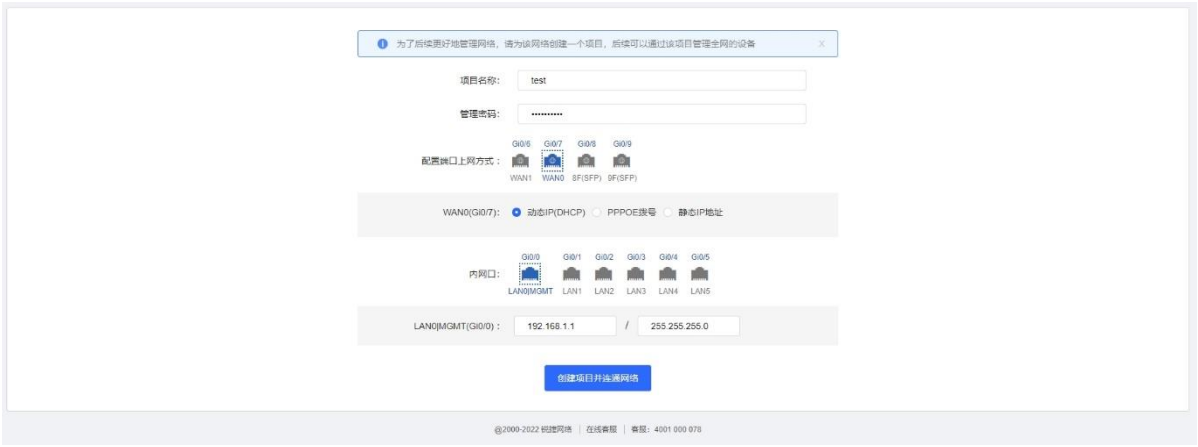
RG-NBR6210-E设备出厂设置了管理口Gi0/0的IP地址为192.168.1.1/24，默认登录账号密码为admin/admin。

(2) 登录NBR设备Web页面，设备默认进入如下页面。点击<开始配置>。

(3) 按照实际组网环境选择防火墙的WAN口（连接网关的接口，本例为Ge0/2），点击<下一步>。

(4) 按照实际组网环境选择防火墙的LAN口（连接交换机的接口，本例为Ge0/1），点击<NBR接口配置>。

(5) 配置下发成功后进入如下页面，输入项目名称和管理密码，点击<创建项目并连通网络>。



(6) 配置下发完成后，系统提示配置成功。可以扫码或手机号登录诺客云平台，完成设备上云操作。

(7) 登录成功后，根据实际组网场景选择项目类型（本例选择的类型为其他），点击<下一步>。不同类型的项目下发的初始配置不同，请根据实际业务场景选择。

(8) 等待配置前准备完成，进行下一步配置业务网。

(9) 等待所有设备上线后，点击<前往云平台>，进入诺客云平台进行业务配置，如配置接口、路由等。

说明

在诺客云平台上可以通过EWEB方式登录防火墙Web页面进行相关策略的配置。

防火墙设备上云后会自动将连接WAN、LAN口分别加入untrust、trust安全域，并生成一条允许trust到untrust安全域之间的报文通过的安全策略，并开启IPS检测。

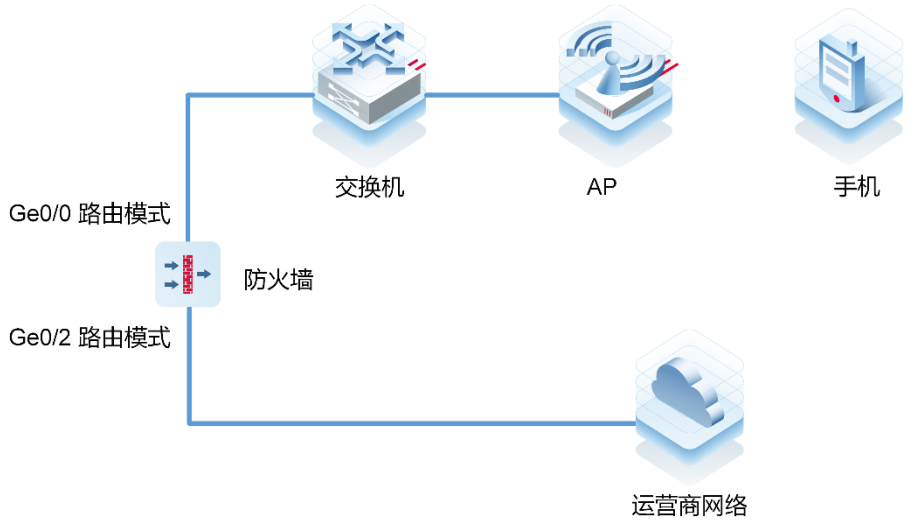
4.3 睿易 APP 开局（路由模式）

1. 应用场景

防火墙作为网关，上联互联网，下联交换机时，建议配置为路由模式。上、下行口配置为路由模式。

说明

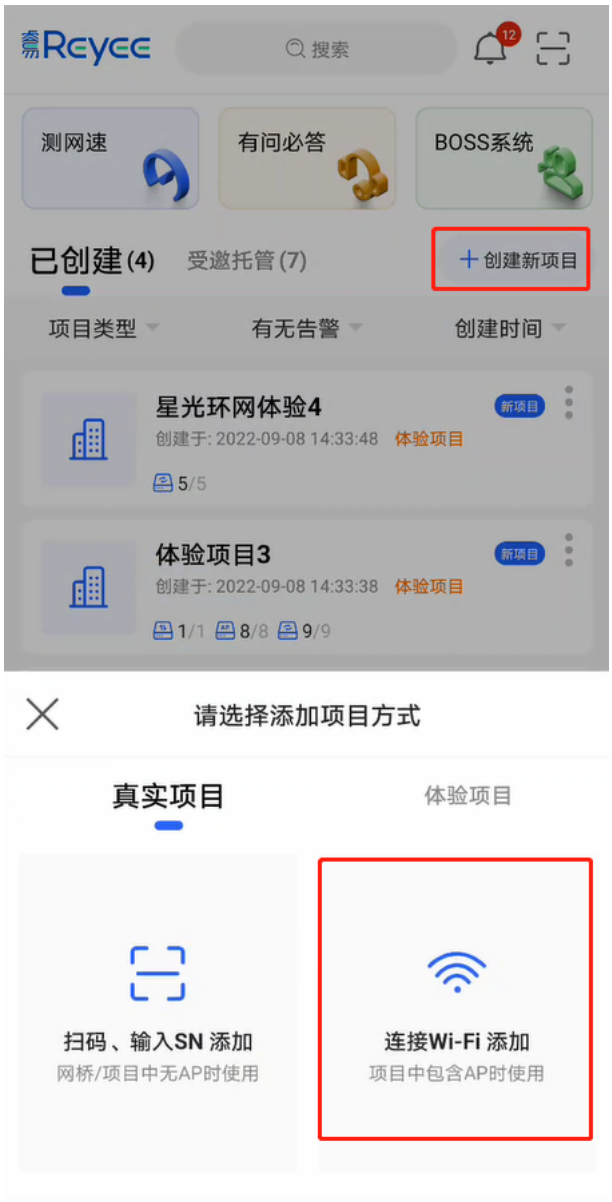
通过睿易APP连接Wi-Fi开局可以不连接PC。



2. 配置步骤

(1) 按图搭建网络环境后，打开睿易APP（易网络APP），点击项目，创建项目。

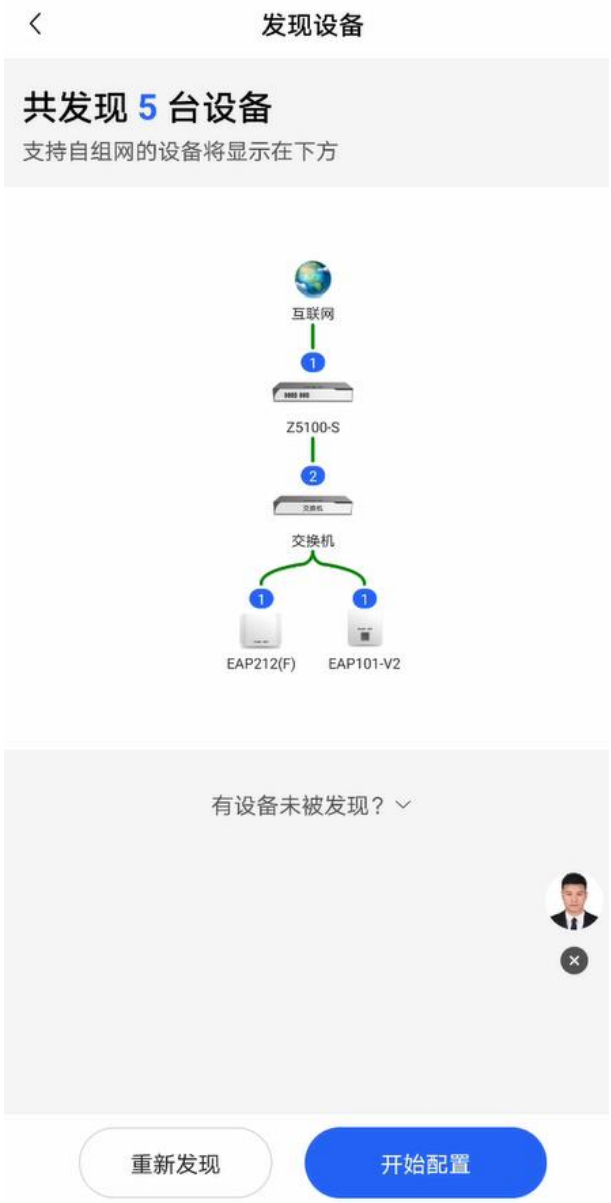
(2) 选择通过“连接Wi-Fi添加”方式添加项目。



(3) 点击“前往连接”，连接至睿易AP的Wi-Fi信号上。

创建新项目
连接Wi-Fi
1.请连接新项目放出的“@Ruijie-m”开头的Wi-Fi信号
无线局域网
@Ruijie-mXXXX
你的网络里只有1台无线AP或1台无线路由器吗？
不是，前往连接 “@Ruijie-mXXXX”
是的，继续下一步。
* 若项目中只有1台无线AP或1台无线路由器，请连接@Ruijie-s开头的Wi-Fi
去连接

(4) 等待30s左右，系统自动生成拓扑，点击<开始配置>。



(5) 输入项目名称和密码，点击<下一步>。

(6) 选中防火墙上连接互联网的接口（作为WAN口），并设置上网方式，点击<下一步>。

(7) 配置Wi-Fi，点击<下发配置>。

(8) 待配置下发成功后，连接新的Wi-Fi。

(9) 连接后将自动检测网络，并展示检测结果。

点击<查看项目详情>，点击拓扑图中的防火墙图标可以查看接口状态或修改设备名称。

防火墙_路由
通用解决方案
基础上网
已配置
终端管理
待开启
扫码连Wi-Fi
待开启
项目状态
优
已运行
0天0小时
在线设备: 5
离线设备: 0
现场
互联网
Z5100-S
交换机
EAP212(F)
EAP101-V2
在线终端
1
无线AP信道干扰情况
查看详情
100.00%
信道无干扰AP: 2

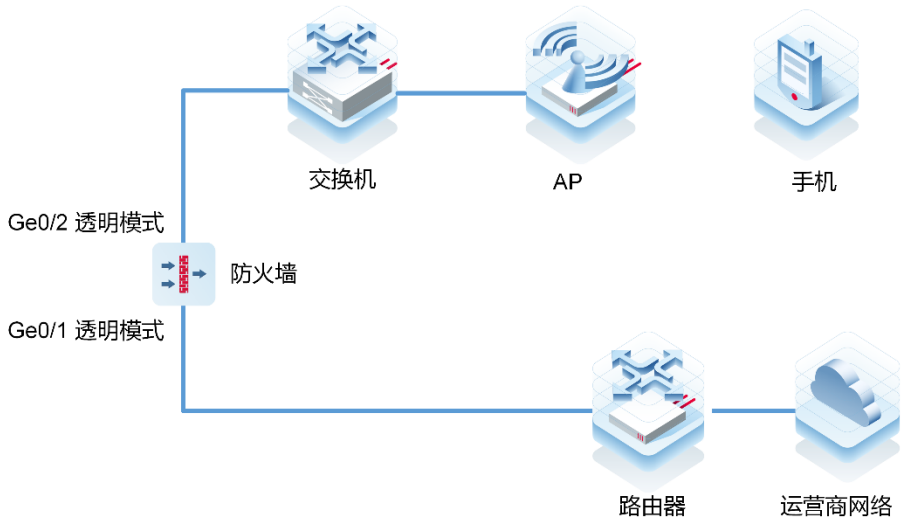
4.4 睿易 APP 开局（透明模式）

1. 应用场景

防火墙上联网关，下联交换机时，建议配置为透明模式，防火墙上下行端口配置为透明模式。

说明

通过睿易APP连接Wi-Fi开局可以不连接PC。



2. 配置步骤

(1) 按图搭建网络环境后，打开睿易APP（易网络APP），点击项目，创建项目。

(2) 选择通过“连接Wi-Fi添加”方式添加项目。

(3) 点击“前往连接”，连接至睿易AP的Wi-Fi信号上。

创建新项目
连接Wi-Fi
1.请连接新项目放出的“@Ruijie-m”开头的Wi-Fi信号
无线局域网
@Ruijie-mXXXX
你的网络里只有1台无线AP或1台无线路由器吗？
不是，前往连接 “@Ruijie-mXXXX”
是的，继续下一步。
* 若项目中只有1台无线AP或1台无线路由器，请连接@Ruijie-s开头的Wi-Fi
去连接

(4) 等待30s左右，系统自动生成拓扑，点击<开始配置>。

(5) 输入项目名称和密码，点击<下一步>。

(6) 选中防火墙上分别用于连接网关和交换机的接口，点击<下一步>。

(7) 配置Wi-Fi，点击<下发配置>。

(8) 待配置下发成功后，连接新的Wi-Fi。

(9) 连接后将自动检测网络，提示结果。

点击<查看项目详情>，点击拓扑图中的防火墙图标可以查看接口状态或修改设备名称。

防火墙_透明
通用解决方案
基础上网
已配置
终端管理
待开启
扫码连Wi-Fi
待开启
智能设
待开
项目状态
优
已运行
0天0小时
在线设备: 5
离线设备: 0
现场
互联网
NBR6205-E
Z5100-S
交换机
RAP2200(E)
在线终端
1
无线AP信道干扰情况
查看详情
工具箱

RG-WALL
Z5100-S
在线
MAC: 00:d0:f8:22:36:9b
IP: 192.168.1.200
软件版本：NGFW_NTOS Trunk, Release(02210601)
序列号：MACC893560130
端口状态
端口图示说明
0 2 4 6 8F 0F 2F
1 3 5 7 9F 1F 3F
端口
状态
0(Ge0/0)
192.168.1.200/24
1000M
1(Ge0/1)
断开
2(Ge0/2)
192.168.18.40/24
1000M
3(Ge0/3)
断开
4(Ge0/4)
断开
5(Ge0/5)
断开

5 策略配置管理

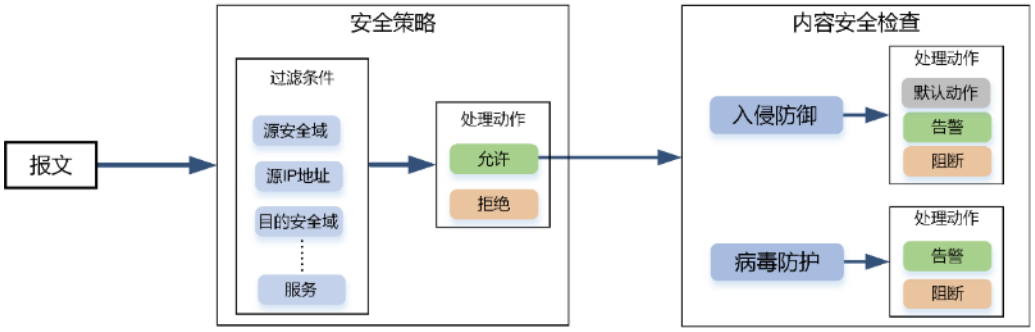
5.1 安全策略

5.1.1 简介

安全策略是根据报文属性对报文进行转发控制的防控策略。在安全策略中，可以设置报文的过滤条件（如源/目的安全域、源/目的IP地址、服务、应用等）、处理动作（允许、拒绝）及是否进行内容安全检查（包括入侵防御和病毒防护）。

设备默认配置了一条阻断所有报文的安全策略，默认策略不能删除或修改。

安全策略处理流程为如下图所示：



配置安全策略后，设备对收到的报文的处理流程如下：

(1) 将报文的属性信息与过滤条件进行匹配，多个过滤条件之间是与的关系，即同时满足多个过滤条件则成功匹配安全策略；当存在多个安全策略时，将按配置顺序逐条向下匹配，直到匹配成功；

(2) 匹配成功的报文将会按照处理动作进行转发（允许）或丢弃并记录安全日志（拒绝）；

(3) 若安全策略中启用了入侵防护或病毒防护，那么安全策略会将报文转发给入侵防护或病毒防护模块进行内容安全检查。

(4) 匹配入侵防御或防病毒策略的报文将会按照处理动作进行转发并记录安全日志（告警）或丢弃（阻断）；未匹配的报文则直接放行。

5.1.2 手动配置安全策略

【应用场景】

Z-S系列防火墙设备除了提供向导式的配置方式，还提供了手动配置方式，用户可以根据业务需要配置对应的安全策略。

【操作步骤】

(1) 点击[策略配置]>>[安全策略]菜单项。

(2) 在操作区，点击<新增>。

系统弹出“提示”信息。

(3) 点击<直接新增>。

系统弹出[新增安全策略]页面。

(4) 设置安全策略相关配置项。

配置项	说明	配置方法
基础信息		
名称	安全策略的名称。	不能包含字符：`~!#%^&*+\/0::"/<>?和空格。 [示例] Trust to untrust
启用状态	是否启用新增的安全策略。	[示例] 启用
策略组	新增安全策略所属策略组。	● 下拉选择。 ● 点击<新增组>，自定义新增策略组。 [示例] 默认策略组
策略位置	将新增的安全策略移动到指定策略之前或之后。策略越靠前匹配优先级越高。	-
描述	安全策略的描述信息。	描述不能包含字符：`~!#%^&*+|{};:'"/<>? [示例] 用于对安全域1到安全域2之间的HTTP流量进行病毒检测。
源与目的		
源安全域	目标数据发起的源安全区域。	● 点击下拉选项，在"待选"区域选择源安全域，自动添加到"已选"区域。 ● 点击<新增安全域>，自定义新增安全域。 [示例] trust
源地址	目标数据连接的发起源地址。	点击下拉选项，在"待选"区域选择源地址，自动添加到"已选"区域。 [示例] Any
目的安全区域	目标数据连接的目的安全区域。	● 点击下拉选项，在"待选"区域选择目的安全域，自动添加到"已选"区域。 ● 点击<新增安全域>，自定义新增安全域。 [示例] trust
目的地址	目标数据连接的目的地址。	在"待选"区域选择目的地址，自动添加到"已选"区域。 [示例] Any

配置项	说明	配置方法
服务	目标数据连接请求的服务类型。	[示例] Any
应用	目标数据连接请求的应用类型。	[示例] Any
时间段	安全策略生效时间段。	[示例] Any
动作	安全策略的执行动作，允许或拒绝目标数据连接。	[示例] 允许
内容安全	目标数据连接是否启用入侵防御和防病毒检查。 选择启用内容安全检查时，必须指定对应的入侵防御和防病毒模板，并设置执行动作。	[示例] ● 入侵防御：启用 ● 病毒防护：启用
高级	安全策略的高级配置选项，包括： 长链接：此选项适用于有长连接请求的特殊服务器。开启该功能后，服务器的连接请求不受防火墙设备连接超时影响。需要选择连接时长。	点击<设置>，在弹出的[高级选项]页面进行设置。 [示例] 勾选“长连接”

(5) 点击<保存>。

【后续处理】

- 安全策略、病毒防护策略、入侵防御策略命中后会记录对应的安全日志，您可以在[安全监控]>>[日志监控]>>[安全日志]页面查看生成的日志信息。
- 用户流量命中安全策略后，点击命中会话列的“查看详情”可以查看会话信息。

5.1.3 模拟运行策略

【应用场景】

创建安全策略后可以进行模拟运行，提前发现策略的漏洞或问题，避免正式执行时对业务形成风险。

【操作步骤】

(1) 点击[策略配置]>>[安全策略]菜单项。

(2) 在操作区点击

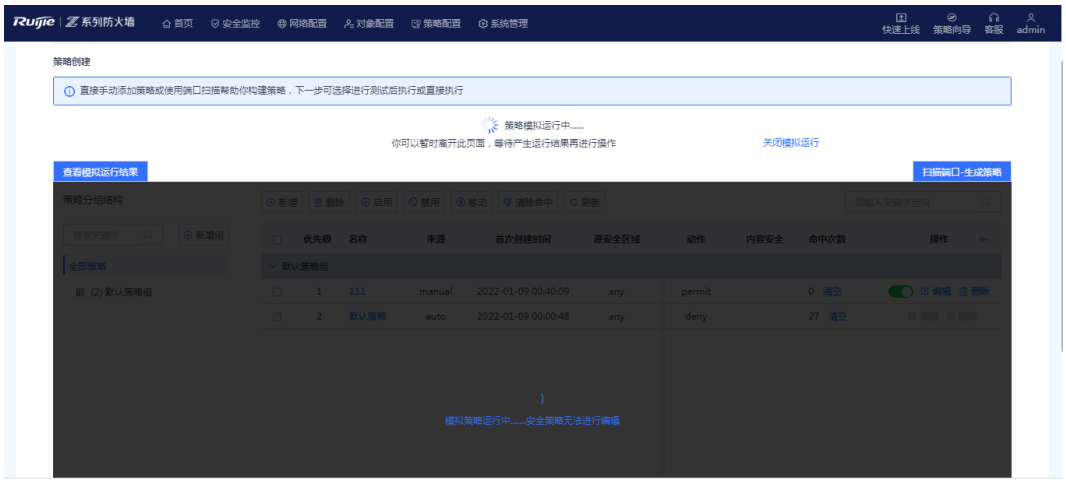
的图标。

(3) 选择需要模拟运行的策略，点击 开始模拟运行 的图标。

(4) 在[设置模拟运行时长]页面，设置模拟运行时长。

(5) 点击<确认>。

系统自动对所选策略进行模拟分析。



(6) 等待运行完成后，在[策略创建]页面，点击<查看模拟运行结果>。

模拟运行结果以源IP为单位，展示：

- 流量在真实策略中放行但在模拟策略中阻断的次数。
- 流量在模拟策略中放行但在真实策略中阻断的次数。

(7) 根据结果分析当前是否存在非期望差异。

(8) 当策略模拟效果符合预期，点击 替换至真实策略 图标，使当前创建的策略生效。

5.1.4 导入配置文件配置安全策略

【应用场景】

Z-S系列防火墙设备支持导入配置文件快速生成安全策略。

【前置条件】

可通过以下两种方式获取配置文件：

- 设备提供了配置文件模板，下载配置文件并根据业务情况进行修改。
- 如果要将原有设备的配置导入到Z-S系列防火墙设备中，可以通过配置策略迁移工具获取对应的配置文件。

说明

配置策略迁移工具的具体使用请联系技术支持工程师。

【操作步骤】

(1) 点击[策略配置]>>[安全策略]菜单项。

(2) 在操作区，点击<导入>。

系统弹出“提示”信息。

(3) 点击<下载示例CSV文件>，下载配置文件模板并填写对应的配置信息。

说明

配置文件修改后，请检查配置文件的命名规格，以满足系统的要求。配置文件的名称格式为：z5100-config-conversion-{yyyyMMddHHmmssSSS}.csv。

(4) 将配置文件拖至上传区域或点击<点击选择>将配置文件上传至设备中。

(5) 设置存在数据冲突时的处理方式。

当导入的数据和已有数据存在冲突时，可以采用以下处理方式：

- 显示冲突数据：系统会显示冲突的配置项及冲突原因，可根据提示信息修改配置文件。
- 跳过：系统忽略存在冲突的配置项，无需进行任何处理。

(6) 点击<确认导入>。

系统自动将配置文件中的信息写入设备，使配置生效。

5.1.5 调整安全策略顺序

【应用场景】

当配置多条安全策略规则时，安全策略列表默认是按照配置顺序排列的，越先配置的安全策略规则位置越靠前，优先级越高。安全策略的匹配就是按照策略列表的顺序执行的，即从策略列表顶端开始逐条向下匹配，如果流量匹配了某个安全策略，将不再进行下一个策略的匹配。

通过调整安全策略顺序，调整安全策略的优先级，使其更精准的与业务进行匹配。

说明

- 系统中存在一条默认安全策略，其优先级最低，阻断所有数据连接的策略。
- 当数据连接无法命中用户配置的策略时（命中默认策略），数据连接将会被阻断处理。

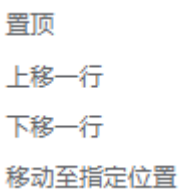
【操作步骤】

(1) 点击[策略配置]>>[安全策略]菜单项。

(2) 勾选待调整优先级的策略。

(3) 点击

图标，在快捷菜单主动选择对应的操作，移动选中的策略。



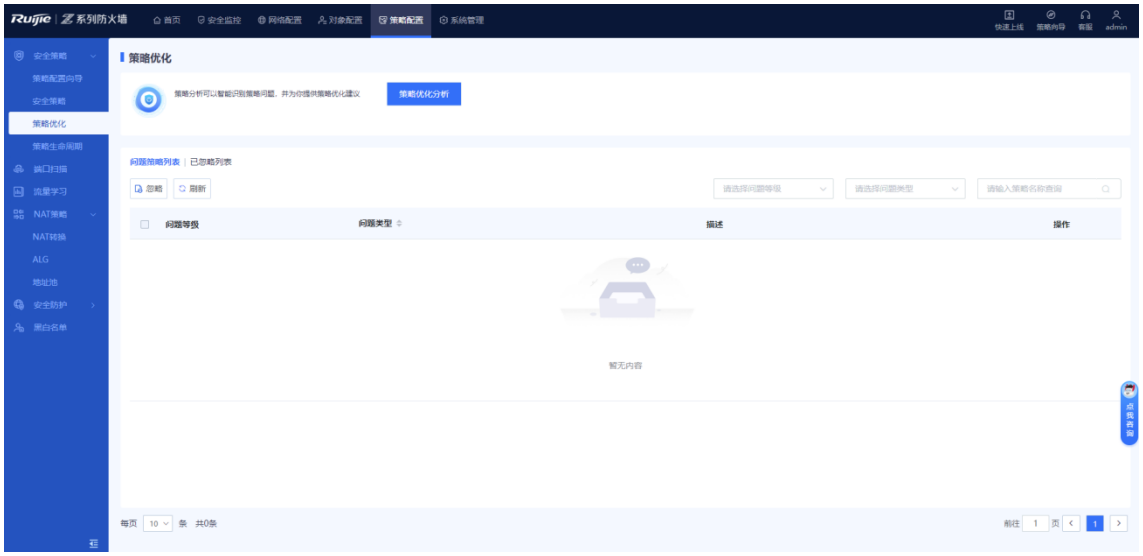
5.1.6 优化安全策略

【应用场景】

在日常的安全策略运维过程中，随着业务的累加、运维人员的变更等因素，安全策略的配置复杂度会越来越高。Z-S系列防火墙策略优化功能可以智能地对当前已配置的安全策略的过滤条件做比较分析，从而识别出冗余的策略，便于运维人员精简策略、优化策略，从而降低运维成本。

【操作步骤】

(1) 点击[策略配置]>>[安全策略]>>[策略优化]菜单项。



(2) 点击 的图标，开始对安全策略进行分析。

分析完成后，系统显示有问题的策略列表。

说明

使用策略优化对安全策略进行分析后，系统将问题等级分为3类：严重问题、一般问题和建议优化。

(3) 点击具体策略的 前往处理 的图标，查看策略的问题详情。

针对具体问题做详细的描述，系统显示具体危害，并提供相应的解决方案建议供运维人员做修订参考。

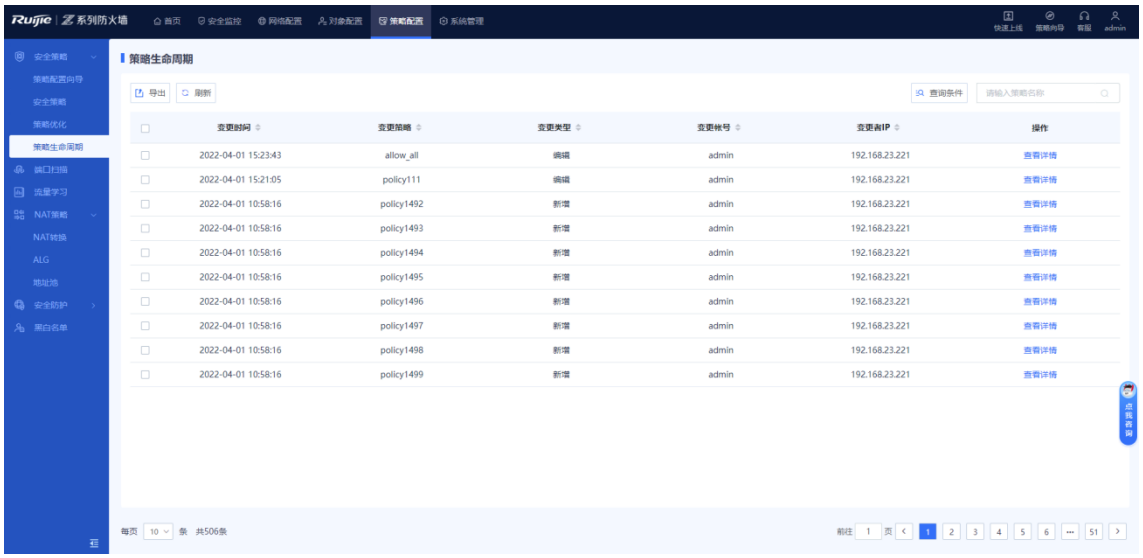
5.1.7 查看策略生命周期

【应用场景】

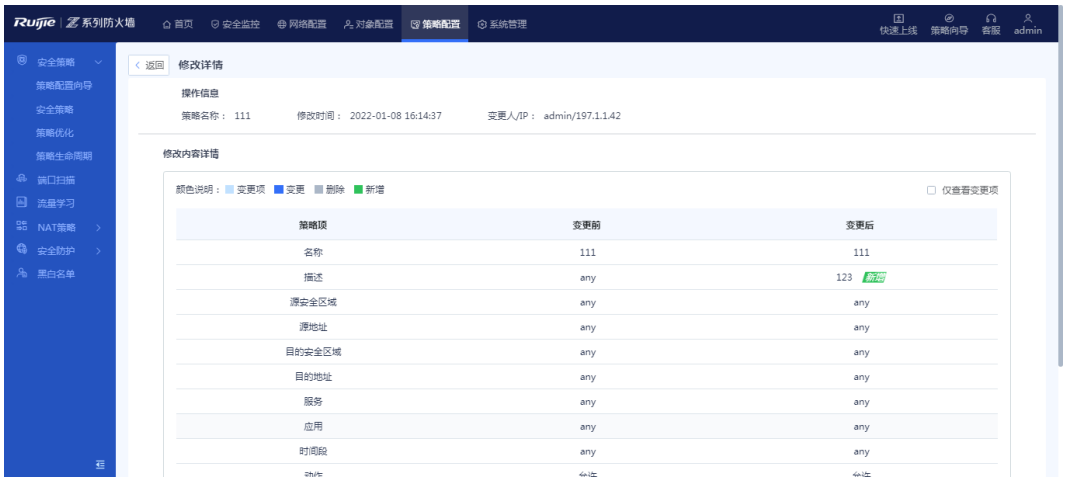
策略生命周期用于记录用户对安全策略的新增、修订、删除的详细记录，便于运维人员回溯问题。

【操作步骤】

(1) 点击[策略配置]>>[安全策略]>>[策略生命周期]菜单项。



(2) 点击<查看详情>，查看策略的具体变更详情。



5.2 开启基础协议报文控制功能

【应用场景】

通过本操作可以开启或关闭安全策略对基础协议报文的控制。

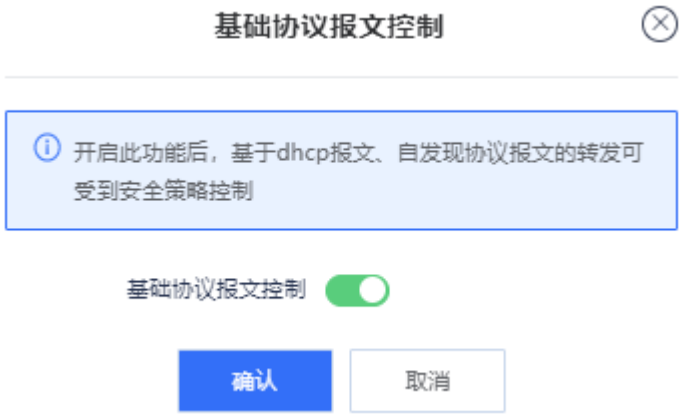
缺省情况下，防火墙对网络基础协议报文（例如：DHCP报文、自发现协议报文）不做安全策略控制，在无其他额外配置的情况下则直接转发，可以使设备快速接入网络。当希望基础协议通过配置安全策略来控制转发行为时，可以开启基础协议报文控制功能，使安全策略能够控制基础协议报文。

【操作步骤】

(1) 点击[策略配置]>>[安全策略]>>[安全策略]菜单项。

(2) 点击 。

(3) 在[基础协议报文控制]页面，开启“基础协议报文控制”开关。



(4) 单击<确认>。

5.3 开启端口扫描

【应用场景】

端口扫描功能可以帮助管理员快速地了解内网服务器的IP及开放的端口信息，并且可根据扫描结果选择是否生成安全策略，以便帮助构建企业内网的安全性。

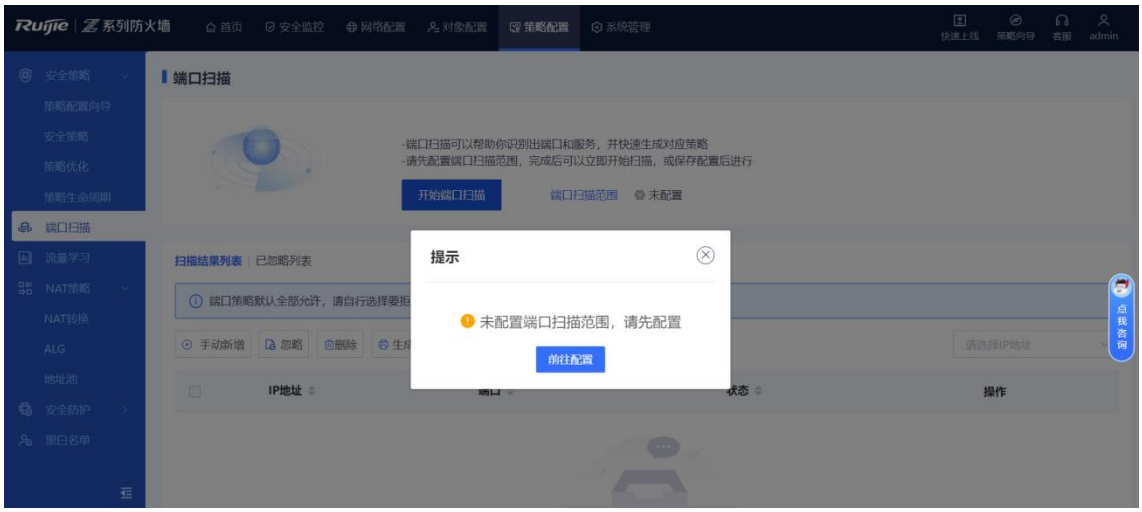
【操作步骤】

(1) 点击[策略配置]>>[端口扫描]菜单项。

(2) （可选）如果未配置端口扫描范围，请先进行配置。

a 点击<开始端口扫描>。

如果弹出提示"未配置端口扫描范围，请先配置"，点击<前往配置>。



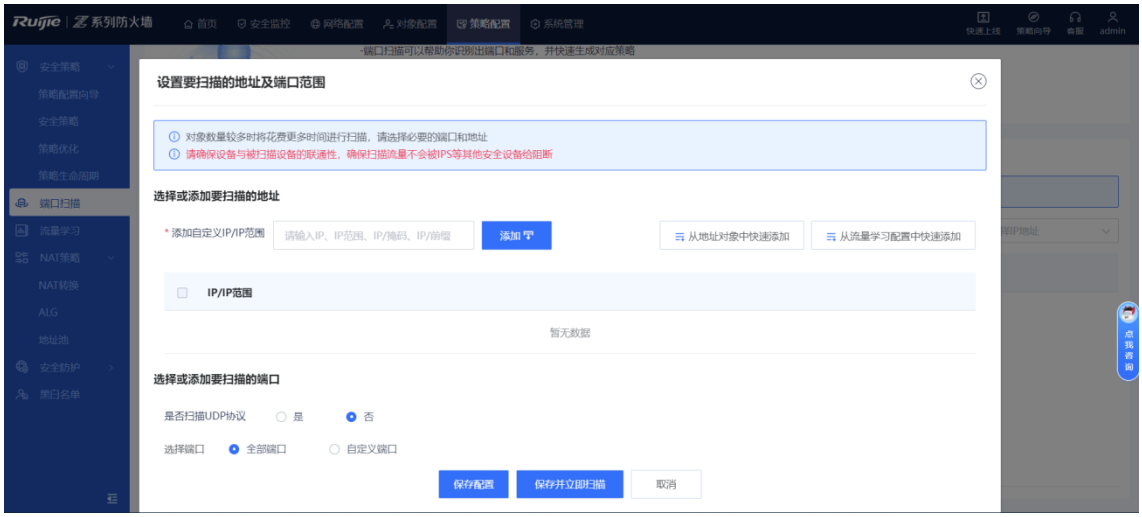
b 选择或添加要扫描的IP地址。

在"添加自定义IP/IP范围"框中填写需要扫描的IP地址网段，并点击<添加>将其添加到“IP/IP范围”区域。

说明

点击<从地址对象中快速添加>或点击<从流量学习配置中快速添加>可以快速添加IP地址。

c 选择或添加要扫描的端口。



配置项	说明	配置方法
是否扫描UDP协议	选择是否扫描UDP协议。	[示例] 开启

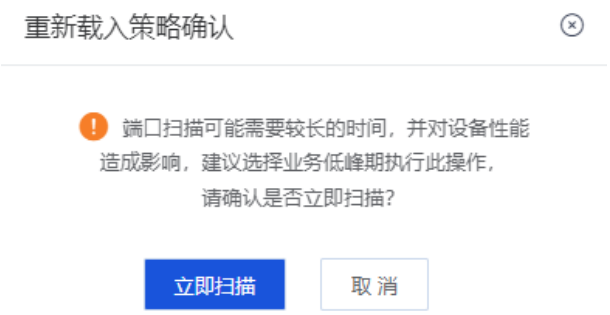
配置项	说明	配置方法
选择端口	选择需要扫描的端口： ● 全部端口：扫描所有端口。 ● 自定义端口：自定义需要扫描的端口。 ● 勾选"扫描常用端口（选择常用端口）"选择常用服务的端口。 ● 勾选"扫描自定义端口”，自定义添加需要扫描的端口。	[示例] 全部端口

d 根据业务情况，选择是否立即开启端口扫描功能。

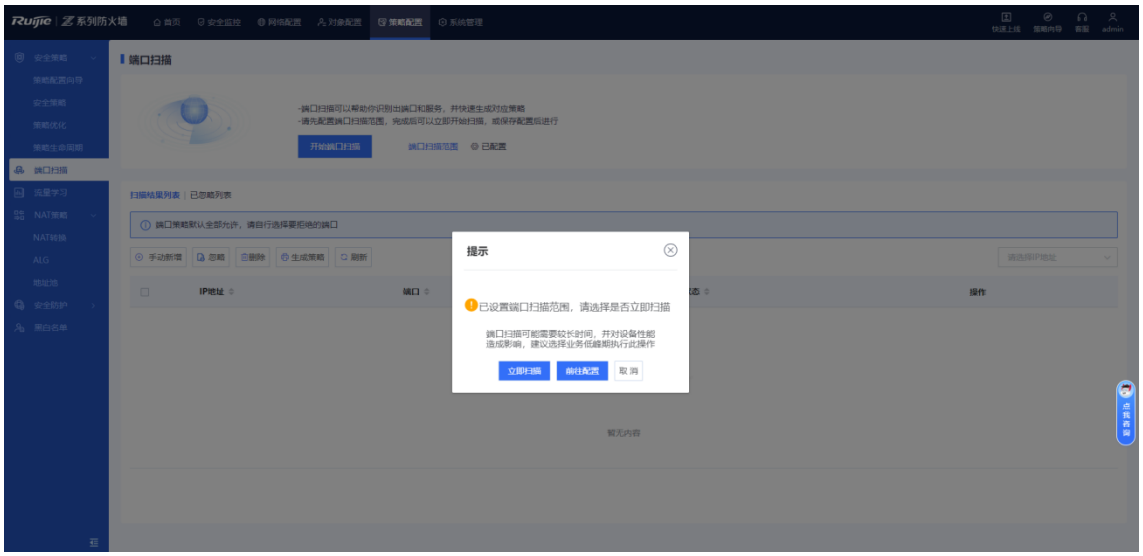
o 业务繁忙时，点击<保存配置>，保存端口扫描配置信息，并在稍后开启端口端口。

o 业务空闲时，点击<保存并立即扫描>，保存端口扫描配置信息并立即启动端口扫描功能。

确认系统提示信息，并点击<立即扫描>。

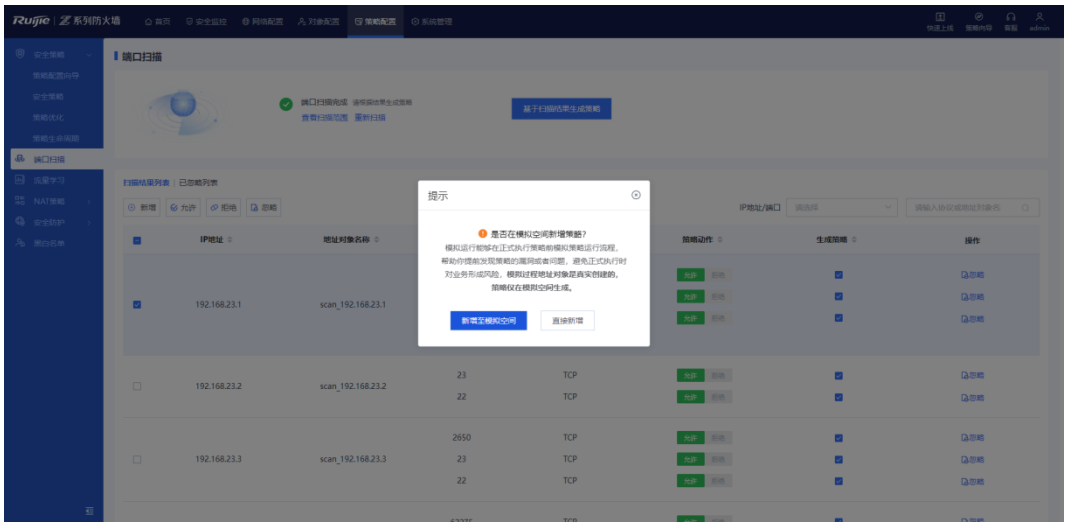


(3) （可选）如果已经配置了端口扫描策略，点击<开启端口扫描>启动端口扫描。

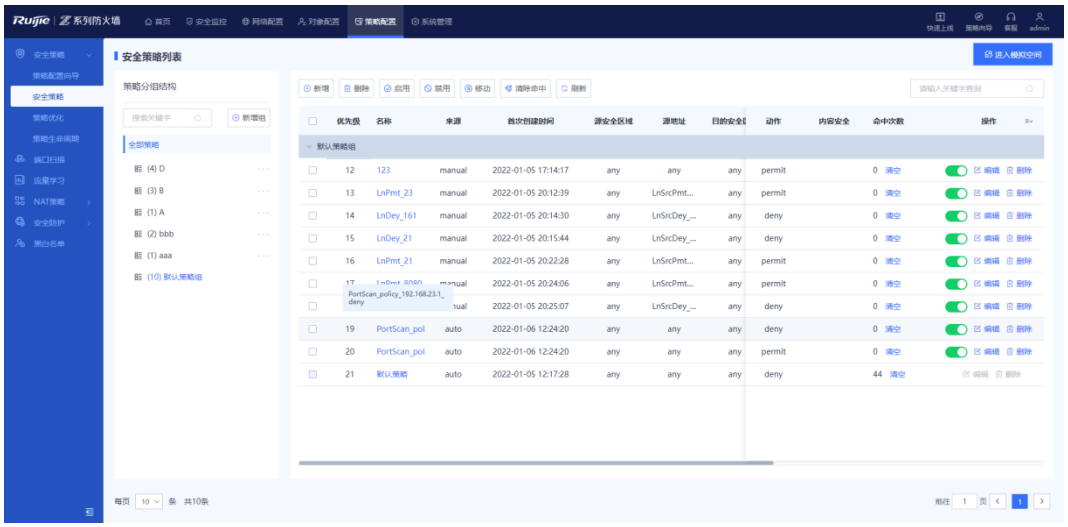


(4) 点击<立即扫描>。

扫描完成，点击<基于端口扫描结果生成策略>，勾选扫描结果并进行不同的处理。



- 点击<直接新增>，将生成的安全策略直接添加到安全策略列表中。



- 点击<新增至模拟空间>，将生成的策略添加至模拟空间，对该策略进行模拟运行后再添加到安全策略列表中。

【后续处理】

- 数标移动到扫描出来的端口号上，页面将展示常用端口的作用和高危端口存在的风险信息。
- 选择一个IP地址，点击操作列“生成策略”，可以生成针对该IP的安全策略；在端口扫描详情页可以设置安全策略动作，您也可以在安全策略页面编辑策略。
- 选择一个IP地址，点击操作列“查看详情”，可以查看该IP开发的端口号，并支持针对单个端口号生成安全策略。
- 选择一个IP地址，点击操作列“忽略”，可以将该IP的所有端口加入已忽略列表并设置忽略时长（也可以在端口扫描详情页将单个端口加入已忽略列表）。在忽略时长内，设备不再扫描这些端口；超过忽略时长后，端口将会被移出已忽略列表，此时，设备可对其进行扫描。
- 选择一个IP地址，点击操作列“删除”，可以删除该条扫描结果。

5.4 开启流量学习

【应用场景】

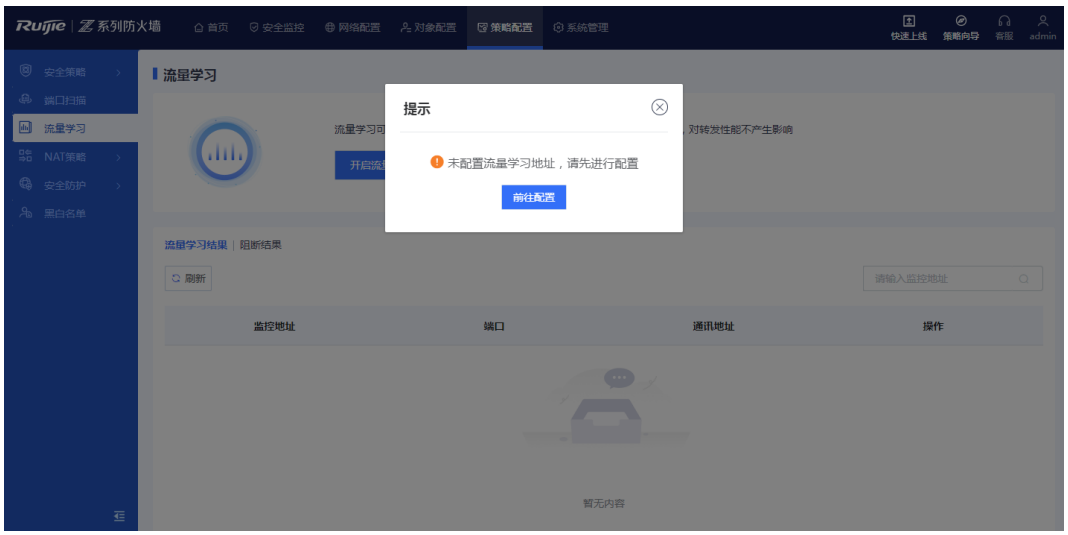
设备开局配置时，用户需要分析一段时间的流量日志后，才能梳理出当前网络中存在的资产。而流量学习功能自动分析流量日志，通过用户设定的需要分析的资产IP或IP范围，梳理当前网络中的资产IP、开放的端口和资产之间访问关系。

【操作步骤】

(1) 点击[策略配置]>>[流量学习]菜单项。

(2) （可选）如果未配置流量学习地址，请先进行配置。

a 点击<开启流量学习>，在提示框中点击<前往配置>配置流量学习地址。



b 选择或添加要学习的IP地址。

在"添加自定义IP"框中输入需要学习的IP地址范围，并点击<添加>将其加入"IP/IP范围"区域。

说明

点击<从地址对象中快速添加>或点击<从流量学习配置中快速添加>可以快速添加IP地址。

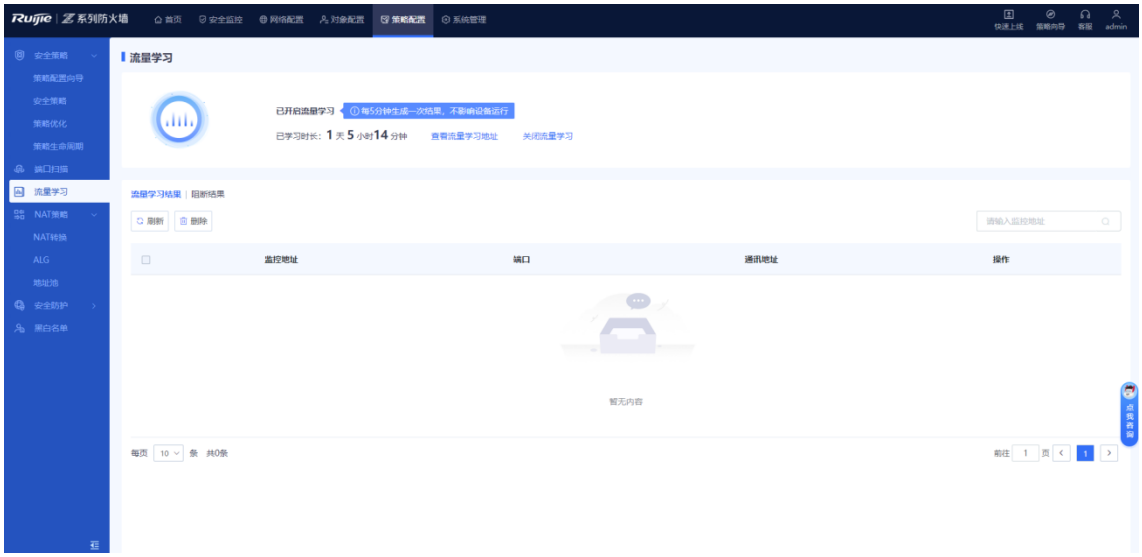
c 根据业务情况，选择是否立即开启流量学习功能。

o 业务繁忙时，点击<保存配置>，保存流量学习地址配置信息，并在稍后开启流量学习。

o 业务空闲时，点击<保存并立即开启>，保存流量学习地址配置信息并立即启动流量学习。

确认系统提示信息，并点击<立即扫描>。

(3) （可选）如果已经配置流量学习地址，直接点击<开启流量学习>。



【后续验证】

- 点击"流量学习结果"标签页可以看到学习到的IP地址以及端口信息。点击<查看详情>可以查看详细的访问关系。

- 针对某条流量学习结果，可以选择生成拒绝策略或生成允许策略。

a 在"流量学习详情"页面，点击“生成拒绝策略”或“生成允许策略”。

b 根据业务需要，将该条策略新增至模拟空间或直接新增。

c 在模拟空间生成策略后，确认没问题可转成真实空间策略。

d 点击"阻断结果"标签页可以看到学习到的被阻断的访问关系，点击<查看详情>可以查看具体的阻断次数，阻断策略，阻断业务，以及最近一次阻断发生的时间。

5.5 NAT 策略

5.5.1 简介

NAT（Network Address Translation）是一种地址转换技术，将IP数据报文头中的IP地址转换为另一个IP地址的过程，支持将报文的源地址进行转换，也支持将报文的目的地址进行转换。

在实际应用中，NAT主要应用在连接两个网络的边缘设备上，用于实现允许内部网络用户访问外部公共网络以及允许外部公共网络访问部分内部网络资源（例如内部服务器）的目的。

NAT主要分为以下三类：

NAT分类	转换内容	使用场景
源地址转换	源IP地址	适合公网IP地址数量充足的、仅有少量私网用户访问Internet场景。私网地址与公网地址一对一转换。
目的地址转换	目的IP地址	公网用户可以利用公网地址访问内部服务器的场景。
双向地址转换	源IP地址和目的IP地址同时转换	内网PC通过公网地址访问内网服务器的场景。

5.5.2 手动配置 NAT 策略

1. 配置源地址 NAT 转换

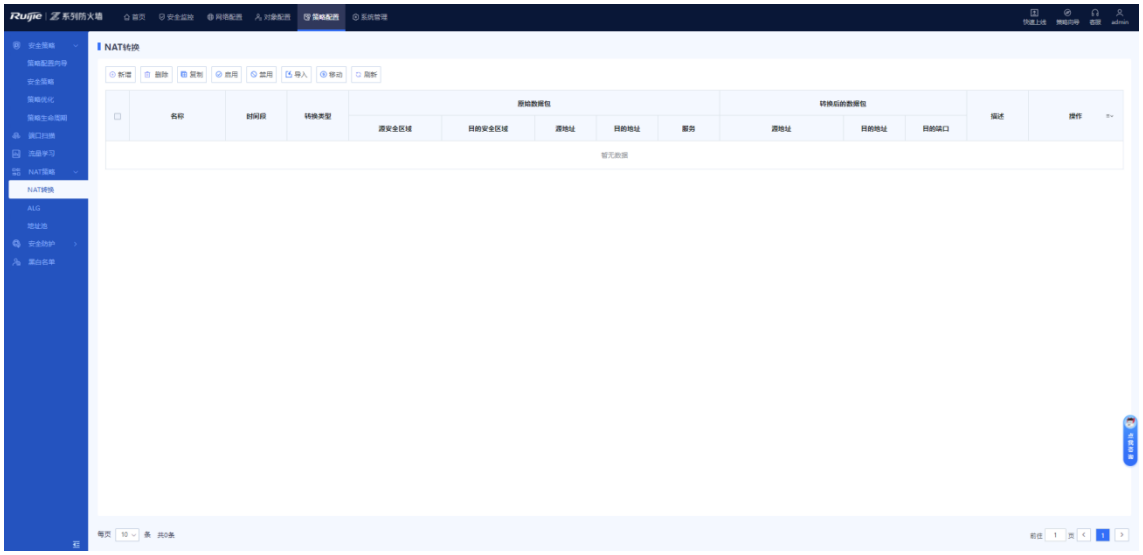
【应用场景】

源地址转换是指对报文中的源地址进行转换，通常用于内网访问外网的场景。

通过源NAT技术将私网IP地址转换成公网IP地址，使私网用户可以利用公网地址访问Internet。

【操作步骤】

(1) 点击[策略配置]>>[NAT策略]>>[NAT转换]菜单项。



(2) 在操作区上方，点击<新增>。

系统弹出[新增NAT转换]页面。

(3) 配置源地址NAT转换策略。

源地址转换策略的配置参数如下表所示。

配置项	说明	配置方法
转换类型		
转换类型	表示NAT转换的类型。	[示例] 源地址转换
基础信息		
名称	NAT策略的名称。	不能包含字符：`~!#%^&*+|{};:'"/<>?和空格。 [示例] NAT policy_1

配置项	说明	配置方法
启用状态	配置完成后是否立即启用此NAT策略。	[示例] 启用
描述	NAT策略的描述信息。	不能包含字符：`~!#%^&*+|{};:'"/<>?。 [示例] NAT policy_1
时间段	NAT策略执行的时间段。	● 下拉选择适用的时间段。 ● 默认值为any。 ● 点击<新增单次时间计划>和<新增循环时间计划>新增时间计划。 [示例] any
原始数据包		
源安全区域	策略将会转换来自此安全区域的数据包。	[示例] Any
源地址	策略将会转换此类地址发出的数据包。	[示例] Any
目的安全区域	策略将会转换发往此安全区域的数据包。	[示例] Any
目的地址	策略将会转换发往此类地址的数据包。	[示例] Any
服务	策略将会转换此类服务的数据包。	[示例] Any
转换后数据包		
源地址转换为	根据场景选择源地址转换后的地址，包括： ● 地址池 需要设置地址池。 ● 指定IP 需要设置指定IP。 ● 出接口地址	[示例] 地址池

(4) 点击<保存>。

【后续处理】

- 对于已有的策略，可以点击“编辑”修改策略的配置；点击"删除"可以删除该条策略；点击开关按钮可以启用或禁用该条策略
- 需要批量删除多条策略时，请勾选多条待删除的策略并点击上方栏目中的"删除"。

- 需要使多条策略生效时，请勾选多条待生效的策略并点击上方栏目中的"启用"。
- 需要禁用多条策略时，请勾选多条待禁用的策略并点击上方栏目中"禁用"。
- 选中一条NAT转换策略，点击上方栏目中的“复制”将进入新增NAT转换策略界面，策略配置内容将根据勾选的策略自动填写。
- 选中一条NAT转换策略，点击上方栏目中的“移动”可以调整策略位置，越靠前的策略匹配优先级越高。

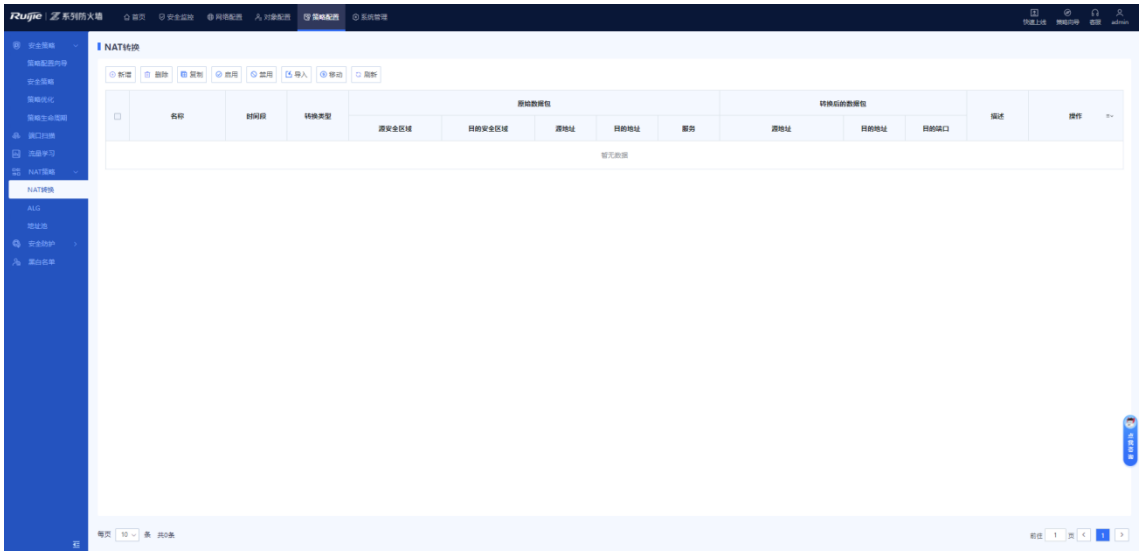
2. 配置目的地址 NAT 策略

【应用场景】

目的地址转换是指对报文中的目的地址和端口进行转换，通常应用于将内网的服务器映射给外网的场景。通过目的NAT技术将公网IP地址转换成私网IP地址，使公网用户可以利用公网地址访问内部Server。

【操作步骤】

(1) 点击[策略配置]>>[NAT策略]>>[NAT转换]菜单项。



(2) 在操作区上方，点击<新增>。

系统弹出[新增NAT转换]页面。

(3) 配置目的地址NAT转换策略。

目的地址转换的配置参数如下表所示。

配置项	说明	配置方法
转换类型		
转换类型	NAT转换的类型。	[示例] 目的地址转换
基础信息		
名称	NAT策略的名称。	不能包含字符：`~!#%^&*+|{};:'"/<>?和空格。 [示例] NAT policy_1
启用状态	配置完成后是否立即启用此NAT策略。	[示例] 启用

配置项	说明	配置方法
描述	NAT策略的描述信息。	不能包含字符：`~!#%^&*+|{};:'"/<>?。 [示例] NAT policy_1
时间段	该NAT策略生效的时间段。	● 默认值为any，也可以下拉选择已经定义好的时间计划。 ● 点击<新增单次时间计划>或<新增循环时间计划>可以创建新的时间计划。 [示例] any
原始数据包		
源安全区域	策略将会转换来自此安全区域的数据包。	[示例] Any
源地址	策略将会转换此类地址发出的数据包。	[示例] Any
目的安全区域	策略将会转换发往此安全区域的数据包。	[示例] Any
目的地址	策略将会转换发往此类地址的数据包。	[示例] Any
服务	策略将会转换此类服务的数据包。	[示例] Any
转换后数据包		
IP地址	目的地址转换后的IP地址。	[示例] 192.168.10.30
端口	目的地址转换后的端口。	[示例] 80

(4) 点击<保存>。

【后续处理】

- 对于已有的策略，可以点击“编辑”修改策略的配置；点击"删除"可以删除该条策略；点击开关按钮可以启用或禁用该条策略
- 需要批量删除多条策略时，请勾选多条待删除的策略并点击上方栏目中的"删除"。
- 需要使多条策略生效时，请勾选多条待生效的策略并点击上方栏目中的"启用"。
- 需要禁用多条策略时，请勾选多条待禁用的策略并点击上方栏目中"禁用"。
- 选中一条NAT转换策略，点击上方栏目中的“复制”将进入新增NAT转换策略界面，策略配置内容将根据勾选的策略自动填写。
- 选中一条NAT转换策略，点击上方栏目中的“移动”可以调整策略位置，越靠前的策略匹配优先级越高。

3. 配置双向地址 NAT 策略

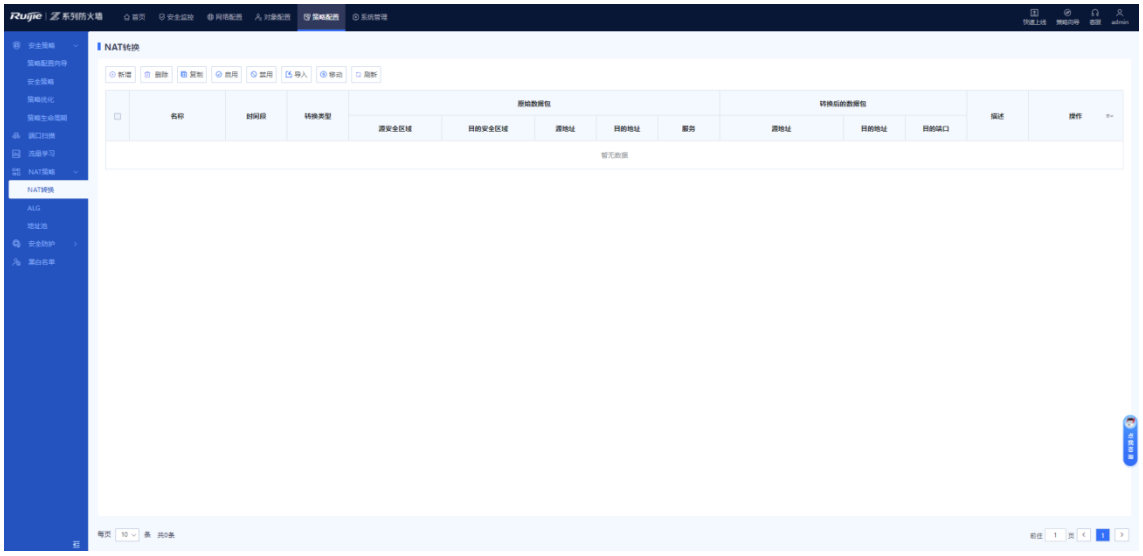
【应用场景】

双向地址转换指的是在转换过程中同时转换报文的源信息和目的信息。双向地址转换不是一个单独的功能，而是源NAT和目的NAT的组合。双向NAT是针对同一条流，在其经过防火墙时同时转换报文的源地址和目的地址。

双向地址转换主要应用于内网PC通过公网地址访问内网服务器的场景。

【操作步骤】

(1) 点击[策略配置]>>[NAT策略]>>[NAT转换]菜单项。



(2) 在操作区上方，点击<新增>。

系统弹出[新增NAT转换]页面。

(3) 配置双向地址NAT转换策略。

根据业务需要，配置不同的NAT转换策略。

双向地址转换策略的配置参数如下表所示。

配置项	说明	配置方法
转换类型		
转换类型	NAT转换的类型。	[示例] 源地址和目的地址同时转换
基础信息		

配置项	说明	配置方法
名称	NAT策略的名称。	不能包含字符：`~!#%^&*+|{};:'"/<>?和空格。 [示例] NAT policy_1
启用状态	配置完成后是否立即启用此NAT策略。	[示例] 启用
描述	NAT策略的描述信息。	不能包含字符：`~!#%^&*+|{};:'"/<>?。 [示例] NAT policy_1
时间段	该NAT策略生效的时间段。	● 默认值为any，也可以下拉选择已经定义好的时间计划。 ● 点击<新增单次时间计划>或<新增循环时间计划>可以创建新的时间计划。 [示例] any
原始数据包		
源安全区域	策略将会转换来自此安全区域的数据包。	[示例] Any
源地址	策略将会转换此类地址发出的数据包。	[示例] Any
目的安全区域	策略将会转换发往此安全区域的数据包。	[示例] Any
目的地址	策略将会转换发往此类地址的数据包。	[示例] Any
服务	策略将会转换此类服务的数据包。	[示例] Any
转换后数据包		
源地址转换为	根据场景选择源地址转换后的地址，包括： ● 地址池 需要设置地址池。 ● 指定IP 需要设置指定IP。 ● 出接口地址	[示例] 地址池
目的地址转换为	目的地址转换后的IP地址。	[示例] 192.168.10.30

配置项	说明	配置方法
目的端口转换为	目的地址转换后的端口。	[示例] 80

(4) 点击<保存>。

【后续处理】

- 对于已有的策略，可以点击“编辑”修改策略的配置；点击"删除"可以删除该条策略；点击开关按钮可以启用或禁用该条策略
- 需要批量删除多条策略时，请勾选多条待删除的策略并点击上方栏目中的"删除"。
- 需要使多条策略生效时，请勾选多条待生效的策略并点击上方栏目中的"启用"。
- 需要禁用多条策略时，请勾选多条待禁用的策略并点击上方栏目中"禁用"。
- 选中一条NAT转换策略，点击上方栏目中的“复制”将进入新增NAT转换策略界面，策略配置内容将根据勾选的策略自动填写。
- 选中一条NAT转换策略，点击上方栏目中的“移动”可以调整策略位置，越靠前的策略匹配优先级越高。

5.5.3 导入配置文件配置 NAT 转换

【应用场景】

Z-S系列防火墙设备支持导入配置文件快速生成安全策略。

【前置条件】

可通过以下两种方式获取配置文件：

- 设备提供了配置文件模板，下载配置文件并根据业务情况进行修改。
- 如果要将原有设备的配置导入到Z-S系列防火墙设备中，可以通过配置策略迁移工具获取对应的配置文件。

说明

配置策略迁移工具的具体使用请联系技术支持工程师。

【操作步骤】

(1) 点击[策略配置]>>[NAT策略]>>[NAT转换]菜单项。

(2) 在操作区，点击<导入>。

系统弹出“提示”信息。

(3) 点击<下载示例CSV文件>，下载配置文件模板并填写对应的配置信息。

说明

配置文件修改后，请检查配置文件的命名规格，以满足系统的要求。配置文件的名称格式为：z5100-config-conversion-{yyyyMMddHHmmssSSS}.csv。

(4) 将配置文件拖至上传区域或点击<点击选择>将配置文件上传至设备中。

(5) 设置存在数据冲突时的处理方式。

当导入的数据和已有数据存在冲突时，可以采用以下处理方式：

- 显示冲突数据：系统会显示存在冲突的配置项及冲突原因，可根据提示信息修改配置文件。
- 跳过：系统忽略存在冲突的配置项，无需进行任何处理。

(6) 点击<确认导入>。

系统自动将配置文件中的信息写入设备，使配置生效。

5.5.4 配置 ALG 功能

【应用场景】

ALG（Application Level Gateway，应用层网关）功能用于NAT场景下自动检测某些报文的应用层信息，根据应用层信息放开相应的访问规则（生成Server-map表），并自动转换报文载荷中的IP地址和端口信息。

普通NAT只能转换报文头中的IP地址和端口，无法对应用层的数据进行转换。在许多应用层协议中，报文载荷中也带有地址或端口信息，如果这些数据不进行转换，可能导致后续通信异常。

通过配置ALG功能，既可以根据应用层信息放开相应的访问规则，同时对应用层的数据进行NAT转换。

【操作步骤】

(1) 点击[策略配置]>>[NAT策略]>>[ALG]菜单项。

(2) 勾选需要开启ALG功能的协议名称并点击<保存配置>。

NAT功能可以正常转换此类协议的流量。

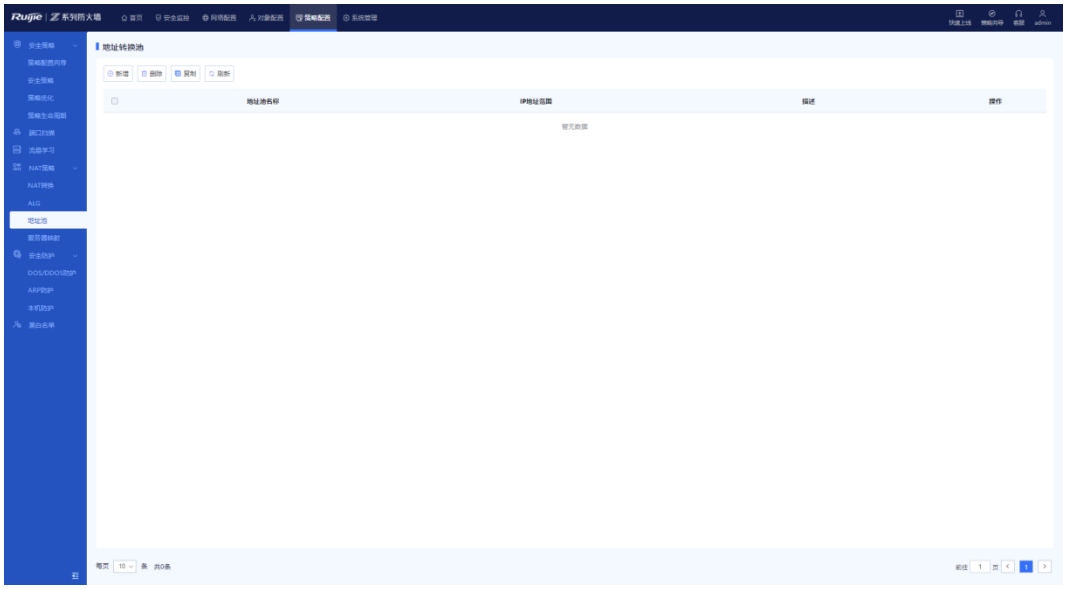
5.5.5 配置地址池

【应用场景】

配置地址池后，地址池中的地址可以作为NAT转换策略中"转换后的数据包"配置项的选择参数。

【操作步骤】

(1) 点击[策略配置]>>[NAT策略]>>[地址池]菜单项。



(2) 在操作区，点击<新增>。

系统进入[新增地址转换池]页面。

(3) 填写地址池名称，为其配置IP地址/范围。

(4) 点击<保存>，完成地址池新增。

【后续处理】

- 配置地址池转换后，会将配置信息同步给ARP代理。针对该地址池中的IP所在接口都会使用ARP代理。
- 需要复制已有的地址池信息时，点击“复制”将进入新增地址池页面，但地址池配置参数将根据勾选的地址池自动填写。
- 需要批量删除多条策略时，勾选多条待删除的策略并点击<删除>。

5.6 安全防护管理

客户环境中可能存在多种形式的攻击，例如基于流量的 DDoS 攻击、基于报文或协议的攻击(teardrop、smurf、redirect)等等。攻击目标可能是内网某个用户或者设备本身。因此客户可以配置策略来帮助内网用户及设备防御攻击。本机防护提供默认策略保证设备的正常运行。此外针对内网的 ARP 攻击，安全防护提供了静态 ARP 配置、ARP 代理以及 ARP 欺骗防御功能。

- 协议类攻击（异常报文攻击）

协议类攻击主要利用目标设备上协议栈实现的漏洞，通过发送特定的流量或特定报文（畸形报文），使目标设备发生异常以达到拒绝服务的目的。常见的协议类攻击包括Land、Smurf、Fraggle、TearDrop、Winnuke、ICMP重定向攻击、ICMP不可达攻击、超大ICMP报文攻击等。

- Land

  攻击原理/特征：用于Land攻击的数据包中的源地址和目标地址是相同的，用户设备在接收到这类数据包时，可能出现不知道该如何处理堆栈中通信源地址和目的地址相同的这种情况或者循环发送和接收该数据包，消耗大量的系统资源，从而有可能造成系统崩溃或死机等现象。

- Smurf

  攻击原理/特征：该攻击向一个子网的广播地址发一个带有特定请求(如ICMP回应请求)的包，并且将源地址伪装成想要攻击的主机地址。子网上所有主机都回应广播包请求而向被攻击主机发包，使该主机受到攻击。攻击者只需要较小的代价，就可以给被攻击主机产生大量的攻击流量。

- Fraggle

  攻击原理/特征：Fraggle攻击对Smurf攻击作了简单的修改，使用的是UDP应答消息而非ICMP报文（攻击端口7（echo）或19（chargen））。

- TearDrop

攻击原理/特征：该攻击主要是利用系统在重组IP数据包过程中的漏洞而进行的。Teardrop是基于UDP的病态分片数据包的攻击方法，其工作原理是向被攻击者发送多个分片重叠的IP包（IP分片数据包中包括该分片数据包属于哪个数据包以及在数据包中的位置等信息，攻击者刻意使这些分片产生重叠），某些操作系统收到含有重叠偏移的伪造分片数据包时将会出现系统崩溃、重启等现象。

- Winnuke

攻击原理/特征：WinNuke攻击又称带外传输攻击，它的特征是攻击目标端口，被攻击的目标端口通常是53、113、137、138和139，而且URG位设为“1”，即紧急模式。

- 泛洪类攻击（基于流量的攻击）

泛洪类攻击主要通过消耗被攻击主机的连接、带宽、CPU等有限的资源，来达到使目的主机拒绝服务的效果。常见的资源消耗类攻击包括各类流量型Flood攻击，包括syn-flood、udp-flood、icmp-flood。

- 扫描类攻击

扫描类攻击通常是攻击者尝试对目标主机/网络进行攻击的第一个步骤，通过端口/IP扫描的方式，来发现目标主机/网络中的可利用端口/服务/OS类型等，为进一步的渗透或攻击提供基础信息。从流量上分析，会发现某个特定主机在短时间内大量地去连接某个IP的连续端口（试图发现开放的服务）或某个网段连续的IP（试图发现存活的主机）。

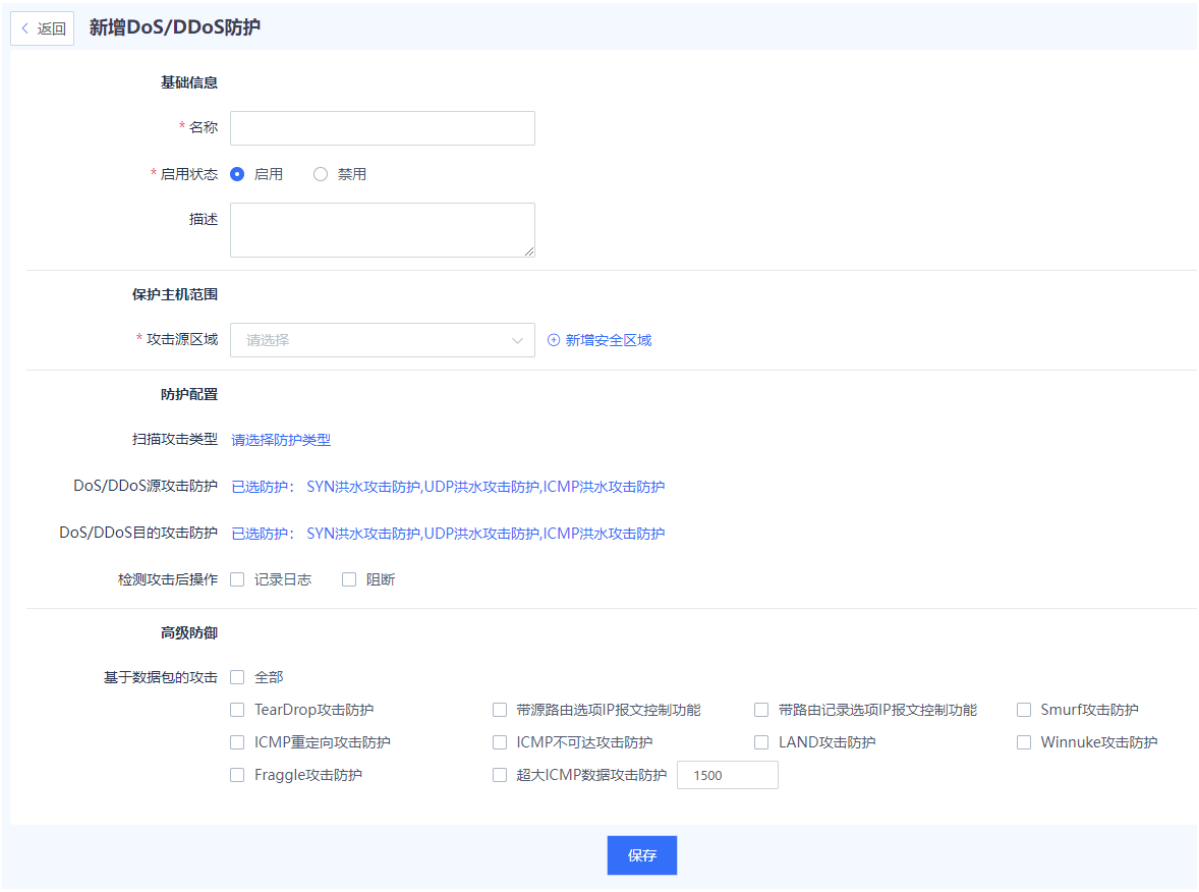
5.6.1 配置 DoS/DDoS 防护

【操作步骤】

(1) 点击[策略配置]>>[安全防护]>>[DoS/DDoS防护]菜单项。

(2) 在操作区上方，点击<新增>。

系统进入[新增DoS/DDoS防护]页面。



(3) 设置DoS/DDoS防护策略相关配置。

配置项	说明	配置方法
基础信息		
名称	DoS/DDoS防护策略的名称。	不能包含字符：`~!#%^&*+|{};:'"/<>?和空格。 [示例] DoS policy_1
启用状态	配置完成后是否立即启用此防护策略。	[示例] 启用
描述	DoS/DDoS防护策略的描述信息。	不能包含字符：`~!#%^&*+|{};:'"/<>?。 [示例] 新增策略
保护主机范围 为策略关联攻击源区域，命中时策略生效。		
攻击源区域	策略将关注来自该安全区域的流量。	[示例] any

配置项	说明	配置方法
防护配置		
扫描攻击类型		
IP地址扫描防护	是否开启IP地址扫描防护。	[示例] 开启
阈值	进行IP地址扫描攻击的阈值。	[示例] 10000
封锁时间	检测到攻击后，对流量进行封锁的时间。	[示例] 300秒
端口扫描防护	是否开启IP地址扫描防护。	[示例] 开启
阈值	进行端口扫描攻击的阈值。	[示例] 10000
封锁时间	检测到攻击后，对流量进行封锁的时间。	[示例] 300秒
DoS/DDoS攻击防御：支持基于源和基于目的两种类型。		
攻击防护类型	支持SYN Flood攻击防护、UDP Flood攻击防护和ICMP Flood攻击防护。	选择对应标签页，开启对应的攻击防护。 [示例] SYN洪水攻击防护：开启
源IP封锁阈值/目的IP封锁阈值	泛洪攻击防范的全局触发阈值。	[示例] 1000
封锁时间	检测到攻击后，对流量进行封锁的时间。	[示例] 300秒
检测攻击后操作	系统检测到攻击后的操作，包括： ● 记录日志：仅记录安全日志，不阻断流量。 ● 阻断：仅阻断流量不记录安全日志。	[示例] 记录日志+阻断
高级防御		
基于数据包的防御	是否基于数据包进行防御。	[示例] 全部

(4) 点击<保存>，完成DoS/DDoS防护策略配置。

【后续处理】

- 对于已有的策略，可以点击“编辑”修改策略的配置；点击“删除”可以删除该条策略；点击开关按钮可以启用或禁用该条策略
- 需要批量删除多条策略时，勾选多条待删除的策略并点击“删除”。
- 需要批量使多条策略生效时，勾选多条待生效的策略并点击“启用”。
- 需要禁用多条策略时，勾选多条待禁用的策略并点击“禁用”。
- 在搜索栏中输入策略名、策略关联对象、策略描述中的完整或部分内容可进行模糊搜索。

5.6.2 配置 ARP 防护

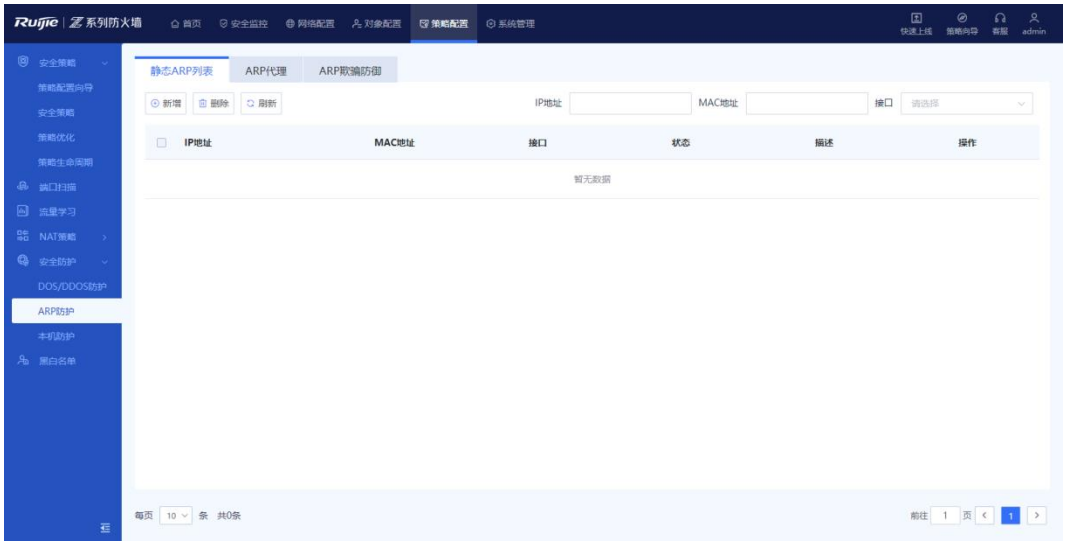
1. 配置静态 ARP

【应用场景】

配置静态ARP表项，防止因为收到伪造的免费ARP、ARP响应报文而被修改。

【操作步骤】

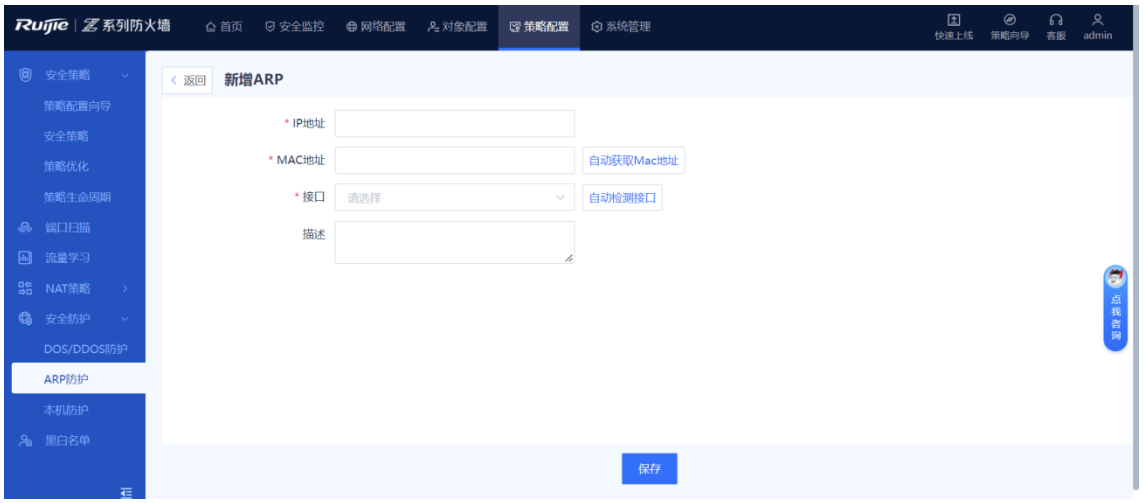
(1) 点击[策略配置]>>[安全防护]>>[ARP防护]>>[静态ARP列表]菜单项。



页面将显示设备已经配置的静态ARP表项，"状态"栏目将根据表项绑定的接口状态显示为"生效"或"失效"。

(2) 在操作区上方，点击<新增>。

系统进入[新增ARP]页面。



(3) 设置ARP列表的基本信息。

配置项	说明	配置方法
基础信息		
IP地址	要绑定静态ARP的IP地址。	[示例] 192.168.10.3
MAC地址	要绑定的MAC地址。	支持以下两种配置方式： ● 手动填写 ● 点击<自动获取Mac地址>，设备将根据已知ARP表项寻找IP对应的MAC地址。若查找失败，则返回提示"没有找到匹配的地址"。 [示例] 30:0d:9e:41:d9:0b
接口	要绑定的物理接口。	支持以下两种配置方式： ● 手动填写 ● 点击<自动检测接口>，设备将根据相关的信息设定IP可能对应的接口。若查找失败，则返回提示"没有找到匹配的接口"。 [示例] Ge0/8

(4) 点击<保存>，完成静态ARP策略配置。

【后续处理】

- 对于已有的策略，可以点击“编辑”修改策略的配置。
- 需要批量删除多条策略时，勾选多条待删除的策略并点击<删除>。
- 在搜索栏中输入相关参数可以筛选查询。

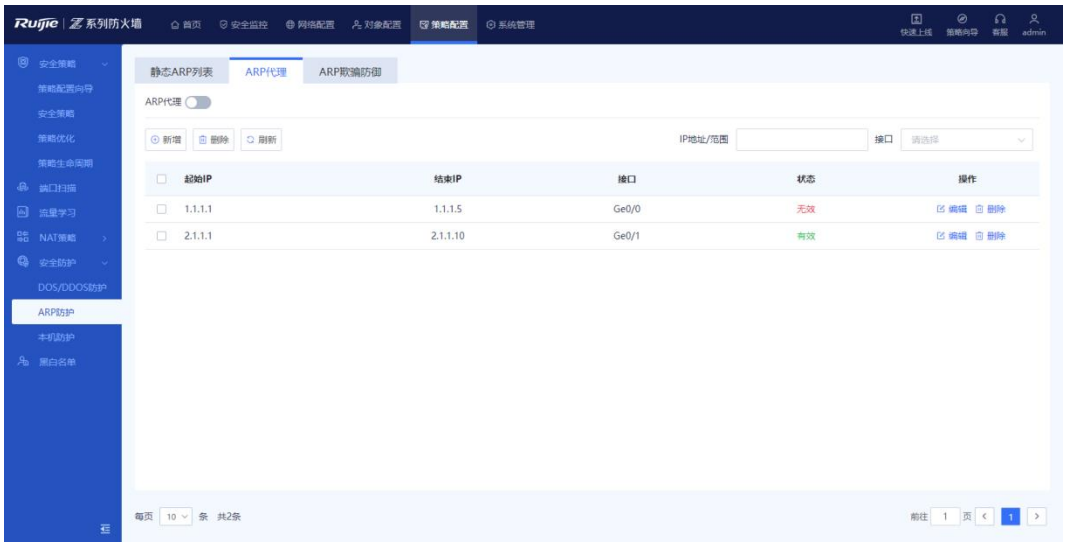
2. 配置 ARP 代理

【应用场景】

当设备收到接口代理地址段的ARP请求时，设备将会响应并提供接口的MAC地址。

【操作步骤】

(1) 点击[策略配置]>>[安全防护]>>[ARP防护]>>[ARP代理]菜单项。



页面将显示设备已经配置的ARP代理地址段，"状态"栏目将根据表项绑定的接口状态显示为“生效”或“失效”。

(2) 将"ARP代理"开关设置为开启状态，开启ARP代理。

(3) 点击<新增>。

系统进入[创建ARP代理]页面。

(4) 填写需要代理的起始IP、结束IP，并选择要代理的接口。

(5) 点击<保存>，完成ARP代理配置。

【后续处理】

对于已有的ARP代理配置，点击<编辑>可修改原有的配置参数。

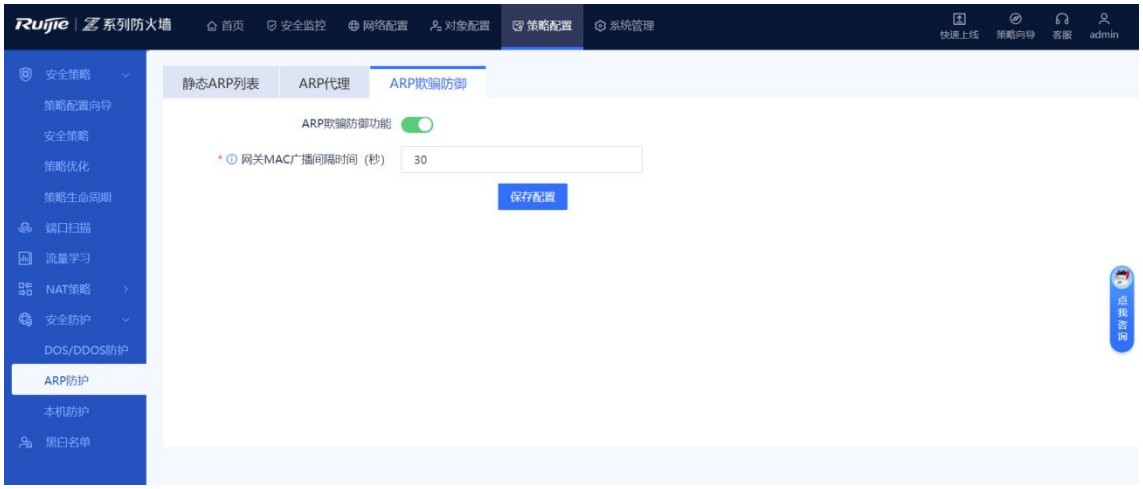
3. 配置 ARP 欺骗防御

【应用场景】

设备发送免费ARP广播报文，帮助同一网段的终端获取正确的设备MAC地址。

【操作步骤】

(1) 点击[策略配置]>>[安全防护]>>[ARP防护] >> [ARP欺骗防御]。



(2) 将“ARP欺骗防御功能”开关设置为开启状态。

(3) 修改“网关MAC广播间隔时间”。

间隔时间范围为1~1800，默认为30，单位为秒。

(4) 点击<保存配置>。

5.6.3 配置本机防护

【应用场景】

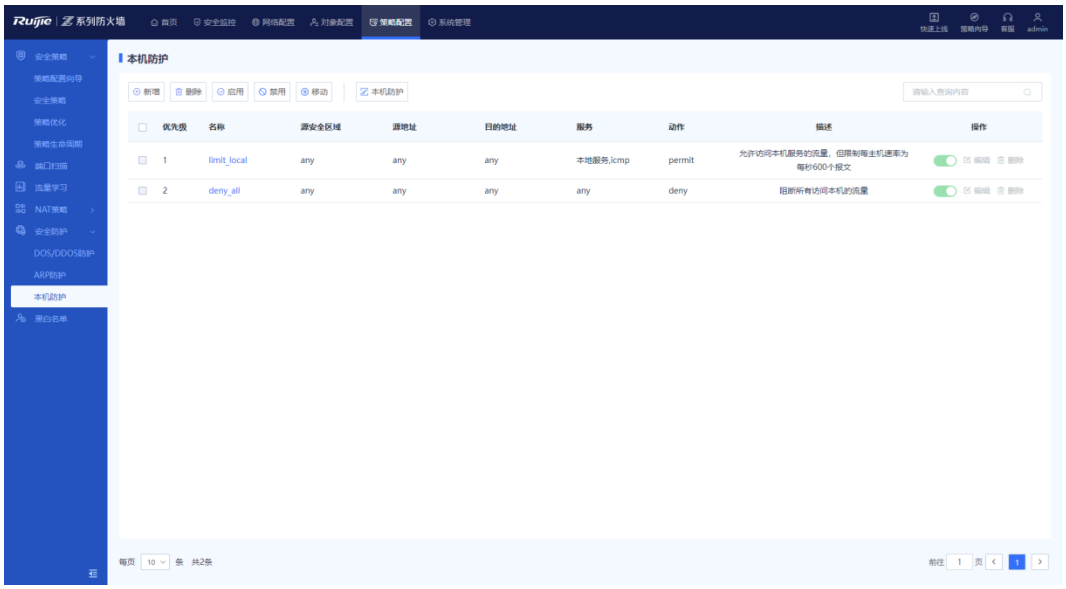
通过本机防护功能可以使用默认策略保证设备的正常运行。

主要应用于以下场景：

- **禁止Web登录：**通过识别送本机报文流量中的https报文，将这些报文直接丢弃，以达到禁止访问设备的web的功能。勾选本功能时，必须要填写管理IP，只有管理IP中的地址可以通过web方式登录管理设备。
- **禁止ping：**通过出识别送本机报文的流量中的ping报文，将这些报文直接丢弃，以达到禁止ping设备的功能。勾选本功能时，必须要填写管理IP，只有管理IP中的地址可以ping通设备。
- **禁止ssh/telnet：**通过出识别送本机报文流量中的ssh/telnet报文，将这些报文直接丢弃，以达到禁止ssh/telnet设备的功能。勾选本功能时，必须要填写管理IP，只有管理IP中的地址可以使用ssh/telnet方式登录设备。
- **添加管理IP：**管理IP不受到防本地ICMP攻击、禁止Web登录、禁止ping、禁止ssh/telnet、禁止SNMP管理、防流量型攻击这些功能的限制，可以正常的通过这些功能而不被丢包。

【操作步骤】

(1) 点击[策略配置]>>[安全防护]>>[本机防护]菜单项。



说明

本机防护设有两条不可修订的默认策略，保证设备出厂后能够防御针对设备的流量攻击。

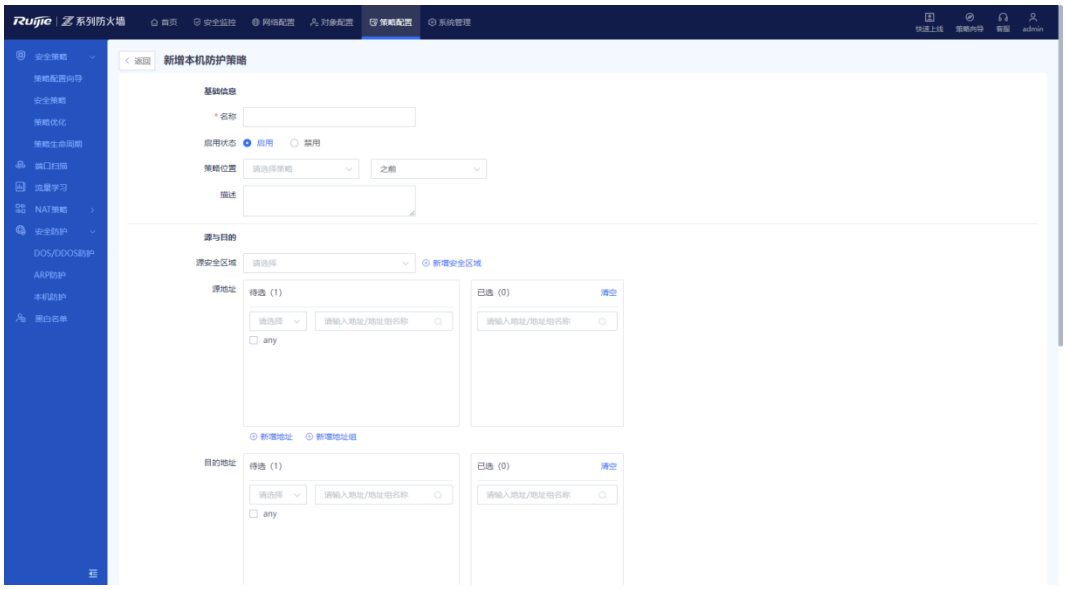
(2) 启用本机防护功能。

a 在操作区上方，点击 本机防护 。

b 将"启用本机防护"设置为开启状态，并点击<确认>。

(3) 新增本机防护策略。

a 点击<新增>，进入[新增本机防护策略]页面。



b 设置本机防护策略相关配置项。

配置项	说明	配置方法
基础信息		
名称	要绑定静态ARP的IP地址。	可以输入任意字符。 [示例] 策略_1
启用状态	要绑定的MAC地址。	支持以下两种配置方式： ● 手动填写 ● 点击<自动获取Mac地址>，设备将根据已知ARP表项寻找IP对应的MAC地址。若查找失败，则返回提示"没有找到匹配的地址"。 [示例] 启用
策略位置	将新增的策略移动到指定策略之前或之后。策略越靠前匹配优先级越高。	-
描述	安全策略的描述信息。	描述不能包含字符：`~!#%^&*+|{};:'"/<>?
源与目的 为策略关联源安全区域、源地址对象、目的地址对象，服务对象，四者同时命中时策略生效。		
源安全区域	策略将关注来自该区域的流量。	any表示所有区域的流量。 [示例] 启用

配置项	说明	配置方法
源地址	策略将关注来自此该址集合的流量。	any表示所有地址。
目的地址	策略将关注发往该地址集合的流量。	any表示所有地址。
服务	策略将关注该类服务的流量。	any表示所有服务。
动作设置		
动作选项	命中策略的流量动作。	[示例] 允许
每IP限速		
每IP限速	是否限制命中策略的流量每秒可以通过的报文数。 ● 不启用：不限制报文数。 ● 启用：限制报文数，且需要设置"每个主机每秒允许通过报文数"。	[示例] 不启用

(4) 在"操作"栏将开关设置为开启状态，启用新增的策略。

(5) 策略自动填写。

【后续处理】

- 需要批量删除多条策略时，请勾选多条待删除的策略并点击上方栏目中的“删除”。
- 需要使多条策略生效时，请勾选多条待生效的策略并点击上方栏目中的“启用”。
- 需要禁用多条策略时，请勾选多条待禁用的策略并点击上方栏目中的“禁用”。
- 点击“移动”，可以调整策略的优先级，处于上方的策略优先进行匹配。
- 在搜索栏中输入策略名、策略关联对象、策略描述中的完整或部分内容进行模糊搜索。
- 选中一条策略，点击上方栏目中的“移动”可以调整策略位置，越靠前的策略匹配优先级越高。

5.7 黑白名单管理

5.7.1 简介

Z-S系列防火墙支持黑白名单功能，基于IP地址对报文进行阻断或放通。

- 白名单

  将指定的IP地址加入白名单后，防火墙设备对于该地址发送的报文或发送到该地址的报文会跳过安全检查，而直接按照正常的转发流程进行处理，从而实现了报文的高速转发。

  例如：当客户希望网络中部分IP地址（如管理员）不受安全策略、抗DoS/DDoS策略的限制时，可以为对应的IP地址配置白名单。

- 黑名单

将指定IP加入黑名单后，对于该地址发送的报文或发送到该地址的报文会被设备丢弃。

例如：当用户希望网络中部分IP地址（如攻击源）的流量无法通过设备时，可以将其加入黑名单。

> ⚠ 注意
> 添加至黑名单中的IP无法登录防火墙设备。

- 临时黑名单

  临时黑名单的作用于黑名单相同，但临时黑名单只会生效一段时间，超过生效时间将会失效并被自动删除。当流量命中暴力破解类型的IPS策略时，会自动生成临时黑名单，阻断时长为暴力破解类安全规则的阻断时长。用户也可以手动配置临时黑名单。

5.7.2 创建白名单

【应用场景】

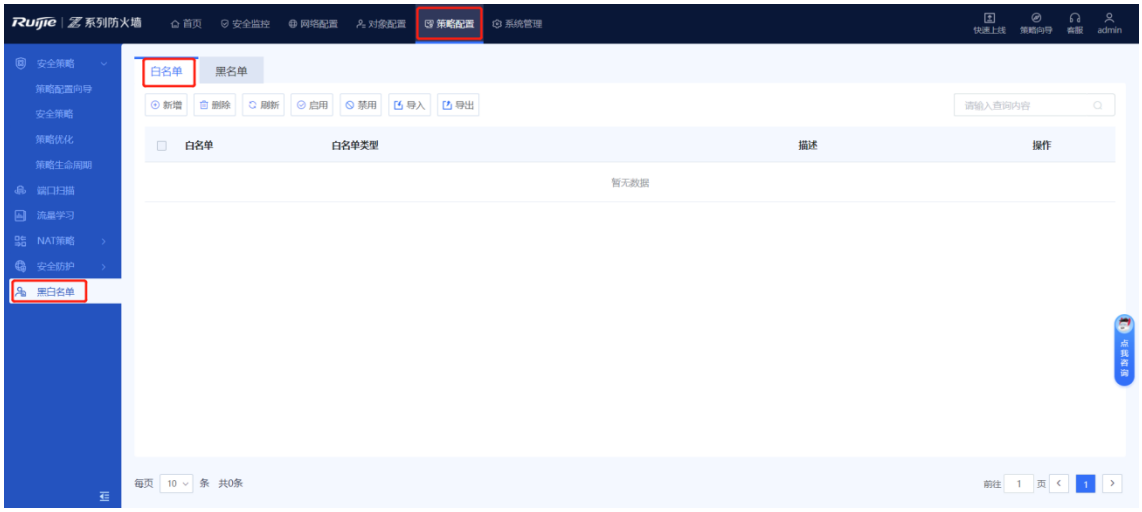
通过Web界面配置白名单。

【操作步骤】

(1) 系统进入[新增白名单]页面。

a 点击[策略配置]>>[黑白名单]>>[白名单]菜单项。

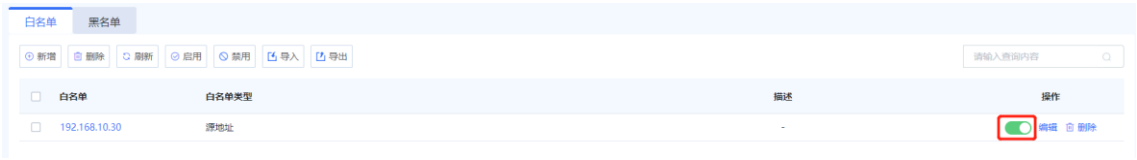
b 在操作区上方，点击<新增>。



(2) 设置白名单策略的相关配置，并点击<保存>。

配置项	说明	配置方法
白名单类型	白名单类型： ● 源地址：报文由此类地址发出。 ● 目的地址：报文发往此类地址。	[示例] 源地址
IP地址/范围	白名单IP地址/范围。	支持配置为以下两种格式： ● 单个IP：192.168.1.1 ● IP地址范围：192.168.1.1-192.168.1.10

(3) 将“操作”栏中的开关设置为开启状态，启用该条白名单设置。



【后续处理】

- 需要批量删除多条白名单策略时，请勾选多条待删除的策略并点击"删除"。
- 需要使多条白名单策略策略生效时，请勾选多条待生效的策略并点击"启用"。
- 需要禁用多条白名单策略时，请勾选多条待禁用的策略并点击"禁用"。
- 点击"导出"，可以导出当前所有的白名单配置。
- 点击"导入"，可以下载导入格式模板，或选择要上传的CSV文件，点击“开始”启动导入任务。
- 在搜索栏中输入白名单IP地址、白名单描述中的完整或部分内容可进行模糊搜索。

5.7.3 创建黑名单

【应用场景】

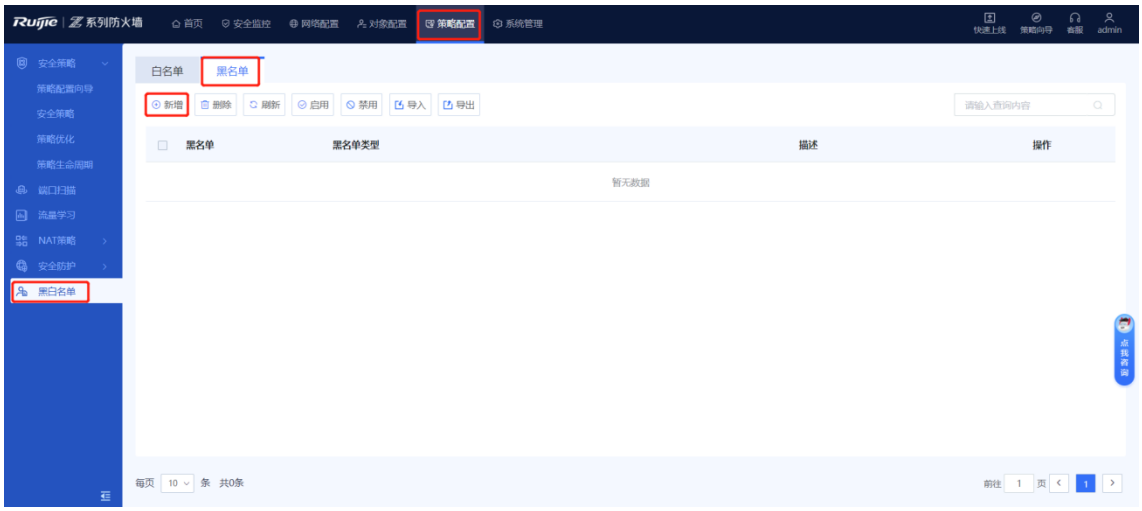
通过Web界面配置黑名单。

【操作步骤】

(1) 进入[新增黑名单]页面。

a 点击[策略配置] >> [黑白名单] >> [黑名单]菜单项。

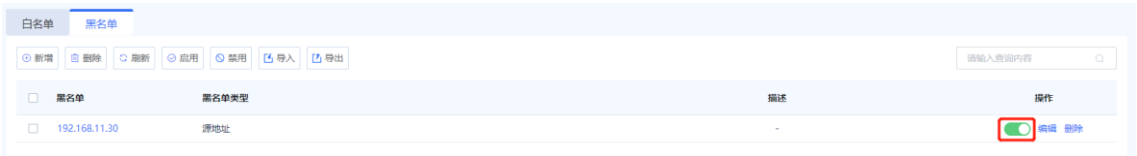
b 在操作区上方，点击<新增>。



(2) 设置黑名单策略相关配置，并点击<保存>。

配置项	说明	配置方法
黑名单类型	黑名单类型： ● 源地址：报文由此类地址发出。 ● 目的地址：报文发往此类地址。	[示例] 源地址
IP地址/范围	黑名单IP地址/范围。	支持配置为以下两种格式： ● 单个IP：192.168.1.1 ● IP地址范围：192.168.1.1-192.168.1.10

(3) 将“操作”栏中的开关设置为开启状态，启用该条黑名单设置。



【后续处理】

- 需要批量删除多条黑名单策略时，请勾选多条待删除的策略并点击"删除"。
- 需要使多条黑名单策略策略生效时，请勾选多条待生效的策略并点击"启用"。
- 需要禁用多条黑名单策略时，请勾选多条待禁用的策略并点击"禁用"。

- 点击"导出"，可以导出当前所有的黑名单配置。
- 点击"导入"，可以下载导入格式模板，或选择要上传的CSV文件，点击“开始”启动导入任务。
- 在搜索栏中输入黑名单IP地址、白名单描述中的完整或部分内容可进行模糊搜索。

5.7.4 创建临时黑名单

【应用场景】

通过Web界面手动配置临时黑名单。

【操作步骤】

(1) 进入[新增临时黑名单]页面。

a 点击[策略配置] >> [黑白名单] >> [临时黑名单]菜单项。

b 在操作区上方，点击<新增>。

(2) 设置黑名单策略相关配置，并点击<保存>。

配置项	说明	配置方法
黑名单类型	临时黑名单类型： ● 源地址：报文由此类地址发出。 ● 目的地址：报文发往此类地址。	[示例] 源地址
IP地址/范围	临时黑名单IP地址/范围。	支持配置为以下两种格式： ● 单个IP：192.168.1.1 ● IP地址范围：192.168.1.1-192.168.1.10
阻断时长	临时黑名单生效时间，超过生效时间将会失效并被自动删除。	[示例] 5分钟
描述	临时黑名单的描述信息。	不能包含字符：`~!#%^&*+|{};:'"/<>?

(3) 配置完成后，点击<保存>。

【后续处理】

- 需要批量删除多条临时黑名单策略时，请勾选多条待删除的策略并点击"删除"。
- 需要重新设置多条临时黑名单策略的生效时长时，请勾选多条策略并点击"阻断时长设置"。

6 对象配置管理

6.1 地址对象

6.1.1 简介

地址对象是IP地址或MAC地址的集合，地址组是地址对象的集合。

【地址组】

地址对象包含一个或若干个IP地址，它类似于一个基础组件，只需定义一次，就可以被各种策略（例如安全策略、NAT策略）多次引用。

例如，某个办公网络的网段地址是192.168.1.0/24，当要对该网络的IP报文进行地址转换时，可以创建一个名为“办公区”的地址，将192.168.1.0/24网段加入到“办公区”地址中。在配置办公网络的NAT策略时，可以直接引用“办公区”这个地址对象。

防火墙设备支持将如下类型的地址加入到地址对象中：

- IP地址
- IP地址范围

【地址组对象】

地址组的成员是已经定义好的地址对象，使用地址组对象提高了地址管理的灵活度。

例如，一个企业包括财务部、研发部、市场部，三个部门能够访问的网络资源是不同的，但是接入Internet都要经过地址转换，通常配置规则如下：

- 为三个部门分别配置地址对象“财务部”、“研发部”和“市场部”，配置每个部门的访问控制策略分别引用各自的地址。
- 创建地址组“企业1”，将地址对象“财务部”、“研发部”和“市场部均加入到地址组“企业1”中，地址转换策略引用地址组“企业1”即可。

6.1.2 创建地址对象

【应用场景】

通过Web管理界面，创建地址对象。

【操作步骤】

(1) 进入“新增IP地址对象”页面。

a 点击[对象配置]>>[地址]>>[地址]菜单项。

b 点击<新增>。

(2) 设置地址对象相关配置项。

配置项	说明	配置方法
名称	IP地址对象的名称。	[示例] Addr1
描述	IP地址对象的描述信息。	[示例] 用于办公区1
IP地址/范围	IP地址或范围。	支持如下三种配置方式： ● IP地址：一个或多个IP地址。每行输入一个IP地址，如果输入多个IP地址时，使用回车键空行。例如：192.168.20.3 ● IP范围：同一个地址段中的范围，用-进行连接。例如：192.168.20.1~192.168.20.3。 ● 网段：IP网段。例如：192.168.1.0/24 或 192.168.1.0/255.255.255.0。

(3) 点击<保存>。

【后续处理】

- 点击<编辑>，修改地址对象的描述信息和IP范围。
- 点击<删除>，可以删除未被引用的地址对象。

6.1.3 创建地址组对象

【应用场景】

通过Web管理界面，创建地址对象。

【操作步骤】

(1) 进入“新增地址组”页面。

a 点击[对象配置]>>[地址]>>[地址组]菜单项。

b 点击<新增>。

(2) 设置地址组对象相关配置项。

配置项	说明	配置方法
名称	地址组对象的名称。	[示例] Addr_total
描述	地址组对象的描述信息。	[示例] 整个企业的地址信息
包含IP	地址组对象中包含的地址对象。	在“待选”区域选择需要加入到该地址组对象的地址对象，自动添加到“已选”区域。 [示例] 地址对象1

(3) 点击<保存>。

【后续处理】

- 点击<编辑>，修改地址组对象的描述信息和成员IP。
- 点击<删除>，可以删除未被引用的地址组对象。

6.2 应用

6.2.1 简介

为了有效区分对使用相同协议和端口号的不同应用程序，Z-S系列防火墙引入应用的概念。通过利用应用程序的特征，能够精确地识别各种常见的应用程序。例如，网页游戏和网页视频都是使用HTTP协议8080端口进行数据传输，通过每种应用程序的特征有效区分这两种应用程序。

锐捷网络通过分析各种常见应用形成了应用识别特征库，应用识别特征库对各种常见的应用特征进行了预定义，系统可以根据应用的特征识别出各种应用。防火墙加载应用识别特征库后能够识别特征库里已经定义过的应用，这些应用在防火墙设备上以预定义应用的形式呈现。

说明

预定义应用不可以被修改或删除，您可以通过定期更新应用识别特征库来获取最新的预定义应用。

6.2.2 创建自定义应用组

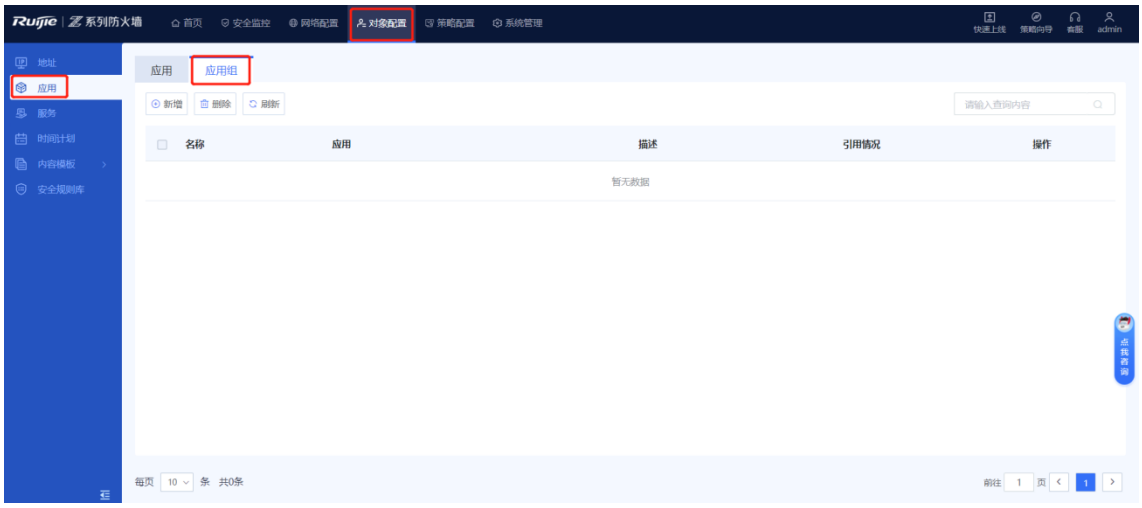
【应用场景】

为简化管理，可以将相同管控需求的应用组合在一起，多个应用的集合被称为一个应用组。

【操作步骤】

(1) 进入[新建应用组]页面。

a 点击[对象配置]>>[应用]>>[应用组]菜单项。



b 点击<新增>。

(2) 设置应用组相关配置。

配置项	说明	配置方法
名称	自定义应用组名称。	● 支持输入任意字符。 ● 不允许与已有应用同名。 ● 一经创建，无法修改应用组名称。 [示例] Zone1
描述	自定义应用组的相关描述信息。	支持输入任意字符。 [示例] New app group
包含应用	自定义应用组中包含的应用。	在"待选"区域选择对应的应用，该应用将自动添加到"已选"区域。

(3) 点击<保存>。

【后续处理】

- 应用组创建成功后，可以查看应用组的详细信息：

配置项	说明
应用	应用组所包含的应用。
引用情况	与策略相关的信息。

- 在搜索框中输入查询字段，可以对自定义应用组进行模糊查询。
- 点击<查看>，可以显示该应用组关联的安全策略。
- 当应用组不再使用时，可以将其删除。当应用组关联策略时，无法直接删除应用组，需要先解除应用组与策略的关联后，才可以操作。

6.2.3 查看特征库应用信息

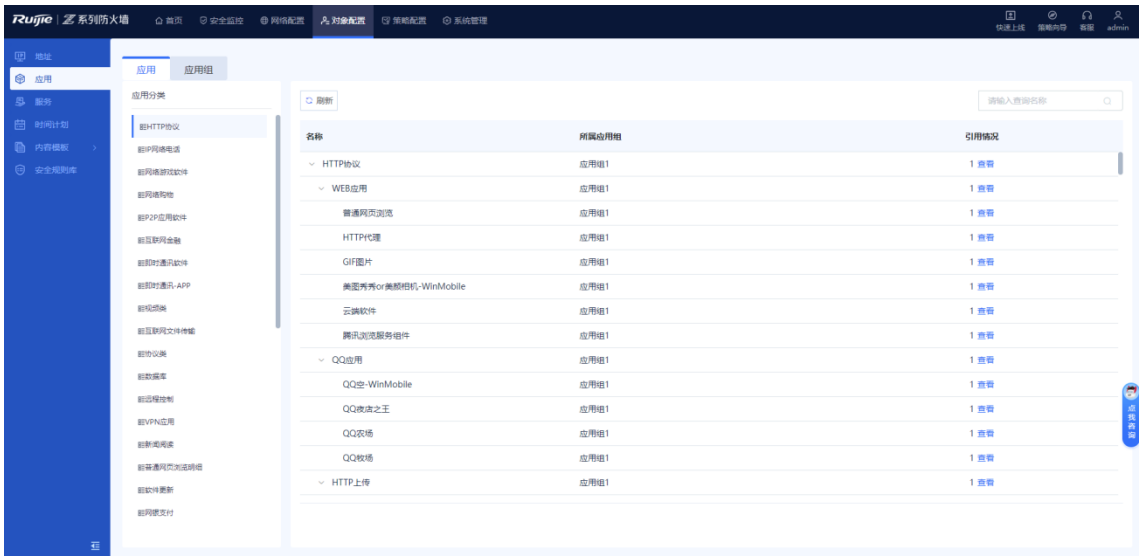
【应用场景】

通过该操作，可以查看系统自定义的应用信息。

【操作步骤】

(1) 点击[对象配置]>>[应用]>>[应用]菜单项。

(2) 查看应用详细信息。



应用详细信息包括：

配置项	说明
所属应用组	包含该应用所属的应用组信息。
引用情况	应用组包含应用、策略关联应用的信息。

说明

左侧显示匹配成功的应用分类，右侧对应是某分类下的应用信息。

【后续处理】

- 在搜索框中输入查询字段，可对应用进行模糊搜索。
- 点击<查看>，可以查看应用的引用信息。上级应用的应用组、策略关联信息将被所属下层应用继承。

6.2.4 升级应用识别特征库

及时升级应用识别特征库可以提升防火墙设备对应用的识别能力。有关特征库升级的详细介绍请参见8.5 特征库升级。

6.3 服务

6.3.1 简介

服务是一个或若干个应用协议的集合。服务通过指定协议类型、源端口、目的端口等信息来标识某个应用协议。

为方便管理，也可以将多个服务集合成一个服务组。

防火墙设备可以根据服务和服务组识别常用的应用协议。当数据流量的协议类型和端口号符合服务的条件后，就会被认为是指定应用协议的流量。对符合服务条件的数据流可以基于服务或服务组应用安全策略或流量控制策略。

Z-S系列防火墙支持两种服务类型：

- 预定义服务

预定义服务是指系统缺省已经存在、可以直接选择的服务类型。预定义服务通常都是常用协议，例如，HTTP、FTP、Telnet等。预定义服务通常通过端口来定义这些协议。所以当实际网络中协议所使用端口与设备预定义的端口不同时，需要为其创建自定义服务。例如，预定义服务http对应端口号为80，但是因为某些原因80端口被占用时，需要自定义一个其他端口号的http服务，并在安全策略中引用，以实现对这类应用协议的数据报文控制。

说明

预定义服务不能被删除。

- 自定义服务

  通过指定协议类型（例如TCP、UDP或ICMP）和端口号等信息来定义的一些应用协议类型。

  - 对于TCP和UDP的报文，通过指定一系列端口或端口范围来区分应用协议类型。
  - 对于ICMP报文，通过ICMP类型名称和编码两个字段来区分ICMP报文类型。
  - 对于IP协议号，通过协议号来区分IP报文类型。

6.3.2 自定义服务

【应用场景】

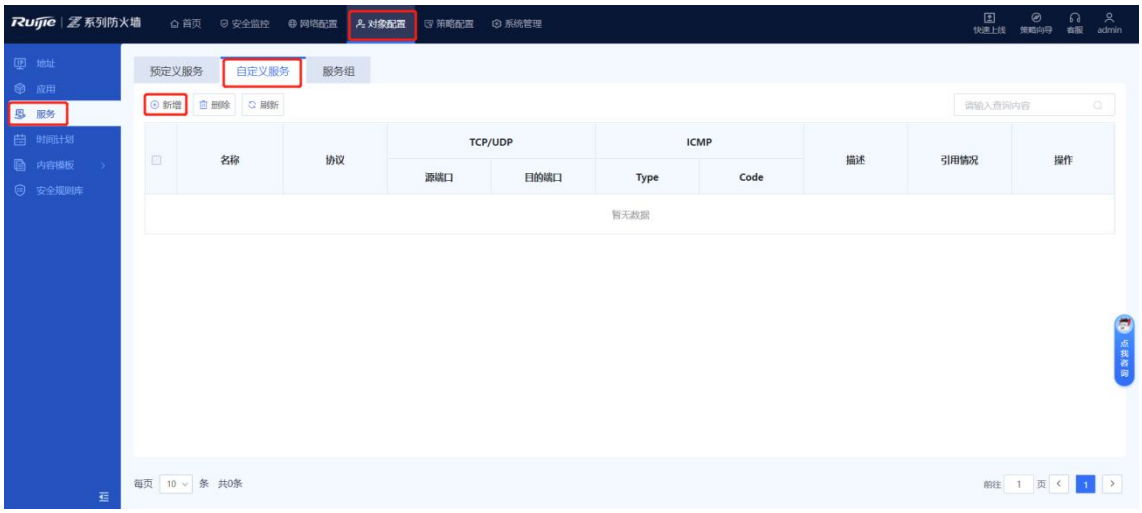
通过指定协议类型（例如TCP、UDP或ICMP）和端口号等信息自定义应用协议类型。

【操作步骤】

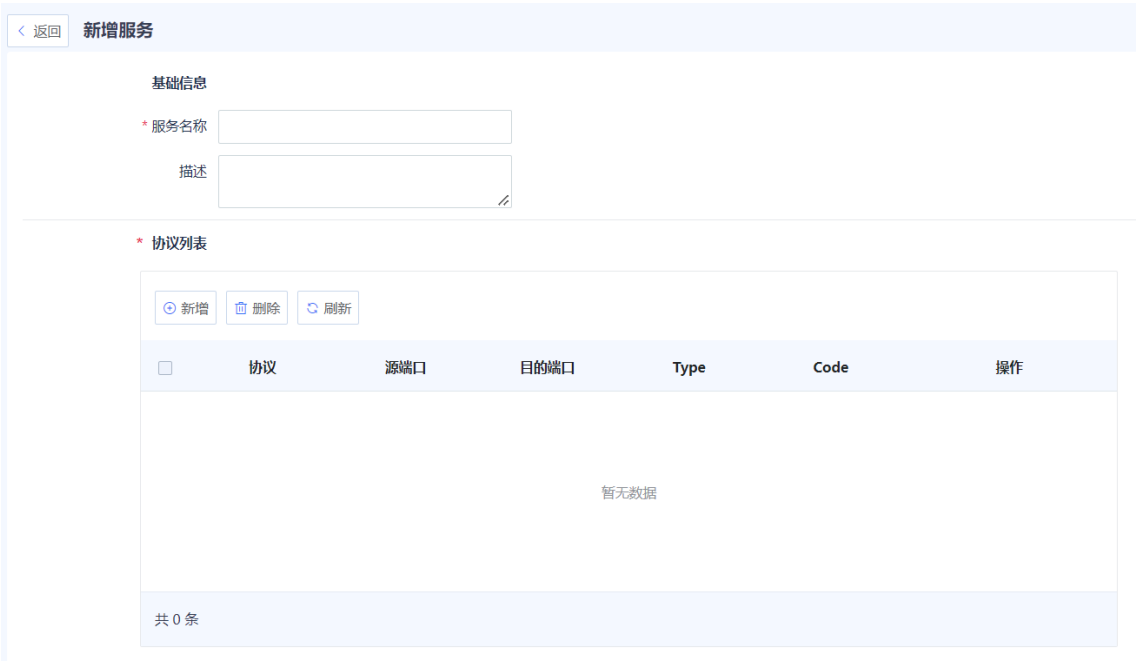
(1) 进入[新增服务]页面。

a 点击[对象配置]>>[服务]>>[自定义服务]菜单项。

b 点击<新增>。



(2) 设置服务相关配置项。



配置项	说明	配置方法
基础信息		
服务名称	新增服务的名称。	● 支持输入任意字符。 ● 不允许与已有应用同名。 ● 一经创建，无法修改应用组名称。 [示例] 服务1
描述	新增服务的描述信息，以便区分不同的服务。	支持输入任意字符。 [示例] New service
协议列表 新增服务中包含的协议。点击<新增>，在[新增协议配置]中进行设置，并单击<确认>。		
TCP协议	使用TCP协议的服务。	需要配置如下参数： ● 协议号 ● 源端口 ● 目的端口
UDP协议	使用UDP协议的服务。	需要配置如下参数： ● 协议号 ● 源端口 ● 目的端口

配置项	说明	配置方法
ICMP	使用ICMP协议的服务。	需要配置如下参数： ● 协议号 ● Type ● Code

(3) 点击<确认>。

【后续处理】

- 管理员只能删除引用情况为0的服务。
- 管理员无法新增、删除、和修改[对象配置]>>[服务]>>[预定义服务]中的服务，预定义服务是当前常用的服务类型的预先定义。

6.3.3 创建服务组

【应用场景】

通过创建服务组，可以管理多个服务。

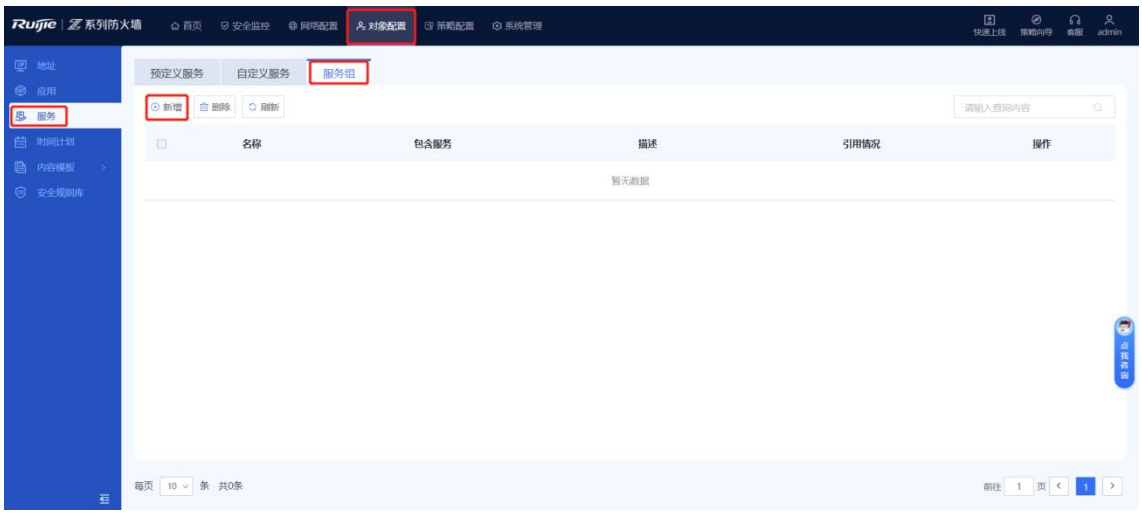
服务组中可以加入自定义服务和预定义服务。

【操作步骤】

(1) 进入[新增服务组]页面。

a 点击[对象配置]>>[服务]>>[服务组]菜单项。

b 在操作区上方，点击<新增>。



(2) 设置服务组相关配置。

配置项	说明	配置方法
基础信息		
服务组名称	新增服务组的名称。	• 支持输入任意字符。 • 不允许与已有应用同名。 [示例] Service group 1
描述	新增服务组的描述信息，以便区分不同的服务组。	支持输入任意字符。 [示例] New service group
服务列表	新增服务组中包含的服务。	在“待选”区域选择对应的服务，该服务将自动添加到“已选”区域。 [示例] ssh

(3) 点击<保存>。

【后续处理】

管理员只能删除引用情况为0的服务组。

6.4 时间计划

6.4.1 简介

时间计划从时间段范围控制各类策略是否生效，从而达到基于时间段对网络进行管理的目的。

时间计划分为：

- 单次时间计划

  指从设定的起始时间到终止时间之间的时间段，该时间段无法循环出现，也没有周期。

  例如，可以通过定义单次时间计划实现只允许员工从2022-04-30晚上19:00:00至第二天24:00:00:00这段时间访问外网，其他时间均不允许。

- 循环时间计划

  指每个星期中固定的时间段，该时间段以一个星期为间隔循环出现。周期时间段由“开始时间”、“结束时间”与“每周生效时间”三个数据确定。

  例如，可以通过定义周期时间段实现只允许员工每周五晚上19:00:00至22:00:00访问外网，其他时间均不允许。

6.4.2 创建循环时间计划

【应用场景】

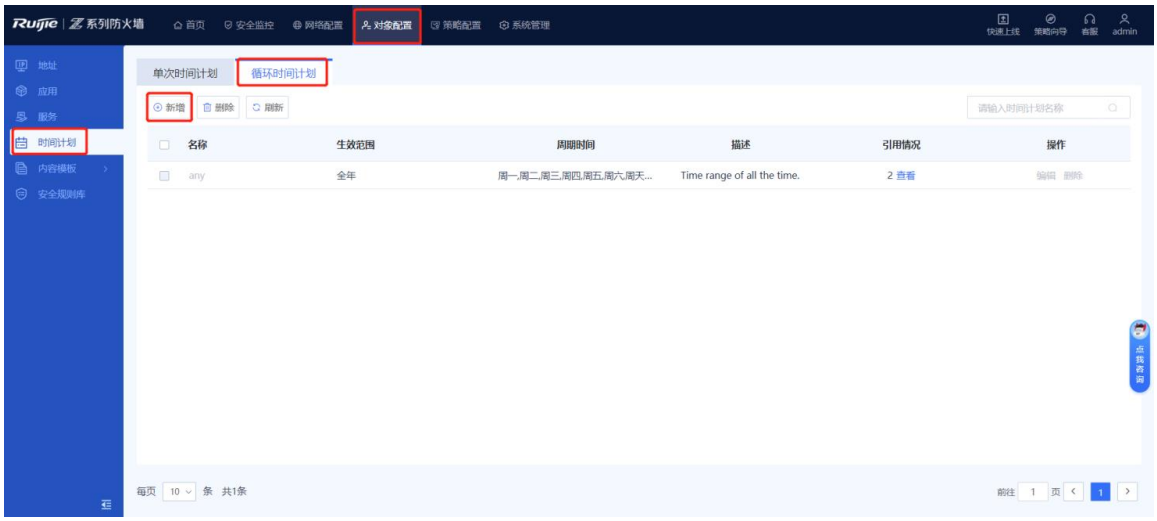
使用循环时间计划时，策略将按照时间策略定时生效。

【操作步骤】

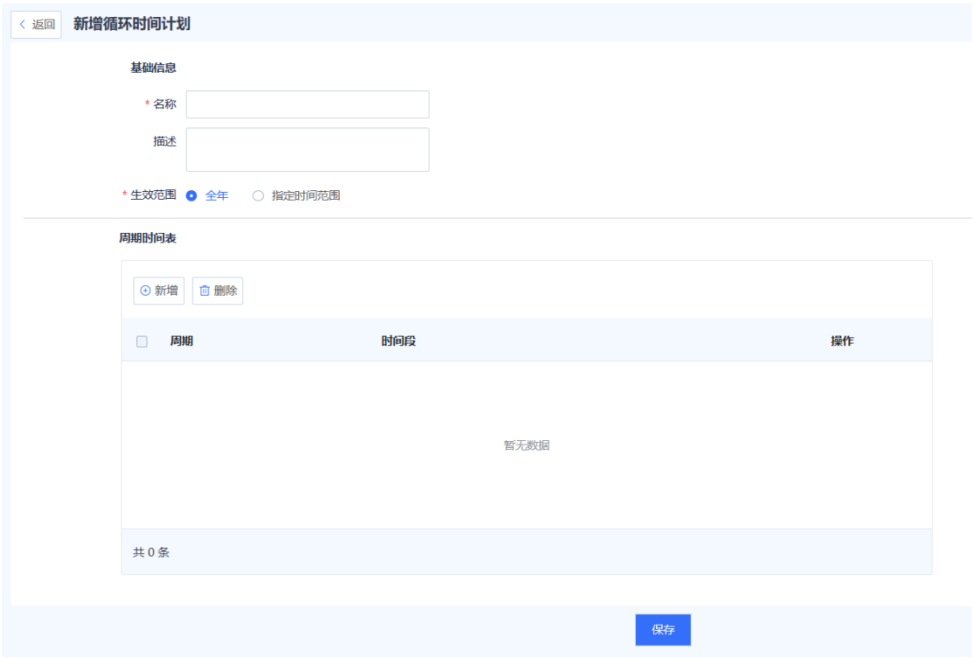
(1) 进入[新增循环时间]页面。

a 点击[对象配置]>>[时间计划]>>[循环时间计划]菜单项。

b 在操作区上方，点击<新增>。



(2) 设置循环时间计划相关配置。



配置项	说明	配置方法
名称	新增循环时间计划的名称。	支持输入任意字符。 [示例] 计划1
描述	新增循环时间计划的描述信息，以便区分不同的循环时间计划。	支持输入任意字符。 [示例] 计划1
生效范围	新增循环时间计划的生效时间范围。	默认全年生效，可以设置在指定时间范围生效。 [示例] 全年
周期时间表	循环时间计划的时间策略。	点击<新增>，选择每周执行的天数及时间段。

(3) 点击<保存>。

【后续处理】

管理员只能删除引用情况为0的循环时间计划。

6.4.3 创建单次时间计划

【应用场景】

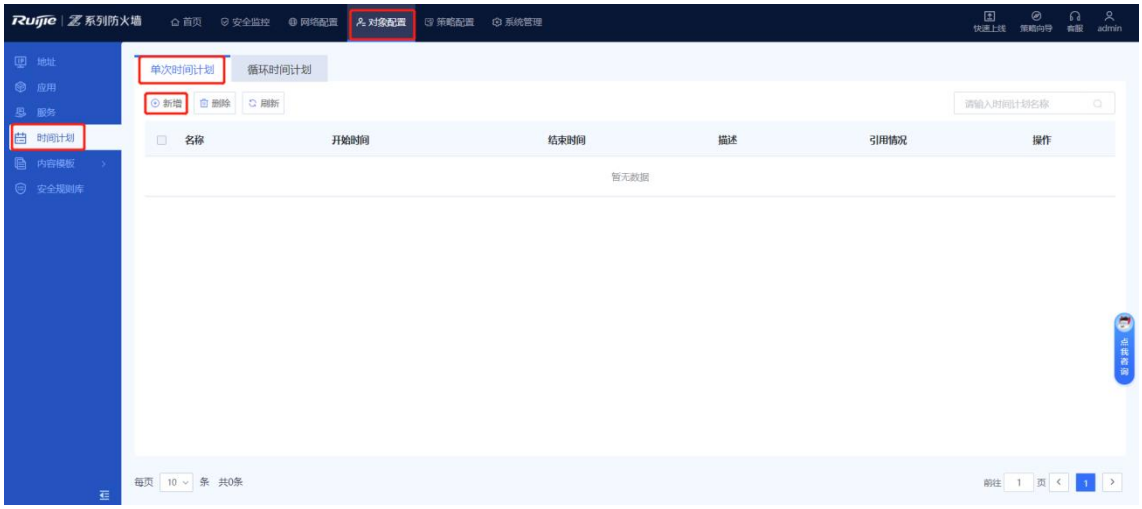
使用单次时间计划时，策略仅执行一次。

【操作步骤】

(1) 进入[新增单次时间计划]页面。

a 点击[对象配置]>>[时间计划]>>[单次时间计划]菜单项。

b 在操作区上方，点击<新增>。



(2) 设置单次时间计划相关配置项。

配置项	说明	配置方法
名称	新增单次时间计划的名称。	支持输入任意字符。 [示例] 计划1
描述	新增单次时间计划的描述信息，以便区分不同的单次时间计划。	支持输入任意字符。 [示例] 计划1
开始时间	新增单次时间计划的开始时间。	[示例] 2022-02-16 00:00:00
结束时间	新增单次时间计划的结束时间。	[示例] 2022-02-16 12:00:00

(3) 点击<保存>。

【后续处理】

管理员只能删除引用情况为0的单次时间计划。

6.5 内容模板

6.5.1 病毒防护

1. 简介

病毒防护是一种安全检测技术，通过实时对网络流量、文件进行分析，识别其中隐藏的病毒并进行告警或阻断，保护内网数据安全。

本功能支持对HTTP、FTP、SMTP、POP3协议传输的视频文件、音频文件、图片文件、可执行文件、文档、压缩文件、网页文件、代码文件、脚本文件、文本文件等进行病毒检测。

病毒检测支持快速查杀和深度查杀两种模式，不同的模式使用的病毒防护特征库不同：

- 快速查杀：使用的是病毒防护特征库（快速查杀），检出率低，性能开销小。
- 深度查杀：使用的是病毒防护特征库（深度查杀），检出率高，性能开销大。

2. 自定义病毒防护模板

【应用场景】

设备提供了一个预定义模板，用户也可以根据不同的防护场景自定义模板。

【前置条件】

您已安装并激活AV许可授权，有关授权激活的详细介绍请参见8.3 激活授权。

说明

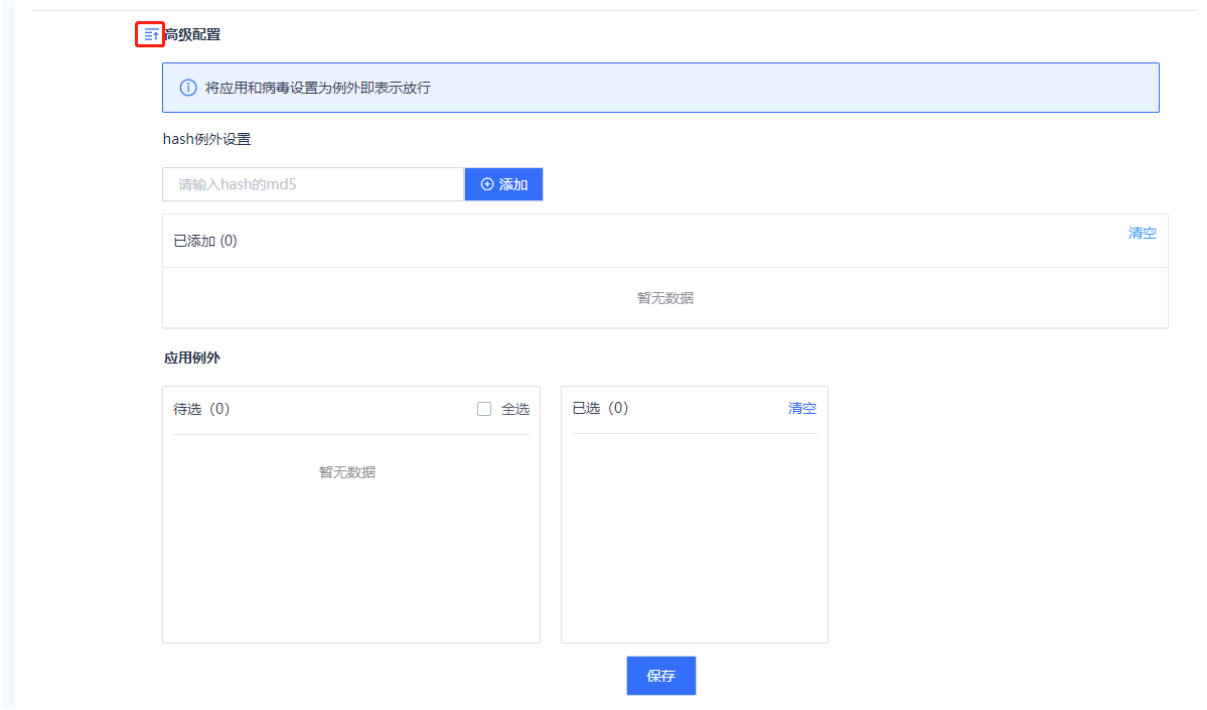
- AV试用许可过期后，病毒防护功能不可用，也不能升级病毒库。
- AV正式许可过期后，病毒防护功能可用，但不能升级病毒库。

【操作步骤】

(1) 点击[对象配置]>>[内容模板]>>[病毒防护>>[自定义模板]菜单项。

(2) 在操作区上方，点击<新增>。

(3) 根据下表参数说明配置模板参数。



配置项	说明	配置方法
基础信息		
模板名称	病毒防护模板的名称。	名称不能包含字符：`~!#%^&*+\/0::"/<>?和空格。 [示例] Template_1
描述	病毒防护模板的描述信息。	描述不能包含字符：`~!#%^&*+|;:'"/<>?。 [示例] 该模板仅用于对全网HTTP流量进行检测。
扫描模式		
扫描模式	支持快速查杀和深度查杀两种模式，不同的模式使用的病毒防护特征库不同： ● 快速查杀：检出率低，性能开销小。 ● 深度查杀：检出率高，性能开销大。	[示例] 快速查杀
协议	指定需要进行病毒检测的协议流量及放行。 未指定的协议流量直接放行，不会进行检测。	-
高级配置（点击 设置高级配置）		
hash例外设置	将指定MD5值设置为例外后，当设备检测到符合该MD5值的报文，设备将对其执行放行动作。	-

配置项	说明	配置方法
应用例外	将指定应用设置为例外后，当设备检测到符合该应用的报文时，设备将对其执行放行动作。	-

(4) 配置完成，点击<保存>。

【后续处理】

自定义病毒防护模板必须被安全策略引用才能触发病毒检测机制，有关安全策略的详细介绍请参见5.1 安全策略。

3. 查看预定义防毒防护模板

【应用场景】

通过查看预定义内容模板可以了解其所检测的协议类型特征，方便后续进行配置。

【前置条件】

预定义模板不允许删除或编辑，但可以将其复制为自定义模板后再进行编辑操作。

【操作步骤】

(1) 点击[对象配置]>>[内容模板]>>[病毒防护>>[预定义模板]菜单项。

(2) 点击模板名称或操作列的“复制”可以复制该模板，再根据实际业务场景修改参数设置，快速创建模板。

(3) 配置完成，点击<保存>。

【后续处理】

自定义病毒防护模板必须被安全策略引用才能触发病毒检测机制，有关安全策略的详细介绍请参见5.1 安全策略。

4. 升级病毒防护特征库

病毒防护特征库会持续更新，以保持最高水平的安全性。通过升级病毒防护特征库，可以检测更多类型的病毒。有关特征库升级的详细介绍请参见8.5 特征库升级。

6.5.2 入侵防御

1. 简介

入侵防御系统(IPS:IntrusionPreventionSystem)是一种安全防御技术，通过实时对网络流量进行分析，检测识别流量中隐藏的恶意信息（包括缓冲区溢出攻击、木马、蠕虫等），并进行实时的告警和阻断，实时地中止入侵行为。

使用IPS技术，可以自动丢弃入侵报文或者阻断攻击源，从根本上避免攻击行为，保护企业信息系统和网络架构免受侵害。

2. 自定义 IPS 内容模板

【应用场景】

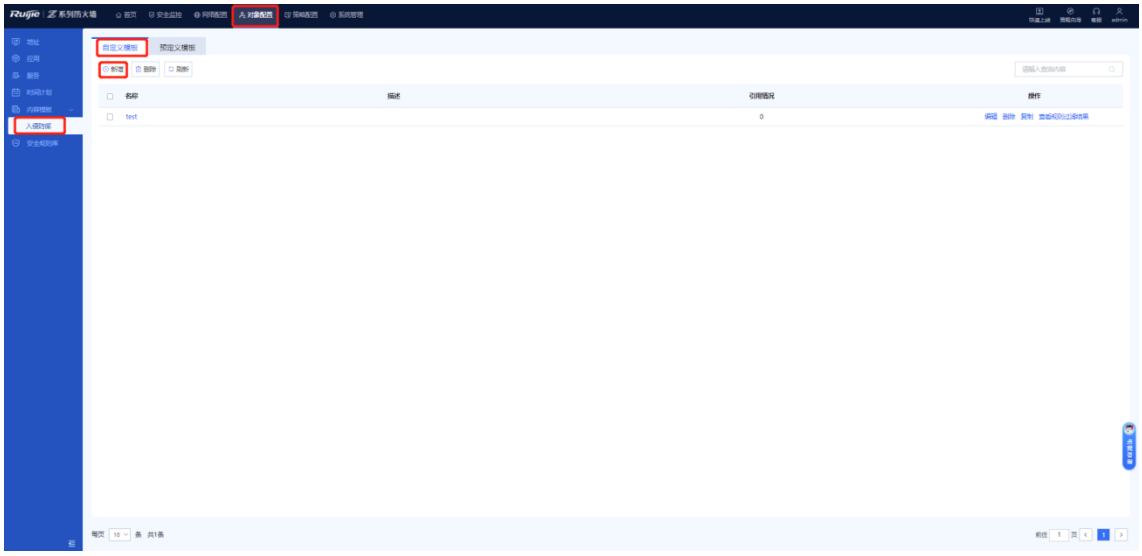
根据不同的防护场景，用户可以使用自定义模板创建入侵防御系统策略。

【操作步骤】

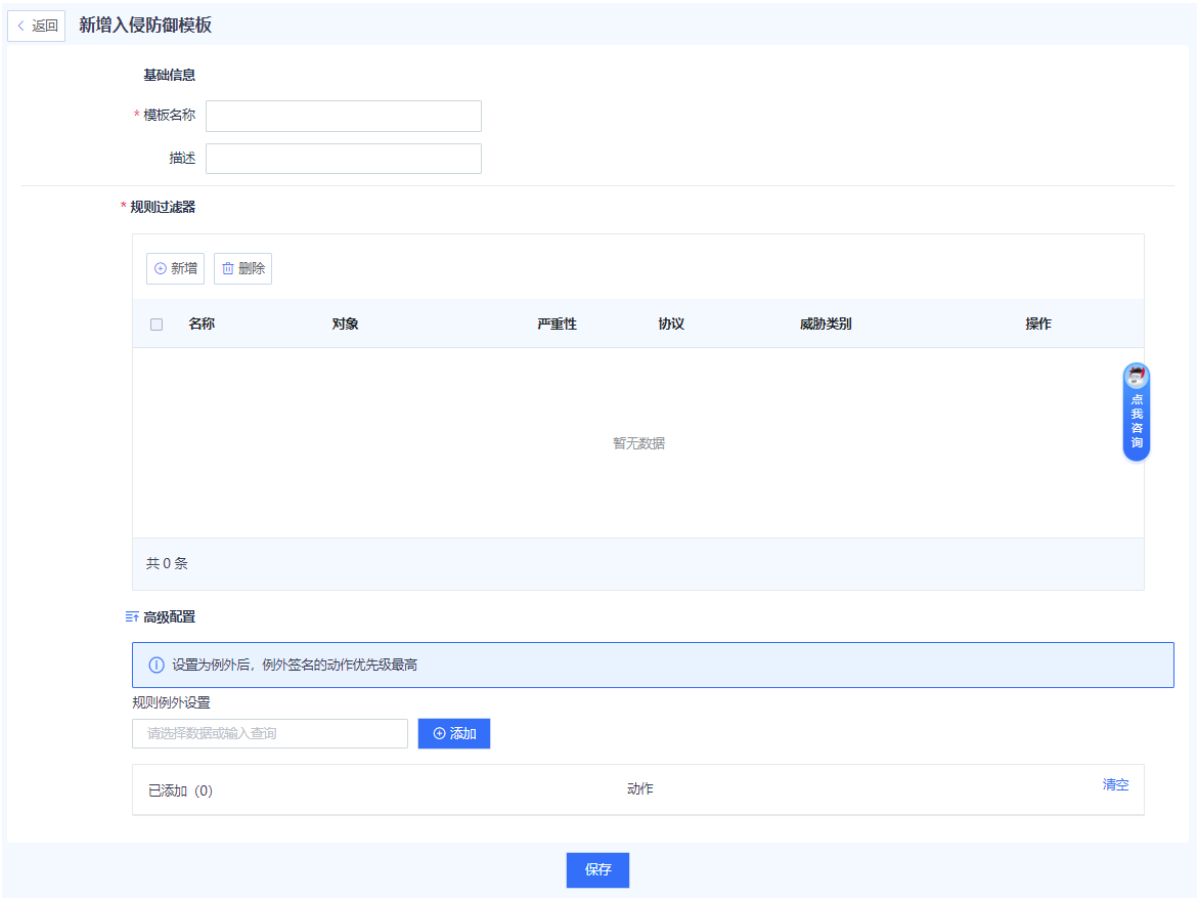
(1) 进入[新增入侵防御模板]页面。

a 点击[对象配置]>>[内容模板]>>[入侵防御]>>[自定义模板]菜单项。

b 在操作区上方，点击<新增>。



(2) 设置防御模板相关配置。



a 根据入侵防御场景或防护需求，填写自定义模板的名称和描述。

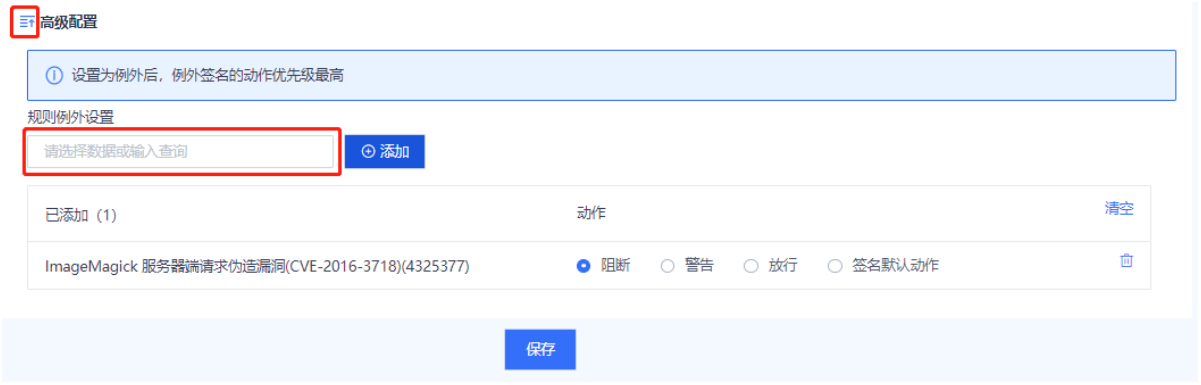
b 在“规则过滤器”区域，点击<新增>，配置相关参数后点击<确认>。

新增规则过滤器
* 名称
* 对象
全部
服务端
客户端
* 严重性
全部
高
中
低
提示
协议
待选（5）
全选
已选（0）
清空
请输入查询内容
DNS
HTTP
TCP
TLS
UDP
威胁类别
待选（92）
全选
已选（0）
清空
请输入查询内容
暴力破解
拒绝服务
反序列化
事件监控
信息泄露
注入攻击
取消
确认

配置项	说明	配置方法
名称	新增规则过滤器的名称。	• 支持输入任意字符。 • 建议使用可以说明该过滤器功能的描述作为名称。 [示例] Filter1
对象	需要保护的对象。	[示例] 全部
严重性	描述攻击后果的严重性。分为高、中、低和提示。 例如，只勾选高，那么只有严重性高的安全规则能命中该过滤器。	[示例] 高
协议	指定过滤器需要检测的协议。 未指定的协议流量不会命中该过滤器。	[示例] DNS
威胁类别	指定过滤器需要检测的威胁类别。 非指定的威胁类别的流量不会命中该过滤器。	[示例] 暴力破解

c （可选）点击“高级配置”前面的 展开高级配置参数。

点击输入框选择例外规则，点击<添加>，然后在下方已添加列表设置该规则的执行动作。规则设置为例外后，无论该模板设置的动作是什么，命中此规则的报文始终按例外动作执行。



(3) 点击<保存>。

3. 查看预定义 IPS 内容模板

【应用场景】

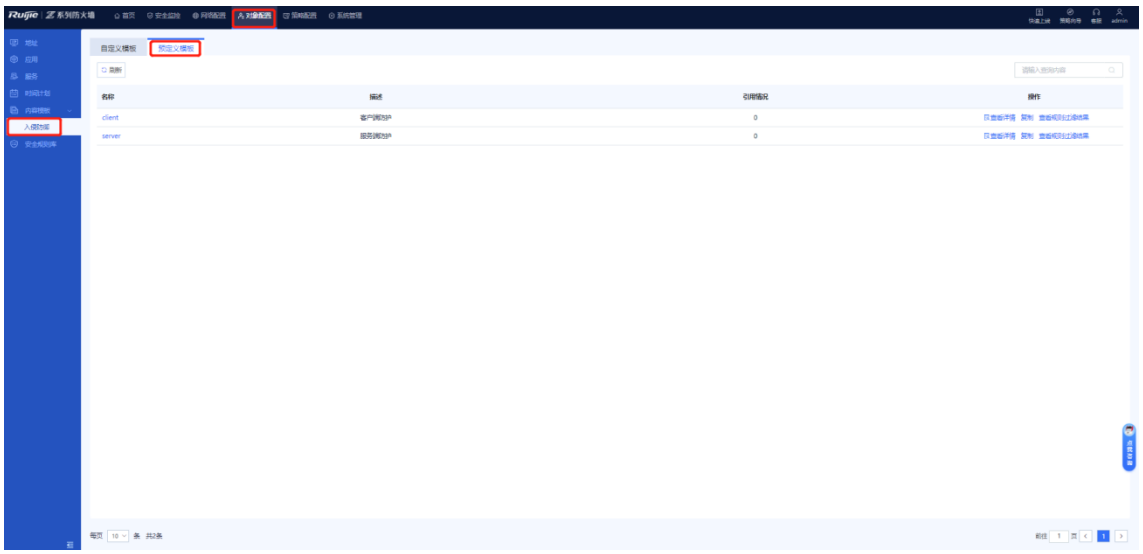
通过查看预定义内容模板可以了解其所检测的入侵的特征，方便后续进行配置。

【前置条件】

预定义模板不允许添加或编辑，但可以将其复制为自定义模板后再进行编辑操作。

【操作步骤】

(1) 点击[对象配置]>>[内容模板]>>[入侵防御]>>[预定义模板]菜单项。



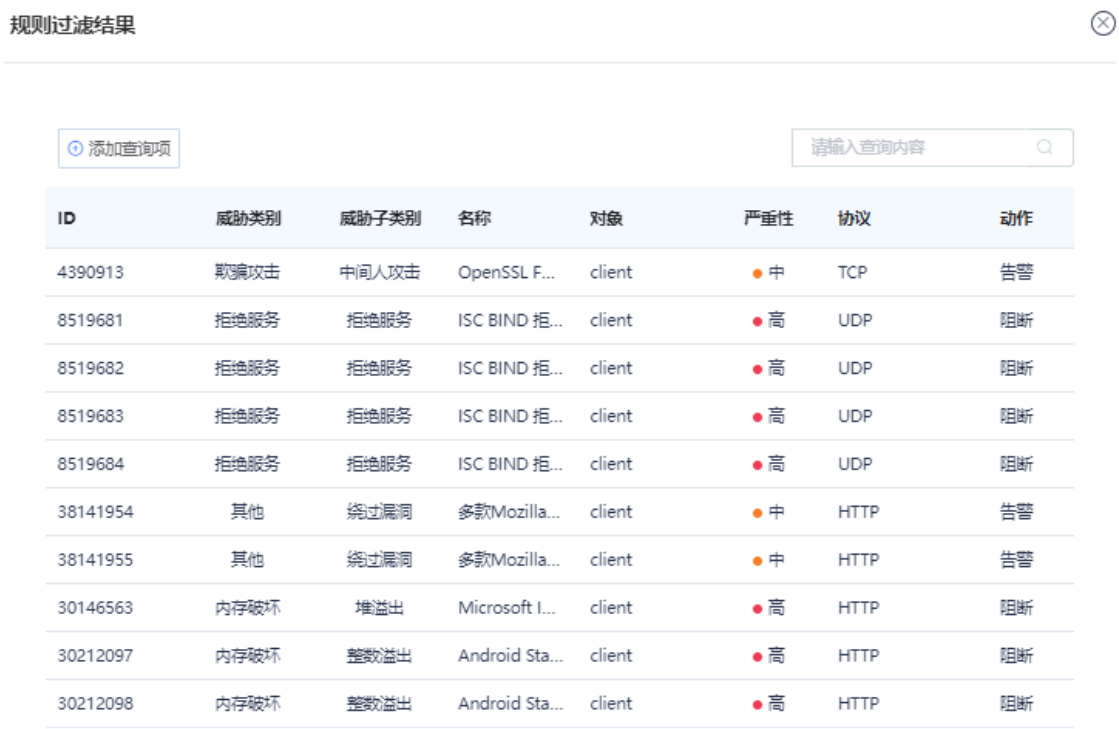
(2) 选择一个预定义模板，执行对应操作。

- 点击<查看详情>，查看预定义模板的名称、描述、规则过滤器详细信息。

配置项	说明
基本信息	
模板名称	预定义内容模板的名称。
描述	预定义内容模板的描述。
规则过滤器	
名称	预定义模板的名称。

配置项	说明
对象	描述所检测的对象，用来描述网络威胁的攻击对象。 ● 服务端：即一个连接中接受访问的一端。该检测主要针对服务器的漏洞发起的攻击。 例如，当本端接受访问时，受到发起访问一端的攻击。本端即为服务端。 ● 客户端：即一个连接中发起访问的一端。该检测主要针对客户端（如PC等）的漏洞发起的攻击。 例如，当用户向含有恶意代码的服务器发起访问时，受到攻击。用户即为客户端。
严重性	描述攻击后果的严重性。分为高、中、低和提示。 签名的严重性越高，说明命中签名的攻击产生的后果越严重。
协议	预定义内容模板检测的协议类型，用来描述网络威胁使用的协议类型。
威胁类别	描述网络威胁的类别。

- 点击<查看规则过滤结果>，查看过滤结果。



配置项	说明
ID	过滤规则的ID。
威胁类别	过滤规则检测的威胁类别。
威胁子类别	过滤规则检测的威胁子类别。
名称	过滤规则的名称。

配置项	说明
对象	描述过滤规则所检测的对象，用来描述网络威胁的攻击对象。
严重性	描述攻击后果的严重性。分为高、中、低和提示。
协议	过滤规则检测的协议类型，用来描述网络威胁使用的协议类型。
动作	过滤规则定义的动作。 ● 放行：当报文命中此过滤规则时，允许通过，且不会记录日志。 ● 告警：当报文命中此过滤规则时，允许通过，但会记录日志。 ● 阻断：当报文命中此过滤规则时，丢弃报文，并记录日志。

说明

点击<添加查询项>可以设置查询条件，界面仅显示对应的结果。

- 点击<复制>，复制预定义模板的内容，并根据业务需要进行修改。

4. 升级 IPS 特征库

入侵防御特征库会持续的更新，以保持最高水平的安全性。通过升级IPS特征库，以保持入侵防御的持续有效性。有关特征库升级的详细介绍请参见8.5 特征库升级。

6.6 安全规则库管理

【应用场景】

安全规则库存储了设备能够从流量中检查出来的威胁的相关特征信息。当流量经过设备时，入侵防御功能会将流量与安全规则库中的特征进行对比，如果匹配为威胁，将根据用户配置进行相应的处理。

【操作步骤】

(1) 点击[对象配置]>>[安全规则库]菜单项。

(2) 对安全规则执行对应的操作。

- 启用某条规则，对经过设备的流量检测该条规则定义的威胁。
- 禁用某条规则，在对流量进行检测时将跳过对该规则的检测。

7 网络配置

7.1 接口

7.1.1 设置物理接口

【应用场景】

物理接口即设备面板上真实连接网线的接口。网线和水晶头的状态会影响物理接口能否正常工作。

【前置条件】

物理接口配置前，请确认网线连接正常。

【配置步骤】

(1) 点击[网络配置]>>[接口] >>[物理接口]菜单项。

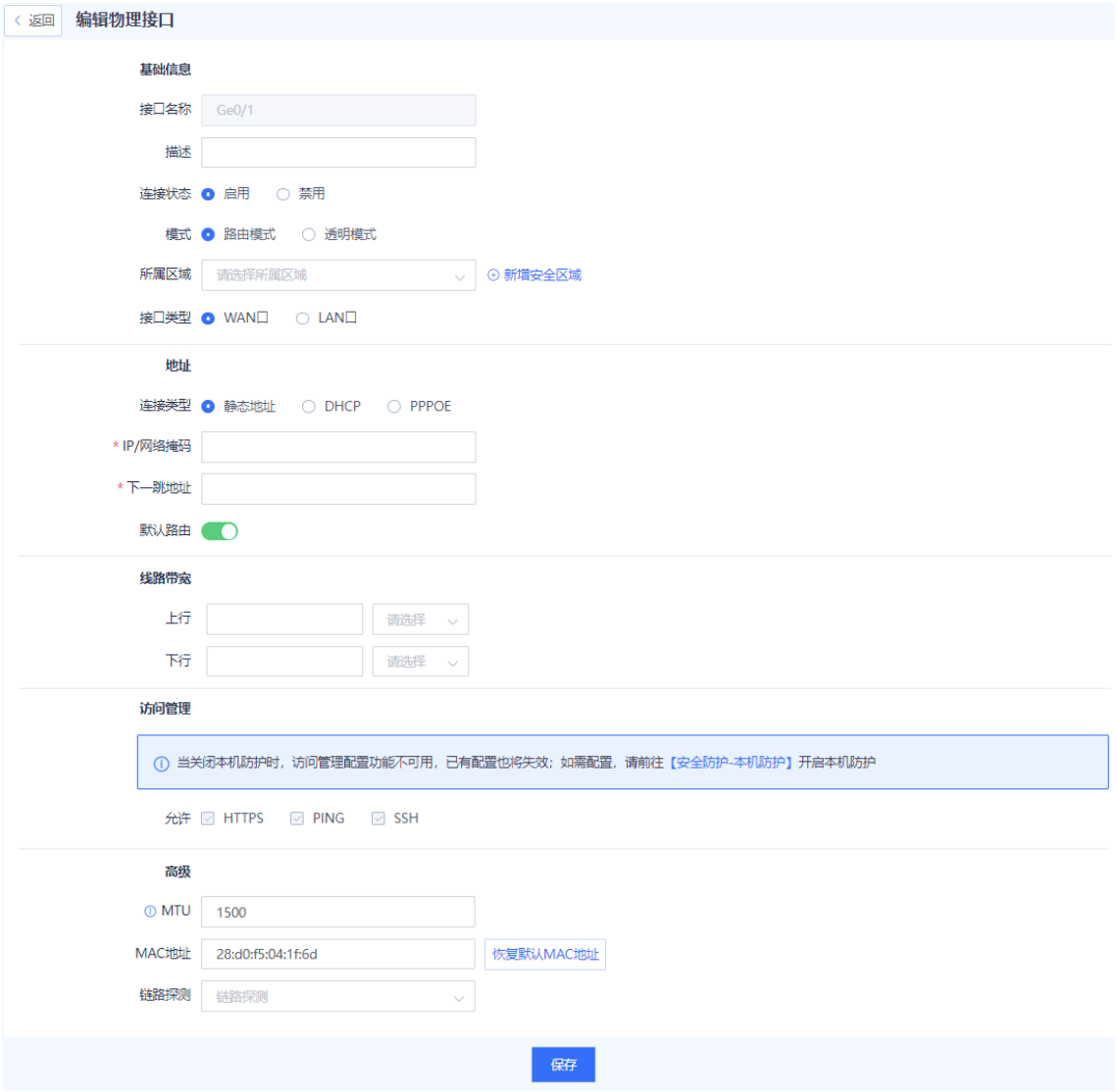
注意

关闭接口开关或修改接口配置可能导致对应接口下全部终端断网。请谨慎操作。

网口状态绿色表示已连接，灰色表示未连接。默认启用所有接口，点击各接口的“ ”可以禁用接口。不允许禁用管理接口Ge0/0。

(2) 在接口右侧，点击<编辑>。

进入[编辑物理接口]页面。



(3) 设置物理接口相关配置项。

配置项	说明	配置方法
接口名称	物理接口的实际名称。	系统自动显示。 [示例] Ge 0/1
描述	接口的描述字段，可以用于标注当前接口用途。	[示例] 连接外网接口
连接状态	用于启用或禁用该配置接口。	[示例] 启用
模式	用于指定接口的接入方式。 ● 路由模式：使用IP地址进行转发。 ● 透明模式：使用MAC地址进行转发。	[示例] 透明模式

配置项	说明	配置方法
所属区域	接口所属的安全区域。	[示例] trust
接口类型	用于指定接口的逻辑属性。	[示例] LAN口
地址		
连接类型	物理接口接入网络的方式，包括静态地址、DHCP、PPPOE。	[示例] 静态地址
IP/网络掩码	物理接口设置的IP地址及网络掩码。	当"连接类型"设置为“静态地址”时，该参数有效。 [示例] 192.168.1.1/24
下一跳地址	转发数据的下一个地址，一般是下一个路由设备的地址。	当"连接类型"设置为“静态地址”时，该参数有效。 [示例] 192.168.1.2/24
帐号	使用PPPOE方式获取IP地址时，拨号使用的帐号。	当"连接类型"设置为“PPPOE”时，该参数有效。 [示例] Admin
密码	使用PPPOE方式获取IP地址时，拨号使用的密码。	当"连接类型"设置为“PPPOE”时，该参数有效。 [示例] Ruijie@123
线路带宽	限制接口的带宽，包括上传带宽和下载带宽。	填写带宽数值，并选择对应单位。 ● 数值范围1~100000000。 ● 单位包括：kbps和mbps。 [示例] 100 kbps
访问管理	指定接口是否允许HTTPS、PING、SSH功能。	设备开启本机防护功能时，该设置有效。 [示例] 勾选HTTPS
高级		

配置项	说明	配置方法
MTU	设置接口单个发送报文最大的数据字节数。MTU值默认1500，即最大效率转发数据。如果上级限制数据包大小导致断网或网速异常，可逐步调整为1492或1400或更小尝试。	设置为64~1600的整数。 [示例] 1500
MAC	设置接口的MAC地址。	[示例] 30:0d:9e:41:d9:0b
链路探测	选择本接口关联的链路探测策略，可以实时测试接口到下一跳之间的网络连通性。	有关链路探测的详细介绍请参见7.6 链路探测。

(4) 点击<保存>。

7.1.2 设置子接口

【应用场景】

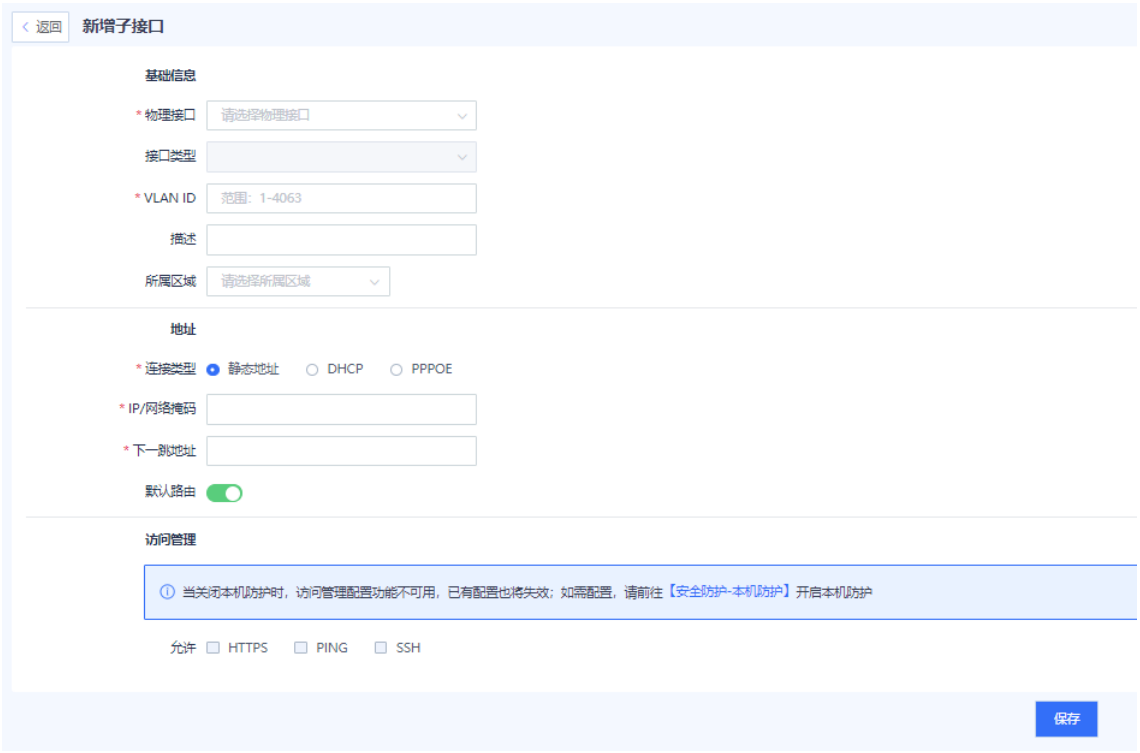
子接口是基于物理的接口创建出来的虚拟接口，通过VLAN来标识，当物理接口收到报文之后，通过判断报文中的VLAN字段，将报文转给对应的子接口进行处理。当用户需要在同一个物理接口，创建多个ip地址进行通信的时候，可以通过创建不同的子接口，然后划分不同VLAN ID，对端设备也创建对应的子接口进行多网段通信。

【操作步骤】

(1) 点击[网络配置]>>[接口] >>[子接口]菜单项。

(2) 点击<新增>。

系统进入[新增子接口]页面。



(3) 设置子接口相关的配置项。

配置项	说明	配置方法
物理接口	需要创建子接口的物理接口。	[示例] Ge 0/1
接口类型	子接口的逻辑类型。	[示例] WAN
VLAN ID	子接口所对应的VLAN ID。	[示例] 1
描述	子接口的描述信息。	[示例] 连接外网接口
所属区域	子接口所属的安全区域。	[示例] trust
地址		
连接类型	物理接口接入网络的方式，包括静态地址、DHCP、PPPOE。	[示例] 静态地址
IP/网络掩码	物理接口设置的IP地址及网络掩码。	当"连接类型"设置为“静态地址”时，该参数有效。 [示例] 192.168.1.1/24
下一跳地址	转发数据的下一个地址，一般是下一个路由设备的地址。	当"连接类型"设置为“静态地址”时，该参数有效。 [示例] 192.168.1.2/24
帐号	使用PPPOE方式获取IP地址时，拨号使用的帐号。	当"连接类型"设置为“PPPOE”时，该参数有效。 [示例] Admin
密码	使用PPPOE方式获取IP地址时，拨号使用的密码。	当"连接类型"设置为“PPPOE”时，该参数有效。 [示例] Ruijie@123
访问管理	指定子接口是否允许HTTPS、PING、SSH功能。	设备开启本机防护功能时，该设置有效。 [示例] HTTPS

(4) 点击<保存>。

【后续处理】

在子接口管理页面，可删除或修改子接口。

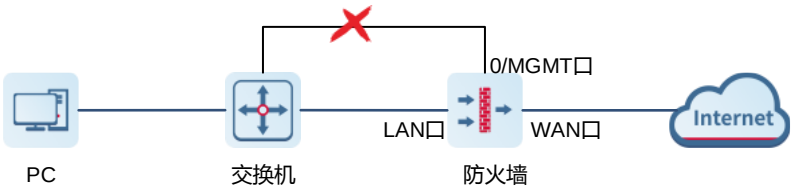
7.1.3 设置桥接口

【应用场景】

桥接口适用于防火墙的透明模式部署场景。

桥口是透明模式下设置的物理接口组成的逻辑虚拟口。通过配置正确的IP地址和网关，防火墙设备可以通过桥口进行三层转发。

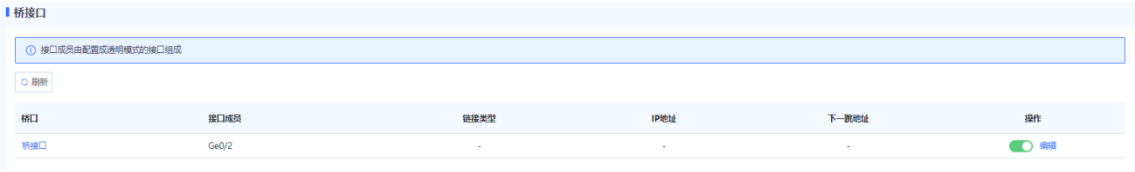
此外，实际组网时无需单独将0/MGMT口与交换机等设备连接，通过桥口即可实现远程维护，实施简单方便。



【操作步骤】

(1) 点击[网络配置]>>[接口] >>[桥接口]菜单项。

系统显示当前系统已配置的桥接口成员。



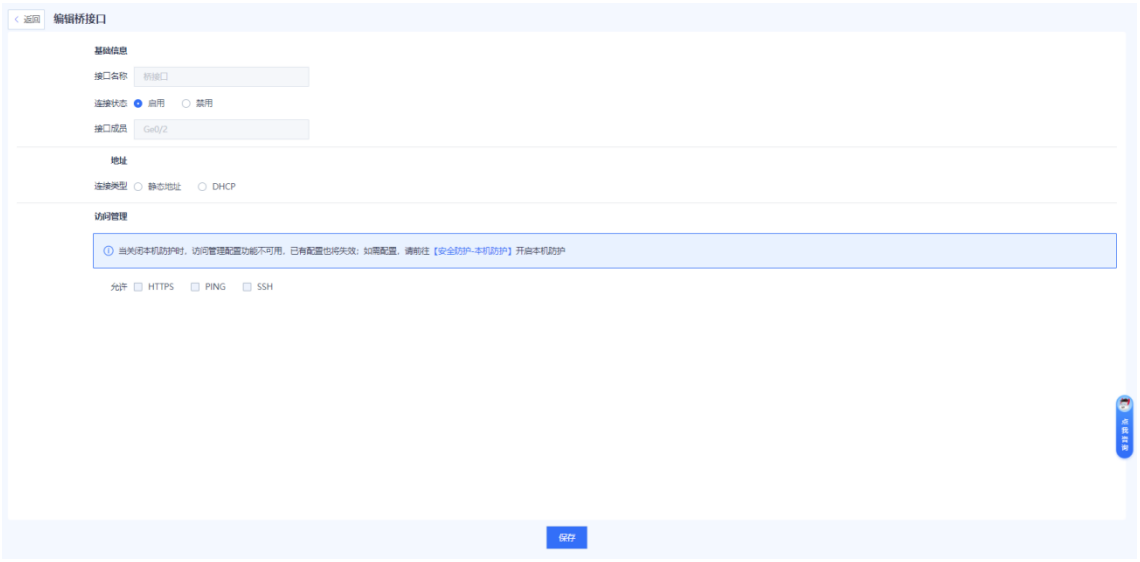
说明

系统会将所有配置为透明模式的接口设置为桥接口成员。

(2) 根据业务需要，对桥接口进行对应的操作。

- 如果有新增配置物理接口为透明模式，点击<刷新>可以获取最新的接口成员信息。
- 点击“ ”可以启用或禁用桥接口。
- 点击<编辑>，设置桥接口相关配置。

  在[编辑桥接口]页面，配置桥接口相关配置项，并点击<保存>。


返回
编辑桥接口
基础信息
接口名称
桥接口
连接状态
启用
禁用
接口成员
Gei0/2
地址
连接类型
静态地址
DHCP
访问管理
当关闭本机防护时，访问管理配置功能不可用，已有配置也将失效；如需配置，请前往【安全防护-本机防护】开启本机防护
允许
HTTPS
PING
SSH
保存

配置项	说明	配置方法
接口名称	桥接口的名称。	默认为“桥接口”，且不支持修改。 [示例] 桥接口
连接状态	是否启用桥接口。	[示例] 启用
接口成员	桥接口中包含的接口成员。 所有配置为透明模式的物理接口，都默认为桥接口的接口成员。	[示例] Ge0/2
地址		
连接类型	桥接口的连接类型，包括： ● 静态地址：适用于网络管理员根据预先定义好的IP地址规划来分配给设备的场景，要求网络管理员拥有一定的网络知识。需要配置“IP/网络掩码”和“下一跳地址”。 ● DHCP：适用于非专业的网络管理人员，用户通过连接防火墙就可以自动获取上网IP的场景。	[示例] 静态地址
IP/网络掩码	接口的IP地址及网络掩码。	当“连接类型”设置为“静态地址”时需要配置该参数。 [示例] 192.168.20.1/24
下一跳地址	要到达目的地址路由器所通过的下一个路由器地址。	“连接类型”设置为“静态地址”时需要配置该参数。 [示例] 192.168.20.2/24
默认路由	是否启用默认路由。	[示例] 启用
访问管理	桥接口是否允许HTTPS、PING、SSH功能。	设备开启本机防护功能时，该设置有效。 [示例] 勾选HTTPS

7.2 安全区域

7.2.1 简介

安全区域（Security Zone），是设备所引入的一个安全概念。一个安全区域是若干接口所连网络的集合，这些网络中的用户具有相同的安全属性。

由于不同的网络部署以及业务需求，不同的网络设备具有不同安全级别要求。引入安全区域的概念之后，网络管理员可以将具有相同安全级别要求的网络设备划入同一个安全区域。由于同一安全区域内的网络设备是“同样安全”的，防火墙认为在同一安全区域内部发生的数据流动是不存在安全风险的，不需要实施任何安全策略。只有当不同安全区域之间发生数据流动时，才会触发设备的安全检查，并实施相应的安全策略。

系统默认存在trust、untrust、DMZ安全区域。

安全区域名称	说明
trust	安全级别较高的安全区域。通常用于定义内网终端用户所在区域。
untrust	安全级别较低的安全区域。通常用于定义Internet等不安全的网络。
DMZ	通常用于定义内网服务器所在区域。因为这种设备虽然部署在内网，但是经常需要被外网访问，存在较大安全隐患，同时一般又不允许其主动访问外网，所以将其部署一个优先级比trust低，但是比untrust高的安全区域中。

安全区域间的数据流动具有方向性，包括入方向（Inbound）和出方向（Outbound）。

- 入方向：数据由低优先级的安全区域向高优先级的安全区域传输。
- 出方向：数据由高优先级的安全区域向低优先级的安全区域传输。

通常情况下，通信双方一定会有交互报文，即安全域间的两个方向上都有报文的传输。而判断一条流量的方向应以发起该条流量的第一个报文为准。

例如，发起连接的终端位于trust区域，它向位于untrust区域的Web服务器发送了第一个报文，以请求建立HTTP连接。由于untrust区域的优先级比trust区域低，所以防火墙设备将认为这个报文属于Outbound方向，并根据Outbound方向上的配置决定是否匹配并进一步处理该数据流。

7.2.2 创建安全区域

【应用场景】

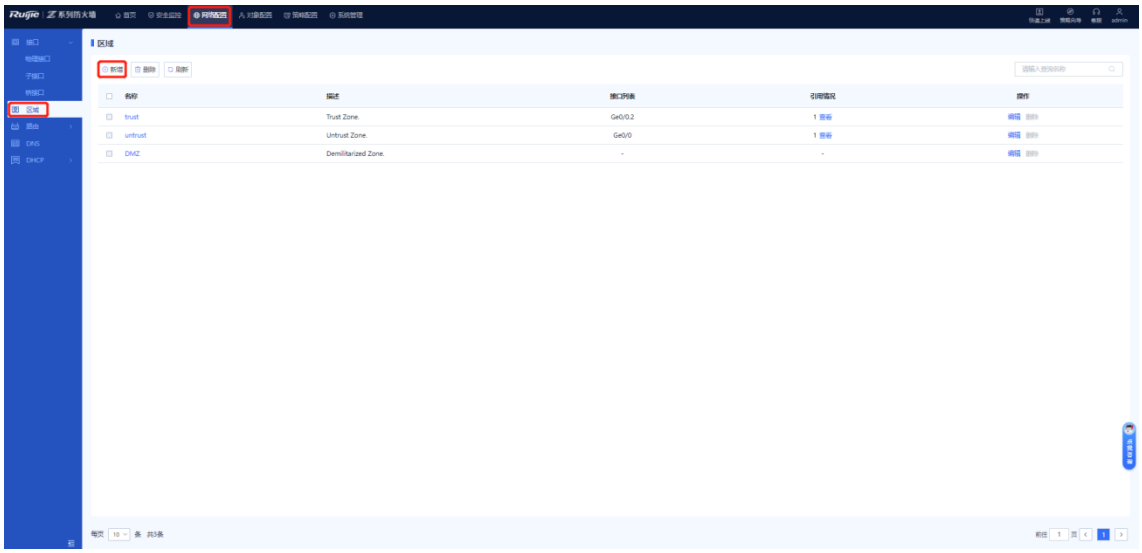
根据业务需要，用户可以自定义创建新的安全区域将接口添加到对应的安全区域中，再通过创建策略对不同区域之间相互访问的流量做管理。

【操作步骤】

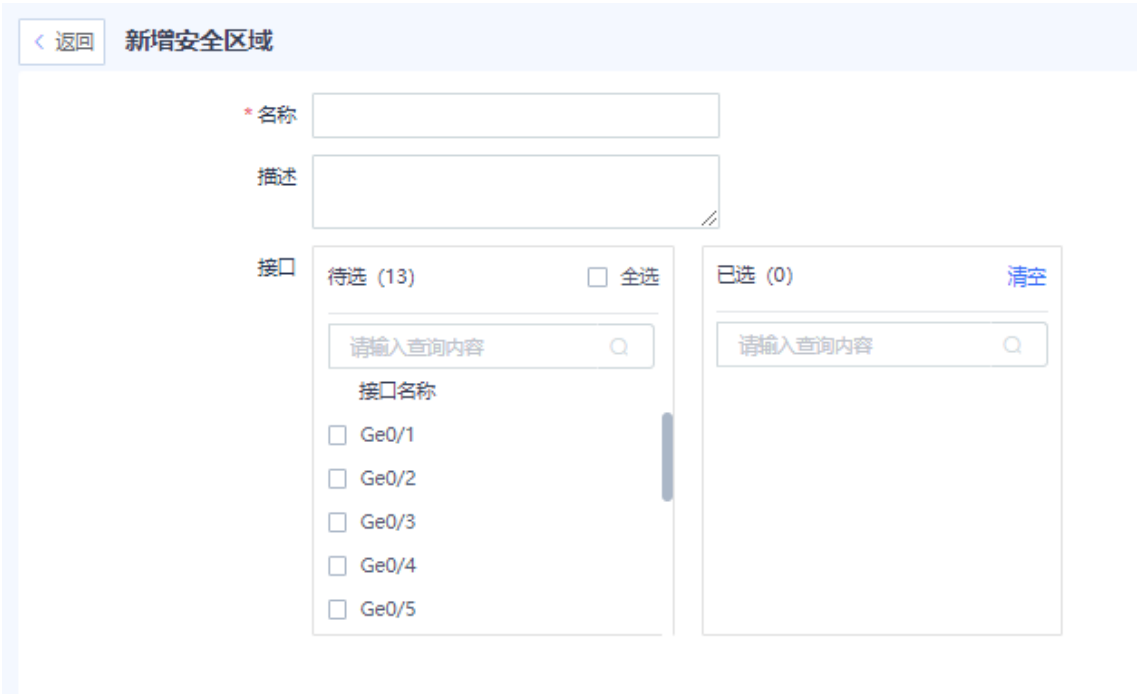
(1) 进入[新增安全区域]页面。

a 点击[网络配置] >> [区域]菜单项。

b 在操作区上方，点击<新增>。



(2) 设置安全区域的相关信息。



配置项	说明	配置方法
名称	安全区域名称。	支持输入任意字符。 [示例] Zone1
描述	安全区域的描述信息，方便区分不同的安全区域。	支持输入任意字符。 [示例] New zone
接口	安全区域中包含的接口。	● 在“待选”区域选择对应的接口，该接口将自动添加到“已选”区域。 ● 同一个接口不能加入不用的安全区域。 ● 如果接口未加入任何安全域，则该接口无法转发报文。 [示例] Ge0/1

(3) 点击<保存>。

【后续处理】

- 只能删除引用情况为0的安全区域。
- 默认的trust、untrust、DMZ及引用情况不为0的安全区域无法删除。
- 若要批量删除多条安全区域，请勾选多条待删除的安全区域并点击<删除>。

7.3 路由管理

7.3.1 简介

路由是数据通信网络中最基本的要素。路由信息就是指导报文发送的路径信息，路由的过程就是报文转发的过程。

设备支持以下两种路由：

- 静态路由：当设备从一个接口上收到数据包后，静态路由功能将根据数据包的目的地址选择并转发至另一个接口。
- 策略路由：根据用户制定的策略进行报文转发。例如，用户可以指定满足某些条件（如源安全区域、源地址、目的地址、服务）的报文从指定出接口转发。

策略路由优先级高于静态路由。当网络结构比较简单时，只需配置静态路由就可以使网络正常工作。静态路由配置方便，对系统要求低，适用于拓扑结构简单并且稳定的小型网络。缺点是不能自动适应网络拓扑的变化，需要人工干预。

7.3.2 创建静态路由

【应用场景】

通过该操作，可以配置IP地址、下一跳地址、接口实现网络互联，进行数据包转发。

【配置步骤】

(1) 进入[新增静态路由]页面。

a 点击[网络配置]>>[路由] >>[静态路由]菜单项。

b 点击<新增>按钮。

(2) 设置静态路由相关配置项。

配置项	说明	配置方法
目的网段/掩码	路由所匹配数据包的目的网段。	[示例] 192.168.10.0/24
下一跳地址	转发数据的下一个地址，一般是下一个路由设备的地址。	[示例] 192.168.20.1
接口	转发数据的出接口。	配置静态路由时，可以同时指定下一跳和出接口，也可以根据实际接口情况，只指定出接口或者下一跳地址。 [示例] Ge0/1
优先级	网段相同的情况下，优先级高的表项优先被匹配中。默认优先级为5。	● 取值范围为1~255。 ● 数值越小，优先级越高。 ● 数值相同，子网掩码越大优先级越高。 [示例] 15
链路探测	选择出接口关联的链路探测策略，可以实时测试出接口到下一跳之间的网络连通性。当出接口到下一跳之间网络不通时，该条静态路由将会失效。	有关链路探测的详细介绍请参见7.6 链路探测。
描述	静态路由的描述信息。	不能包含字符：`~!#%^&*+|;:'"/<>?

(3) 点击<保存>。

7.3.3 创建策略路由

【应用场景】

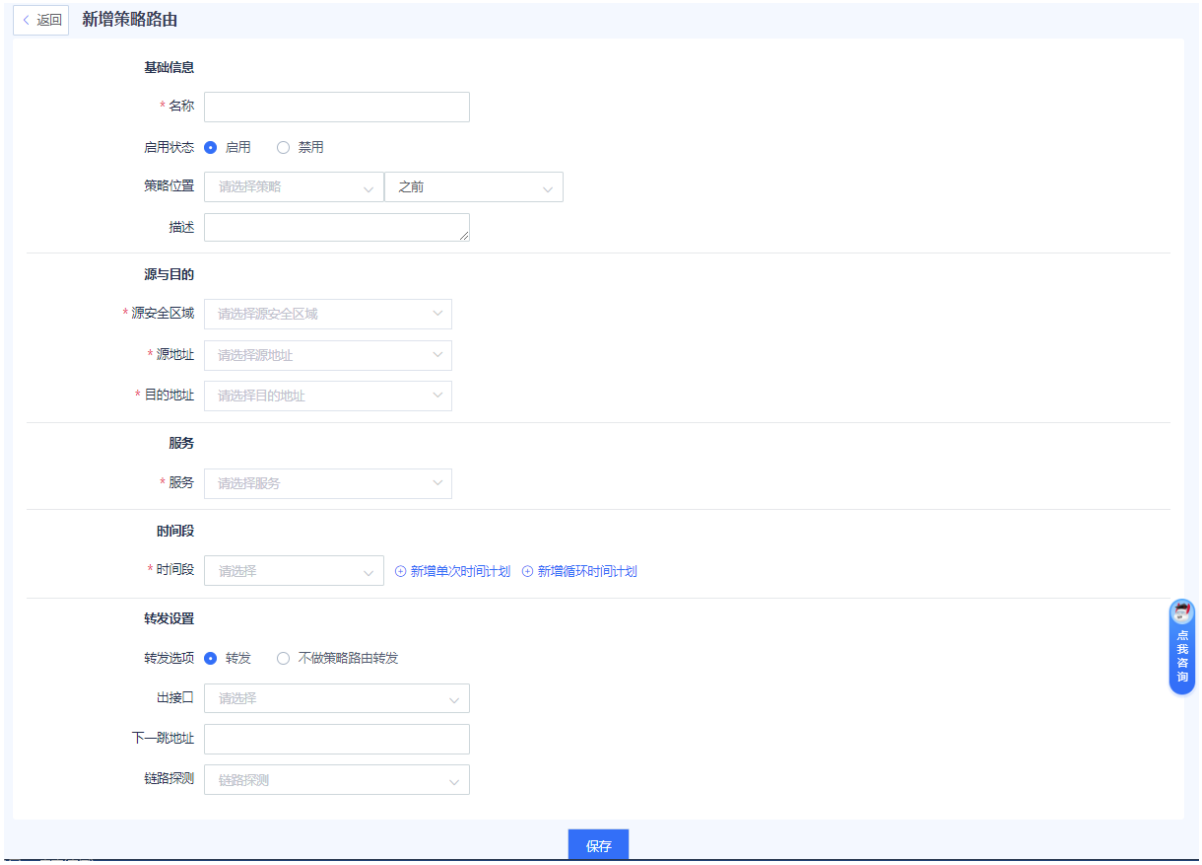
通过该操作，可以配置报文匹配条件及转发出接口、下一跳等。

【配置步骤】

(1) 点击[网络配置]>>[路由] >>[策略路由]菜单项，进入[新增策略路由]页面。

(2) 点击<新增>按钮。

(3) 设置策略路由相关配置项。



配置项	说明	配置方法
基础信息		
名称	策略路由的名称。	不能包含字符：`~!#%^&*+\/0::"/<>?和空格。 [示例] Policy_1
启用状态	是否启用新增的策略路由。	[示例] 启用

配置项	说明	配置方法
策略位置	将新增的策略路由移动到指定策略之前或之后。策略越靠前匹配优先级越高。	-
描述	安全策略的描述信息。	不能包含字符：`~!#%^&*+|{};:'"/<>?
源与目的		
源安全域	来自该源安全区域的报文按本策略进行转发。	● 点击下拉选项，在"待选"区域选择源安全域，自动添加到"已选"区域。 ● 点击<新增安全域>，自定义新增安全域。 [示例] trust
源地址	来自该源地址或地址组的报文按本策略进行转发。	点击下拉选项，在"待选"区域选择源地址，自动添加到"已选"区域。 [示例] Any
目的地址	发送到该目的地址或地址组的报文按本策略进行转发。	在"待选"区域选择目的地址，自动添加到"已选"区域。 [示例] Any
服务	属于该服务类型的报文按本策略进行转发。	[示例] Any
时间段	策略路由生效时间段。	[示例] Any
转发设置		
转发选项	设置命中本策略的报文是否按本策略转发。选择转发时，需要设置出接口和下一跳地址。	[示例] 转发
链路探测	选择出接口关联的链路探测策略，可以实时测试出接口到下一跳之间的网络连通性。当出接口到下一跳之间网络不通时，该条策略路由将会失效。	有关链路探测的详细介绍请参见7.6 链路探测。

(4) 点击<保存>。

7.3.4 查看路由表

【操作步骤】

(1) 点击[网络配置]>>[路由] >>[路由表]菜单项。

(2) 查看到当前防火墙设备存在的路由表项。

系统自动生成直连路由，优先级为0。

7.4 DNS 服务器

7.4.1 简介

TCP/IP提供了通过IP地址来连接到设备的功能，但对用户来讲，记住某台设备的IP地址是相当困难的，因此专门设计了一种字符串形式的主机命名机制，这些主机名与IP地址相对应。在IP地址与主机名之间需要有一种转换和查询机制，提供这种机制的系统就是域名系统DNS（Domain Name System）。

DNS（Domain Name System，域名系统），Internet上作为域名和IP地址相互映射的一个分布式数据库，能够使用户更方便地访问互联网，而不用去记住能够被机器直接读取的IP数串。通过主机名，最终得到该主机名对应的IP地址的过程叫做域名解析（或主机名解析）。

防火墙设备可以作为DNS Client，使用DNS协议从DNS Server动态获得域名对应的IP地址，便于用户通信。

当防火墙执行如下业务时，可作为DNS Client向DNS Server发送DNS请求报文:

- 以域名方式进行Ping或Tracert操作
- 以域名方式访问安全云平台进行特征库升级

7.4.2 创建 DNS 服务器

【应用场景】

通过Web界面配置DNS Server的IP地址，使设备可以作为DNS客户端，向DNS服务器发送域名解析请求。

【前置条件】

系统最多支持配置3个DNS服务器，DNS服务器1优先级最高，DNS服务器3优先级最低。系统优先使用优先级高的服务器。

【配置步骤】

(1) 点击[网络配置]>>[DNS]菜单项。

(2) 设置第一个DNS服务器的IP地址。

a 点击<新增>。

系统弹出"新增DNS"页面。

b 在“DNS服务器地址1”输入框中输入第一个DNS服务器的IP地址。

c 点击<保存>。

(3) （可选）如果网络环境中配置了多个DNS服务器，可以设置第二个或第三个DNS服务器的IP地址。

7.5 DHCP 管理

7.5.1 简介

DHCP（Dynamic Host Configuration Protocol，动态主机设置协议）是一个局域网的网络协议，使用UDP协议工作，被广泛用来动态分配可重用的网络资源，如IP地址。规模较小的网络，通过DHCP可以使后续增加网络设备变得简单快捷。

使用DHCP，可以带来以下受益：

- 降低客户端的配置和维护成本

DHCP易配置部署，对于非技术用户，DHCP能够将客户端与配置相关的操作降至最低，并能够降低远程部署和维护成本。

- 集中管理

DHCP服务器可以管理多个网段的配置信息，当某个网段的配置发生变化时，管理员只需要更新DHCP服务器上的相关配置即可。

Z-S系列防火墙可以作为DHCP服务器，为内网用户提供IP地址。

7.5.2 配置 DHCP 服务器

【应用场景】

系统默认开启DHCP服务器功能，可以将防火墙设备作为DHCP服务器，为内网用户提供IP地址。

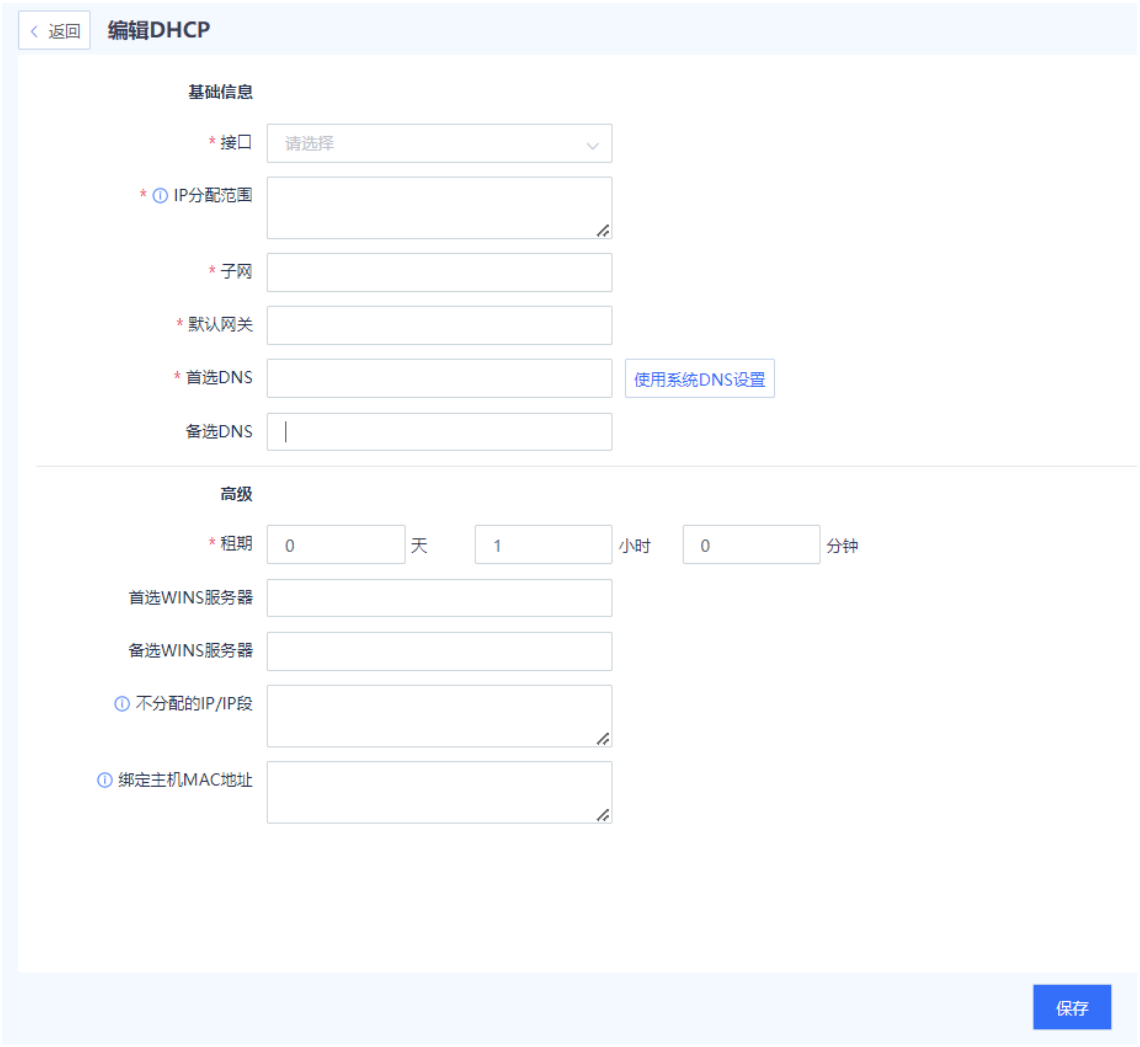
【配置步骤】

(1) 点击[网络配置]>>[DHCP]>>[DHCP]菜单项。

(2) 配置DHCP服务器信息。

a 点击<新增>。

系统弹出[编辑DHCP服务器]页面。



b 设置DHCP服务器相关配置项。

配置项	说明	配置方法
接口	对某个接口配置DHCP服务器功能。 开启DHCP功能后，该接口将能够下发IP地址。	[示例] Ge 0/1
IP分配范围	DHCP服务器分发的IP地址范围。	● 每行输入一个IP地址范围。 ● 中间使用-进行连接。 [示例] 192.168.1.1-192.168.1.10
子网	IP地址所在的子网。	输入网段/掩码位数。 [示例] 192.168.1.0/24
默认网关	为获取地址的终端提供上网的默认网关。	[示例] 255.255.255.0
首选DNS	DHCP服务首选使用的DNS服务器。	点击<使用系统DNS设置>自动填写系统DNS；也可以自行设置公用DNS服务器。 [示例] 192.168.10.1
备选DNS	DHCP服务备选使用的DNS服务器。	[示例] 192.168.30.1
租期	地址租约时间，终端设备在连接状态时一般会自动续租保持IP地址不变；若因终端设备断开连接或网络不稳定等情况，没有续租，过了租期时间，将收回IP地址。此时终端设备恢复连接将重新请求地址。	● 租期最短为3分钟，最长为365天。 ● 默认租期为1小时。 [示例] 1小时
不分配的IP/IP段	在配置的“IP分配范围”中，保留部分IP不分配。	[示例] 192.168.1.2
绑定主机MAC地址	通过静态地址绑定方式将“IP分配范围”中预分配的IP地址与客户端的MAC地址绑定。 当DHCP服务器收到该MAC地址的客户端的申请IP地址的请求时，则将与此客户端MAC绑定在一起的固定IP地址唯一地指定给该客户端。	● 填写格式为：IP地址/MAC地址。其中，IP地址为“IP分配范围”中预分配的IP。 ● 每行填写一组绑定信息。 [示例] 192.168.10.1/d8:9e:f3:3f:d5:64

c 点击<保存>。

【后续处理】

如果DHCP服务列表中，只剩一行，如果要删除该地址池，需要先关闭DHCP服务器再删除。

7.5.3 地址管理列表

【应用场景】

通过该操作，可以查看DHCP服务器已经分配的IP地址。

【操作步骤】

(1) 点击[网络配置]>>[DHCP] >>[地址管理列表]菜单项。

(2) 查看IP地址分配情况。

(3) 对IP地址进行相应处理。

- 选择地址并点击<IP/MAC绑定>或“操作”列的<绑定>，将IP固定地分配给对应MAC的主机。
- 选择地址并点击<解除绑定>，可以解除IP与MAC绑定关系。

7.6 链路探测

7.6.1 链路探测

【应用场景】

链路探测用于探测网络链路的连通性，与静态路由、策略路由进行联动可实现自动路由切换。当链路探测未被策略路由或静态路由关联时，即使探测结果为异常，该接口上的静态路由和默认路由也不会失效。

【操作步骤】

(1) 点击[网络配置]>>[链路探测]>>[链路探测]菜单项。

(2) 点击 开启链路探测功能。

说明

不开启总开关，仅开启单条探测策略中的探测开关时，探测策略不生效，不会进行探测。

(3) 点击<新增>按钮，进入[添加链路探测]页面，设置探测参数。

(4) 点击<保存>。

7.6.2 探测日志

【应用场景】

探测日志用于展示历史探测日志。

【操作步骤】

(1) 点击[网络配置]>>[链路探测]>>[探测日志]菜单项。

(2) 选择查询时间段，页面将会展示指定时段内的探测日志。

8 系统管理

8.1 管理员

8.1.1 简介

防火墙设备支持设置多种角色的管理员，实现权限分离、独立控制。

管理员权限控制

设备出厂时，系统默认提供超级管理员、安全管理员、审计员、用户管理员几类管理员角色。缺省角色的权限说明如表8-1所示。

表8-1 缺省角色权限说明

角色分类	权限说明	默认帐号
超级管理员	对于Web界面所有菜单项，都具有读写权限。	admin
安全管理员	● 无[系统管理]>>[管理员]菜单项权限。 ● 其余菜单项具有读写权限。	securityadmin
审计员	● [首页]菜单项，具有读权限。 ● [安全监控]菜单项，具有读权限。 ● 其余菜单项，无权限。	auditadmin
用户管理员	● [首页]菜单项，具有读权限。 ● [系统管理]>>[管理员]菜单项，具有读写权限。 ● 其余菜单项，无权限。	useradmin

8.1.2 启用默认账号

【应用场景】

对于系统默认的securityadmin、auditadmin、useradmin三个管理帐号，启用并设置密码后，该帐号才能生效。

说明

对于admin帐号，设备出厂即可用，无需执行以下操作。

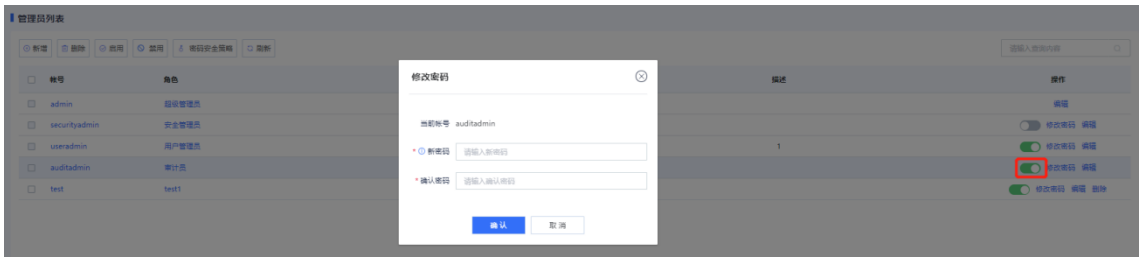
【操作步骤】

(1) 点击[系统管理]>>[管理员]菜单项。

系统显示默认的帐号。

(2) 选择待启用的默认帐号，将其设置为开启状态。

系统弹出[修改密码]对话框。



(3) 设置该账号的新密码并再次输入密码。

密码格式要求如下：

- 至少包含大写字母、小写字母、数字或特殊字符中的任意三种。
- 不能包含中文、空格和全角字符。
- 长度范围为8~15个字符。
- 不能与用户名或用户名的倒序相同。

(4) 点击<确认>。

【后续处理】

- 在管理员列表，点击<编辑>，可以将默认帐号和描述修改为更易于识别的信息。

- 不支持删除默认管理员帐号。

8.1.3 自定义创建管理员

当管理人员发生变动时，可以创建新的管理员账号并为其分配角色；也可以删除不再使用的管理员帐号，避免帐号泄露存在安全隐患。

表8-2 创建管理员步骤

操作步骤	说明
创建管理员角色	内置“超级管理员”角色，超级管理员拥有所有功能的操作权限，不支持修改内置“超级管理员”的权限。
创建管理员账号	内置“admin”的超级管理员账号，admin拥有所有功能的操作权限，不支持禁用内置admin账号与修改admin的角色。

2. （可选）创建管理员角色

【应用场景】

Web管理界面通过管理员角色来控制管理员的权限，即控制对应的角色可以操作哪些菜单项。

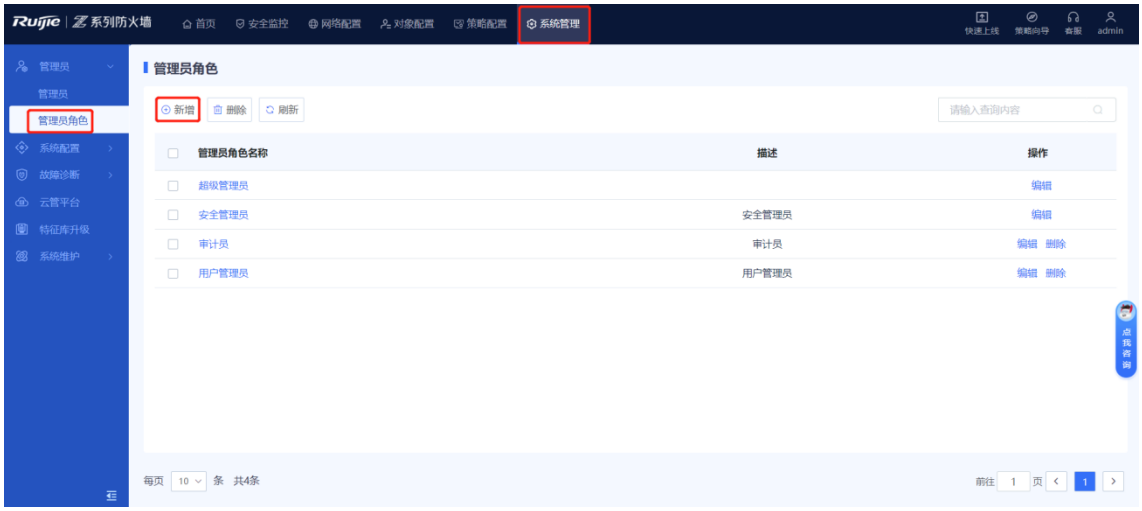
创建管理员时，可以直接把缺省的角色赋予管理员。系统也支持自定义角色，可以根据需要创建新的角色。

【操作步骤】

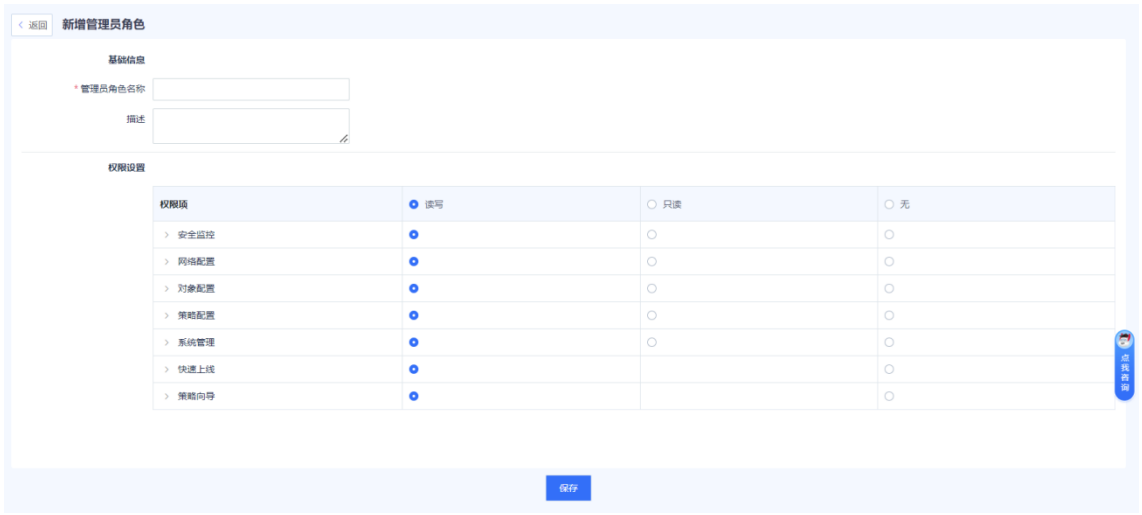
(1) 进入[新增管理员角色]页面。

a 点击[系统管理]>>[管理员角色]菜单项。

b 在操作区上方，点击<新增>。



(2) 设置新角色信息并配置权限。



配置项	说明	配置方法
管理员角色名称	新建管理员角色的名称。	[示例] 管理员角色1
描述信息	新建管理员角色的描述信息，用于区别不同的角色权限。	[示例] 新建
权限设置		
权限项	新建管理角色可操作的Web界面功能。	[示例] 安全监测
权限	新建管理角色对可操作功能的权限，包括： ● 读写：具有查看、新增、删除和编辑的权限。 ● 只读：只有查看的权限。 ● 无：没有任何权限。	[示例] 读写

(3) 点击<保存>，完成角色的创建。

【后续处理】

创建的角色将显示在列表中，可以编辑和删除已创建的角色。

- 编辑：当角色权限变更时，admin可以编辑角色描述和权限。
- 删除：当某个角色无需使用时，admin可以删除未关联管理员账号的角色。若需要删除的角色与管理员账号关联，admin可以使用<编辑>按钮，将关联管理员账号的角色更换为其他角色。

说明

不支持删除默认的管理角色：超级管理员、安全管理员、用户管理员和审计员。

3. 创建管理员账号

【应用场景】

当管理设备的人员增加时，可以创建新的管理员账号并为其分配对应的权限。

新管理员可以通过账号及密码访问Web平台，对设备执行配置、管理操作。

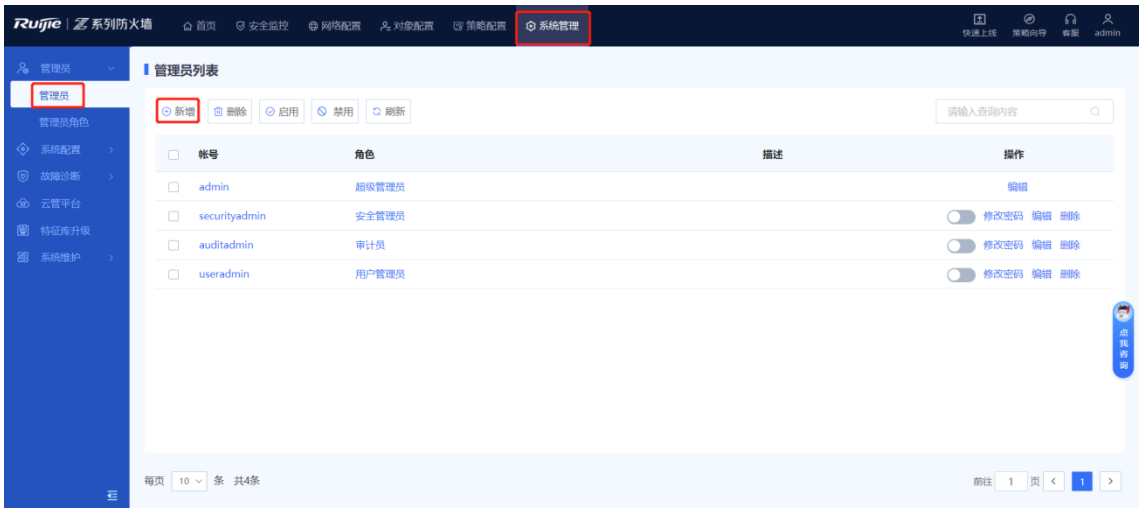
超级管理员和用户管理员均有权限创建管理员账号。

【操作步骤】

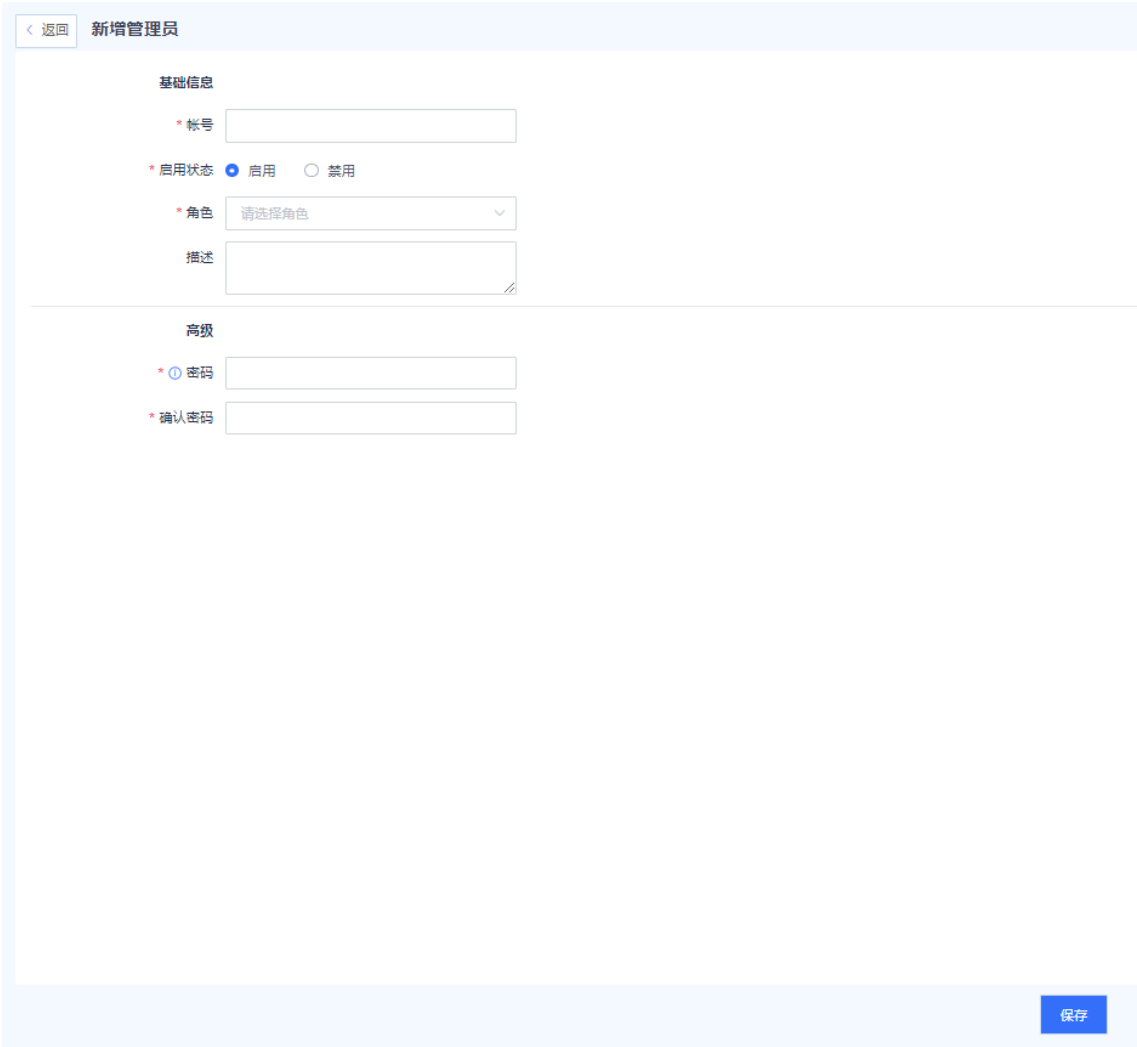
(1) 进入[新增管理员]页面。

a 点击[系统管理]>>[管理员]菜单项。

b 在操作区上方，点击<新增>。



(2) 设置新建管理员的相关配置信息。



配置项	说明	配置方法
基础信息		

配置项	说明	配置方法
帐号	新建管理员的用户名。	● 用户名可以包含字母、数字和下划线“_”，且必须以字母开头。 ● 不能与已有管理员用户名重复。 [示例] Admin_security
启用状态	是否启用该新建管理员帐号。	[示例] 启用
角色	新建管理员的角色，用于指定该管理员的操作权限。	[示例] 安全管理员
描述信息	新建管理员的描述信息。	支持输入任意字符。 [示例] 具有安全监管权限
高级		
密码	新建管理员登录Web管理界面的密码。	● 至少包含大写字母、小写字母、数字或特殊字符中的任意三种。 ● 不能包含中文、空格和全角字符。 ● 长度范围为8~15个字符。 ● 不能与用户名或用户名的倒序相同。 [示例] admin@123
确认密码	再次输入新建管理员登录Web管理界面的密码。	“确认密码”需要与“密码”保持一致。 [示例] admin@123

(3) 点击<保存>，完成管理员账号的创建。

【后续处理】

创建的管理员账号将显示在列表中，可以编辑、禁用、删除已创建的自定义管理员信息。

说明

不支持修改自定义管理员的帐号信息。

8.1.4 修改管理员密码安全策略

【应用场景】

为确保管理员密码安全性，需要定期修改账号密码。通过该操作，可以设置密码使用有效期。密码使用时间到期后，强制用户修改密码。

【操作步骤】

(1) 进入[密码安全策略]界面。

a 点击[系统管理]>>[管理员]菜单项。

b 在操作栏上方，点击<密码安全策略>。

(2) 开启“定期强制修改密码”开关。

(3) 设置“密码最长使用天数”。

(4) 点击<提交>。

【后续处理】

当密码使用时间超过系统限制时，系统会弹出提示强制修改管理员密码。

8.1.5 修改管理员密码

【应用场景】

当管理员密码安全性低或者存在密码泄露风险时，可以修改管理员的登录密码。

- 超级管理员可以修改其他管理员的登录密码。
- 用户管理员可以修改除超级管理员之外其他用户的登录密码。

【操作步骤】

(1) 进入[修改密码]界面。

a 点击[系统管理]>>[管理员]菜单项。

b 选择需要修改密码的管理员帐号，点击<修改密码>。

(2) 设置管理员帐号的新密码。

密码格式要求如下：

- 至少包含大写字母、小写字母、数字或特殊字符中的任意三种。
- 不能包含中文、空格和全角字符。
- 长度范围为8~15个字符。
- 不能与用户名或用户名的倒序相同。

(3) 点击<确认>。

8.2 系统配置

系统配置提供修改系统时间，修改服务参数以及授权导入的功能。

8.2.1 设置系统时间

【应用场景】

系统时间表示设备的当前时间，是设备运行过程中的重要参数。管理员通过查看设备的日志或告警中的时间信息，可以精确掌握系统事件发生的具体时间。另外，网络中的多台设备协同工作时，配置正确的系统时间也可以保证设备间协同工作的准确性和一致性。

为了便于管理，并保证与其它设备协调工作，设备需要准确的系统时间。

【背景信息】

系统时间设置包括手动设置与自动同步两种方式：

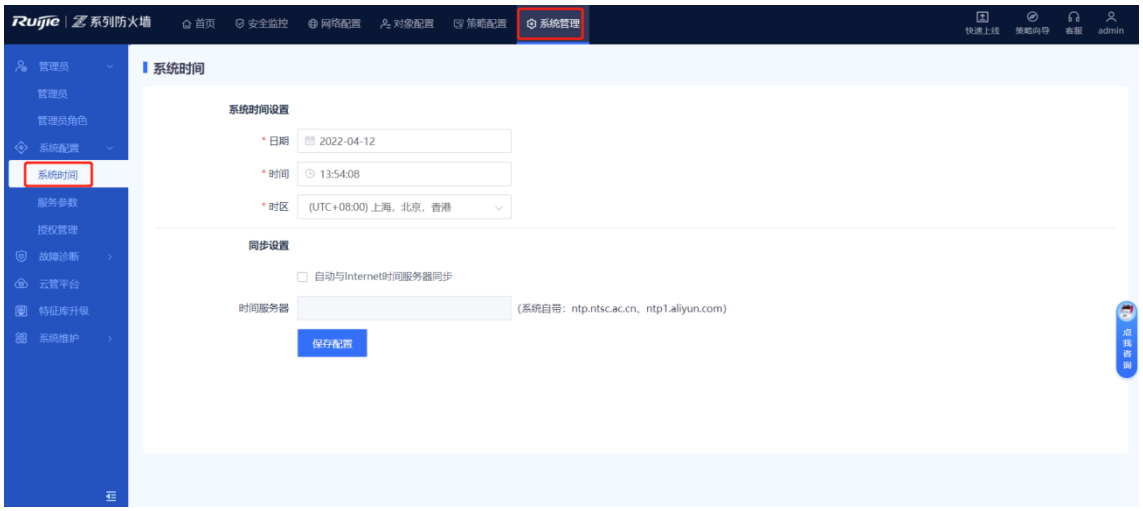
- 手动同步时间：管理员需要手动设置日期、时间和时区，此方式可能会存在时间误差。

- 自动同步时间：利用NTP时间服务器，自动同步时间。NTP（Network Time Protocol）是用于互联网中时钟同步的应用层协议，其用途是在分布式时间服务器和客户端之间进行时钟同步。对于运行NTP的本地系统，既可以接受来自其他时钟源的同步，也可以作为时钟源去同步别的时钟，并且可以通过交换NTP报文互相同步。

【操作步骤】

(1) 进入[系统时间]设置页面。

点击[系统管理]>>[系统配置]>>[系统时间]菜单项。



(2) 根据业务需要，选择不同的设置方式。

- 手动设置时间

在“系统时间设置”区域，设置日期、时间、时区。

- 自动同步设置

在“同步设置”区域，勾选“自动与Internet时间服务器同步”，并填写时间服务器的IP地址或域名。

说明

如果设置为使用时间服务器同步设置，需要确保DNS服务正常。

(3) 点击<保存配置>。

使用时间服务器同步设置成功后，系统将会在几分钟内同步时间。

8.2.2 设置服务参数

1. 修改 Web 平台配置

【应用场景】

为了提高登录安全性，管理员可以设置登录策略，例如当管理员输错登录密码次数超过设定值则锁定管理员账号，以提高登录安全性，降低因密码泄露而造成数据泄露的风险。

【操作步骤】

(1) 进入Web服务参数配置页面。

点击[系统管理]>>[系统配置]>>[服务参数]>>[Web]菜单项。

(2) 自定义Web服务配置。

配置项	说明	配置方法
设备名称	在睿易一体化配置场景中，在诺客云平台和Master设备上可查看修改后的设备名称。有关睿易一体化配置的详细介绍请参见4 睿易一体化开局配置。	[示例] Z5100-S
HTTPS端口	Web服务使用端口号。	默认为443。 [示例] 443
登录超时	管理员登录Web管理界面后，如果在指定的时间范围内无任何操作，再次登录Web管理界面时，系统会提示登录超时。	• 输入0~1440的整数，单位为分钟。 • 默认值为30分钟。 [示例] 30
登录错误允许次数	允许连续输入错误密码的次数。在输入密码出错次数超过已设置的“登录错误允许次数”时，系统自动锁定该用户。	• 输入1~10。 • 默认值为6次。 [示例] 3
锁定时间	用户被自动锁定后，在指定的“锁定时间”内无法登录Web管理界面。	• 输入1~30的整数，单位为分钟。 • 默认值为3分钟。 [示例] 30
验证码	登录Web管理界面时，是否需要输入验证码进行校验。	默认开启。 [示例] 开启

(3) 点击<保存配置>。

2. 修改 SSH 服务配置

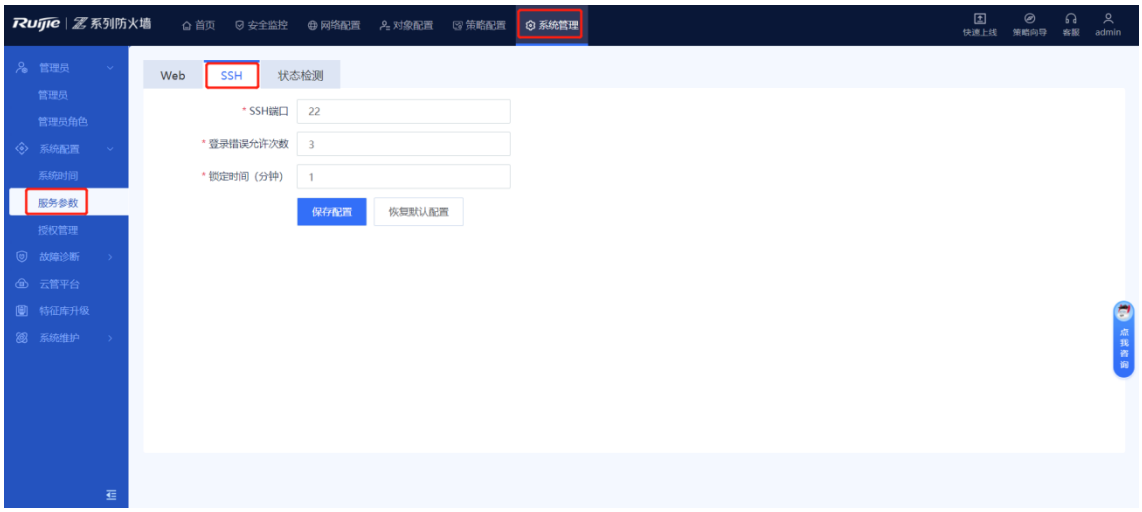
【应用场景】

通过该操作可以修改SSH服务相关配置，保证使用SSH登录设备的安全性。

【操作步骤】

(1) 系统进入SSH服务参数配置页面。

点击[系统管理]>>[系统配置]>>[服务参数]>>[SSH]菜单项。



(2) 修改SSH服务相关配置项。

配置项	说明	配置方法
SSH端口	SSH服务使用端口号。 为了提高安全性，避免默认的22端口号被攻击而泄漏服务器信息，可以修改SSH端口号。	默认为20。 [示例] 20
登录错误允许次数	通过SSH方式登录设备时，允许连续输入错误密码的次数。在输入密码出错次数超过已设置的“登录错误允许次数”时，系统自动锁定该用户。	● 输入1~5的整数。 ● 默认值为3。 [示例] 3
锁定时间	用户被自动锁定后，在指定的“锁定时间”内无法登录Web管理界面。	● 输入1~30的整数，单位为分钟。 ● 默认值为1分钟。 [示例] 1

(3) 点击<保存配置>。

8.3 激活授权

【应用场景】

用户购买设备后，可以使用设备的基本功能。当用户因业务拓展，需要使用增值特性或者扩容设备资源时，可以购买设备对应功能或资源的授权，以满足业务的需求。通过管理授权，可以有效降低用户的成本。用户根据实际需要导入授权，即可获得定制功能。

授权有两种激活方式，在线激活和手动激活。

- 在线激活：需要设备联网才能激活。
- 手动激活：无需设备联网，但是需要上传授权文件（支持zip和lic文件后缀）手动激活。

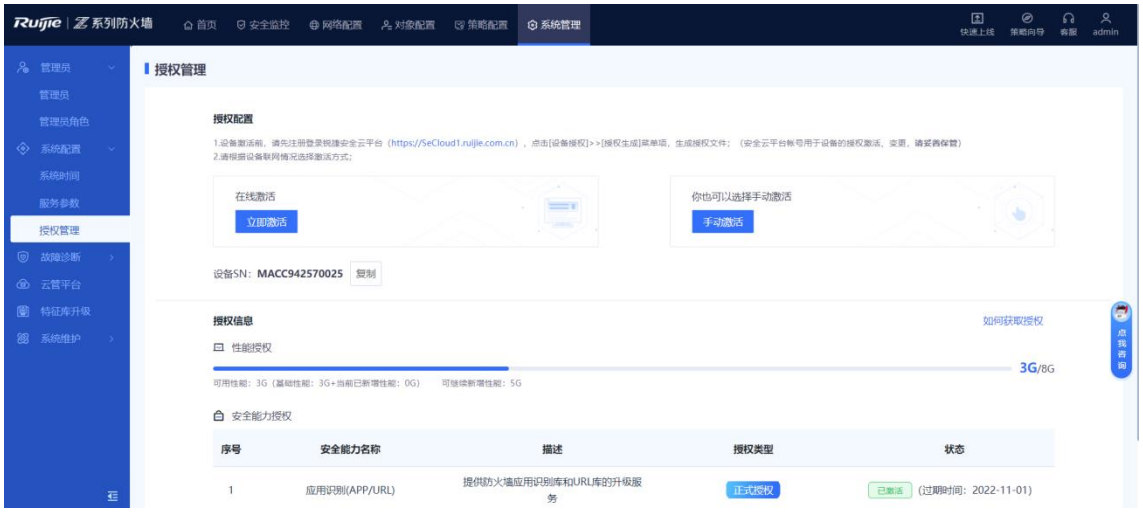
【前置条件】

请先注册登录锐捷安全云平台（https://SeCloud1.ruijie.com.cn），点击[设备授权]>>[授权生成]页面，生成授权文件。

【操作步骤】

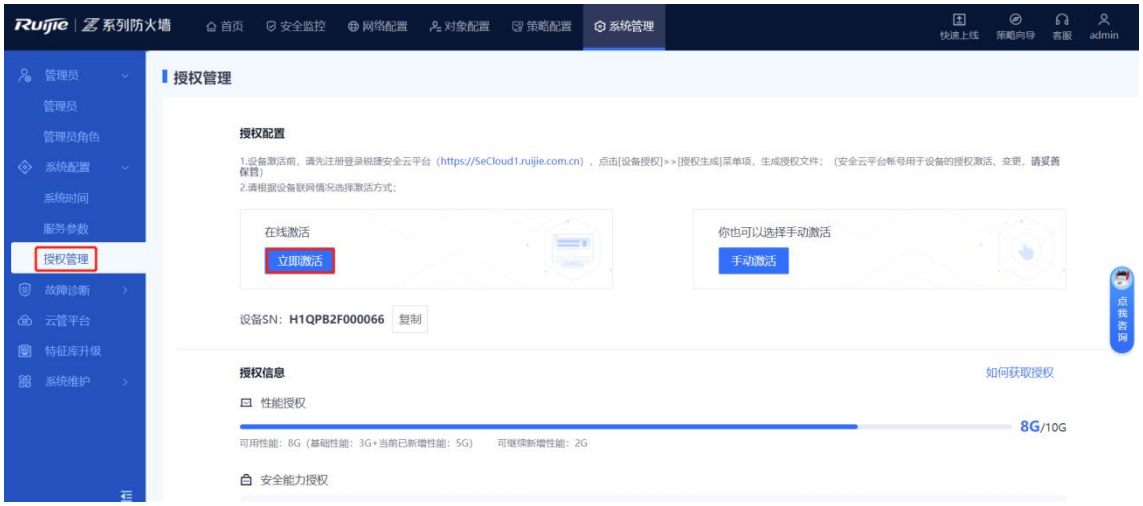
(1) 进入[授权管理]页面。

点击[系统管理]>>[授权管理]菜单项。



(2) 选择激活方式。

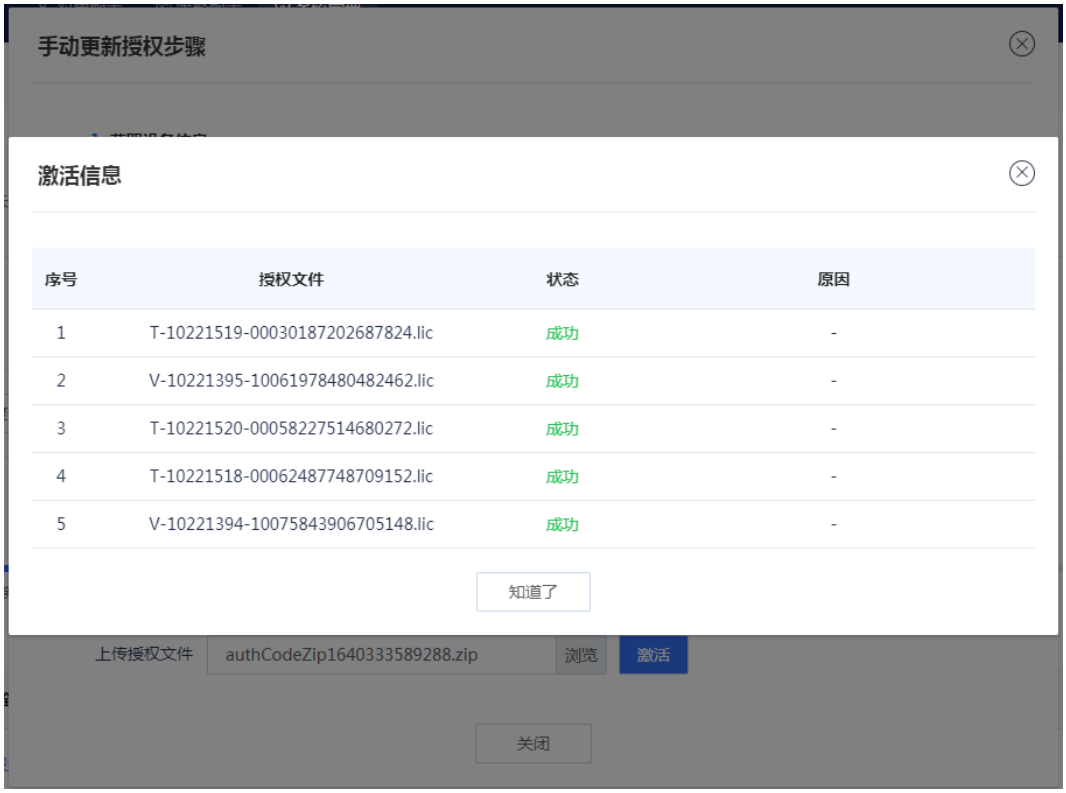
- 若选择在线激活，点击<立即激活>。



- 若选择手动激活，则点击<手动激活>，然后上传授权文件（支持zip和lic文件后缀），点击<激活>。

授权激活后，页面会显示授权的激活状态。

图8-1 成功激活授权



8.4 故障诊断

当出现设备与某个IP或者域名无法正常通信、设备出现故障或软件出现故障时，管理员可以使用故障诊断功能，排查故障和协助研发人员定位故障。

8.4.1 诊断中心

【应用场景】

诊断中心融合流量接收检测、基础配置（如安全策略、NAT策略等）检测、报文示踪、流量转发检测等功能，形成流程化排障思路，可一键定位网络问题，并生成易于理解、操作性强的诊断资料，实现高效率、低门槛的网络排障。

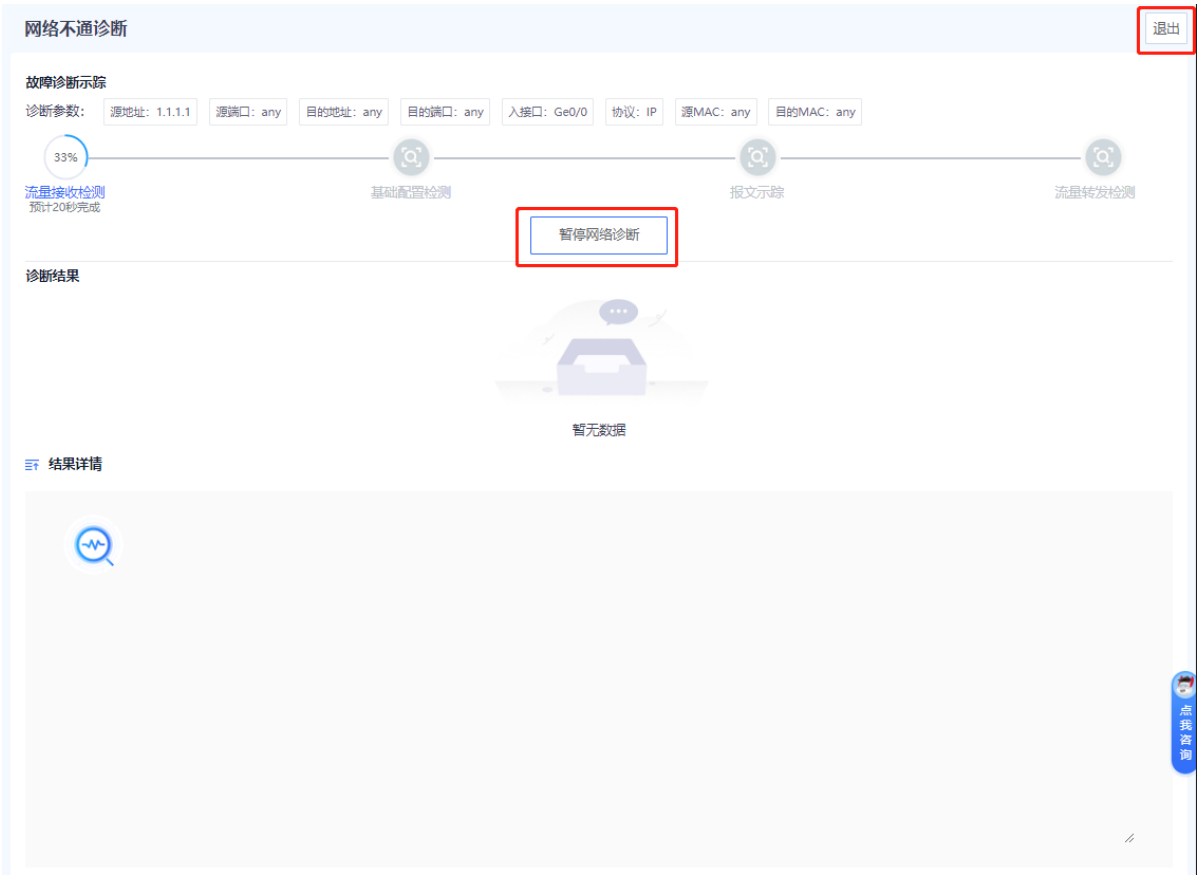
【操作步骤】

(1) 点击[系统管理]>>[故障诊断]>>[诊断中心]菜单项。

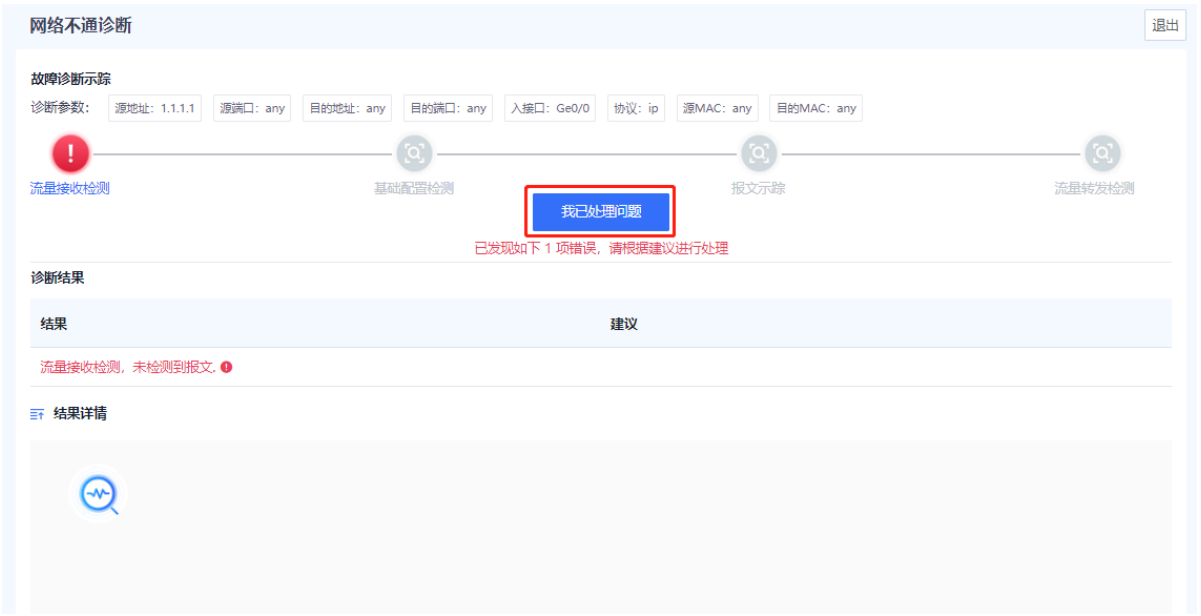
(2) 点击<进入诊断>。

(3) 输入源/目的IP地址、源/目的端口、源/目的MAC、入接口、协议等信息，点击<开始诊断>。设备将测试指定源IP到目的IP之间的网络连通性。

(4) （可选）检测过程中，您可以随时中断或退出本次诊断任务。



(5) 诊断完成后，页面下方将会展示诊断结果和诊断详情，用户根据诊断详情排除故障后，点击<我已处理问题>。



(6) 在弹出的提示框中点击<网络已通>，设备将继续下一项检测。

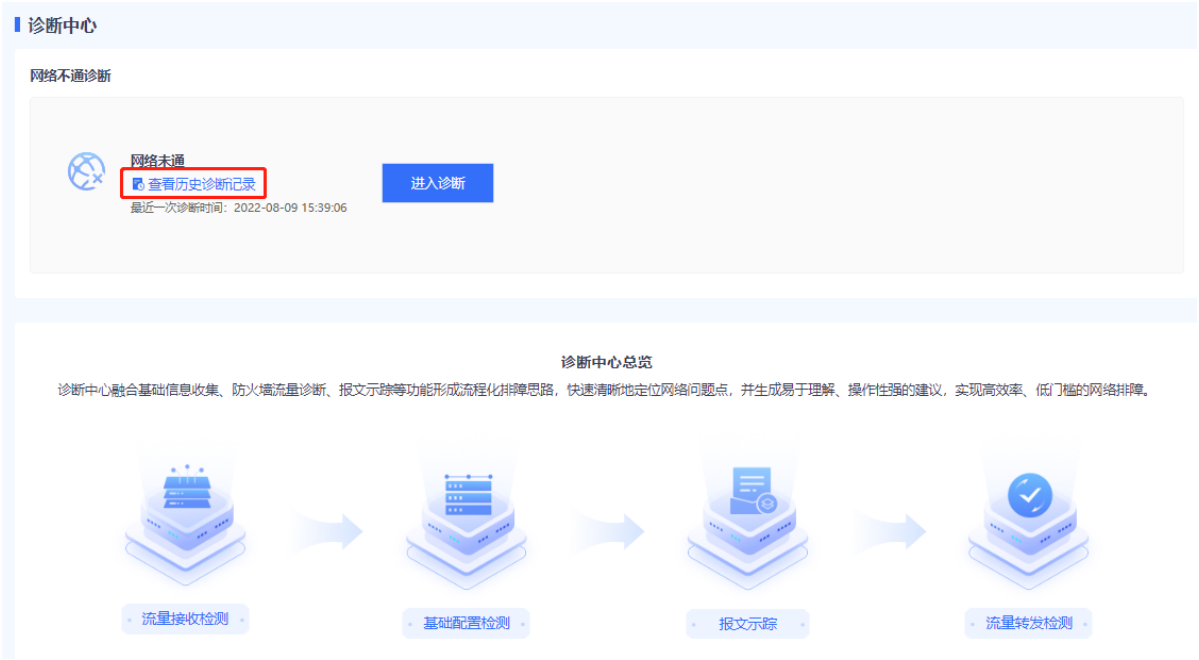
说明

若未进行故障排除，则点击<继续检测>，设备将重新检测。

(7) 重复步骤（5）和步骤（6），直到所有项目都检查完成即可。

【后续处理】

点击“查看历史诊断记录”可以查看并下载历史诊断资料。



8.4.2 设备自检

1. 设备自检

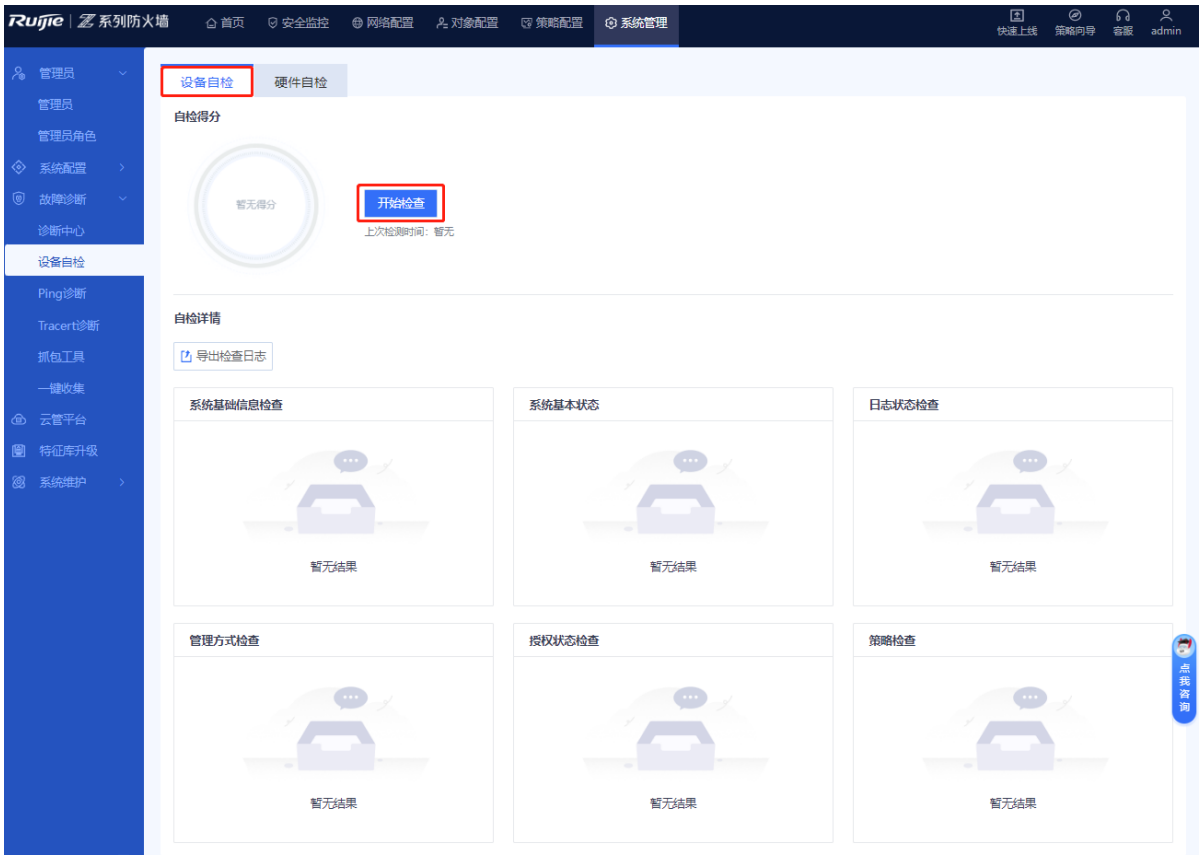
【应用场景】

设备自检功能可以检测设备版本、CPU/内存使用率及是否存在风险配置等信息。

【操作步骤】

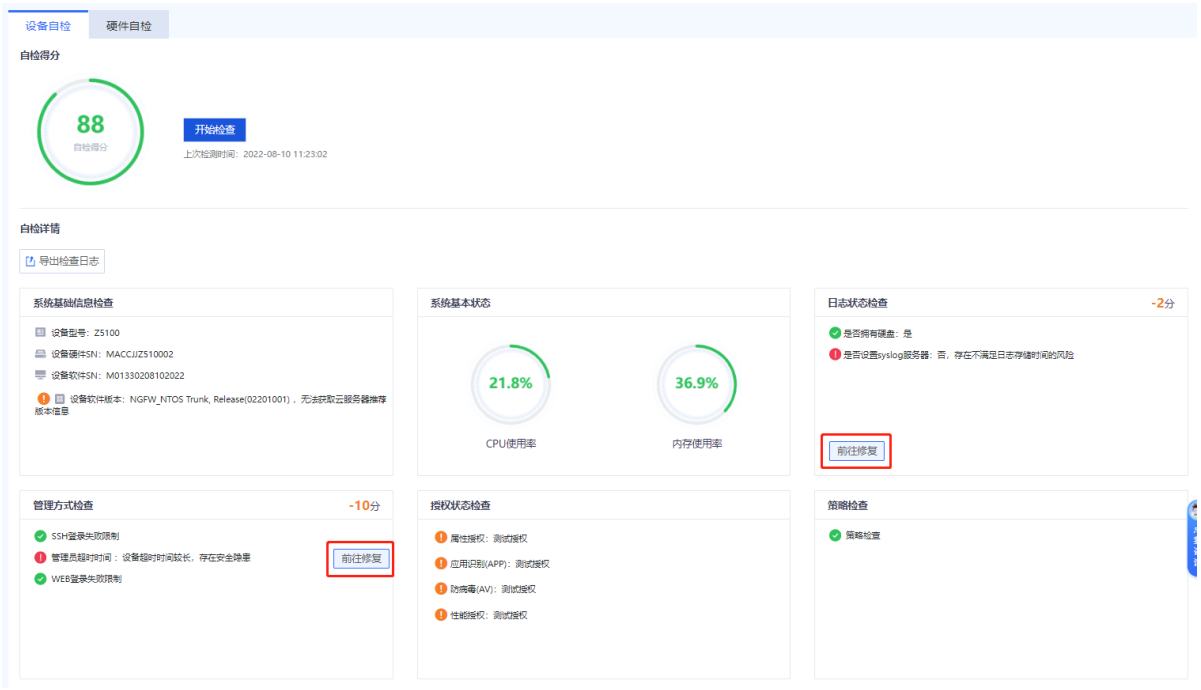
(1) 点击[系统管理]>>[故障诊断]>>[设备自检]>>[设备自检]菜单项，进入[设备自检]页面。

(2) 点击<开始检查>，设备将启动自检。



(3) 检查完成后，在弹出的提示框中点击<确定>。

(4) 对于异常的项目，点击<前往修复>可跳转到对应的配置页面进行配置。



2. 硬件自检

【应用场景】

硬件自检功能可以检测设备温度、风险、硬盘、电源、电压等硬件状态是否正常。

【注意事项】

RG-WALL 1600-Z5100支持硬件自检，RG-WALL 1600-Z3200不支持硬件自检。

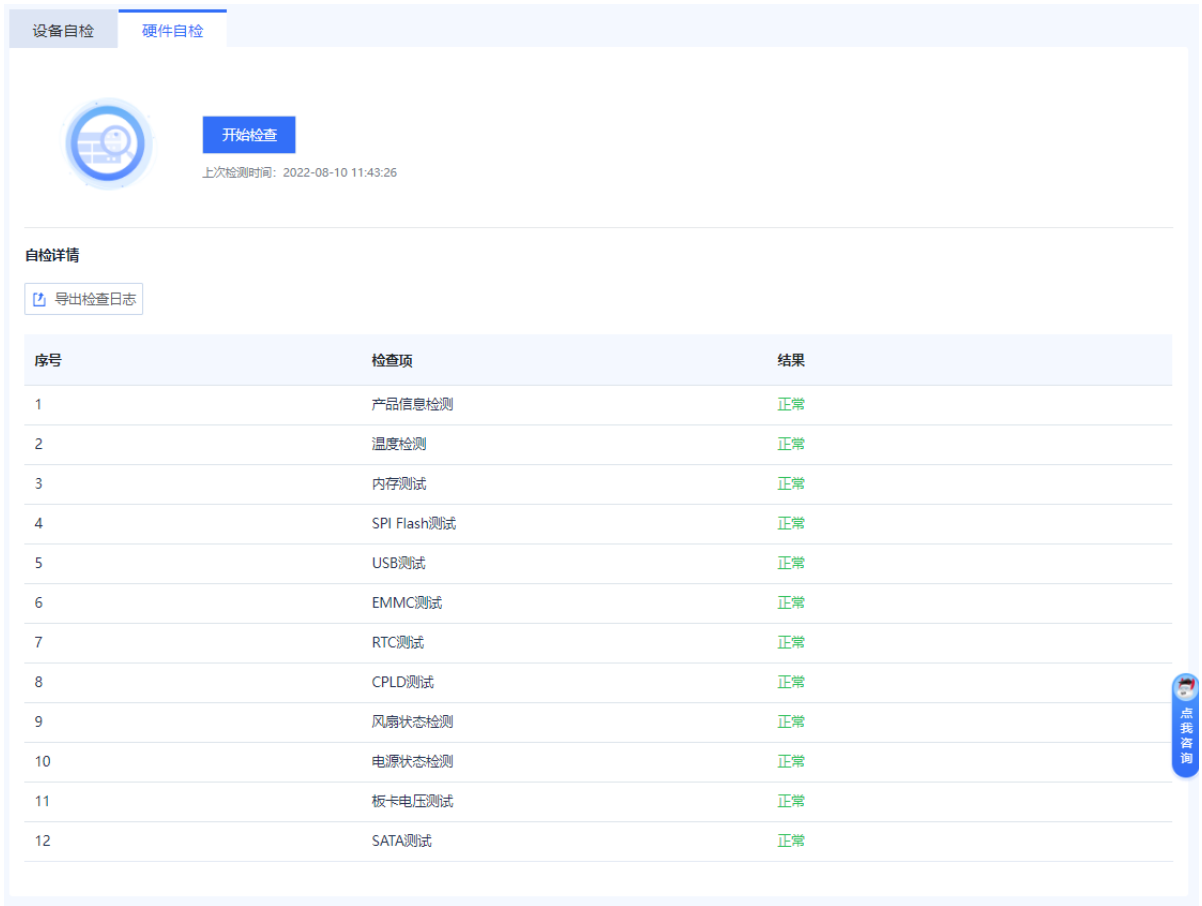
【操作步骤】

(1) 点击[系统管理]>>[故障诊断]>>[设备自检]>>[硬件自检]菜单项，进入[硬件自检]页面。

(2) 点击<开始检查>，设备将启动自检。

(3) 检查完成后，在弹出的提示框中点击<确定>。

(4) 若存在异常的项目，请及时检查并更换配件。



8.4.3 Ping 诊断

【应用场景】

通过Ping诊断功能可以检测设备与某个IP或者域名能否正常通信。

【操作步骤】

(1) 进入[Ping诊断]页面。

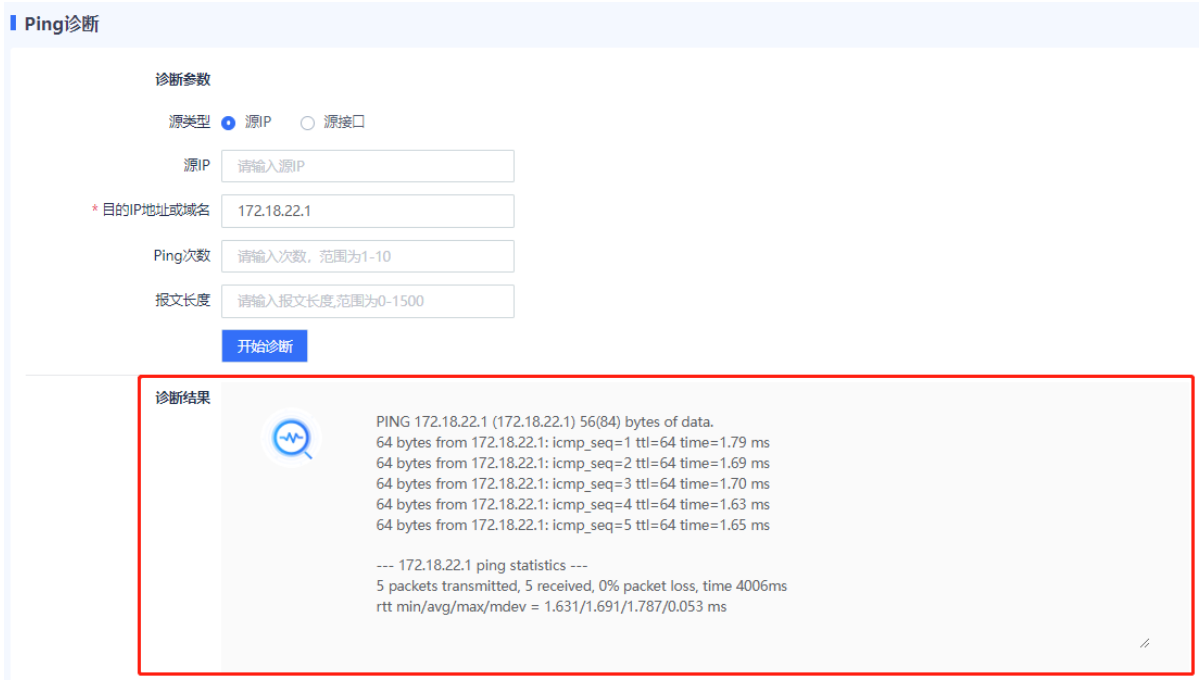
点击[系统管理]>>[故障诊断]>>[Ping诊断]菜单项。

(2) 填写诊断参数。例如：源IP，目的IP或域名等信息。

(3) 点击<开始诊断>。

【后续处理】

诊断结果将显示在页面下方。



8.4.4 Tracert 诊断

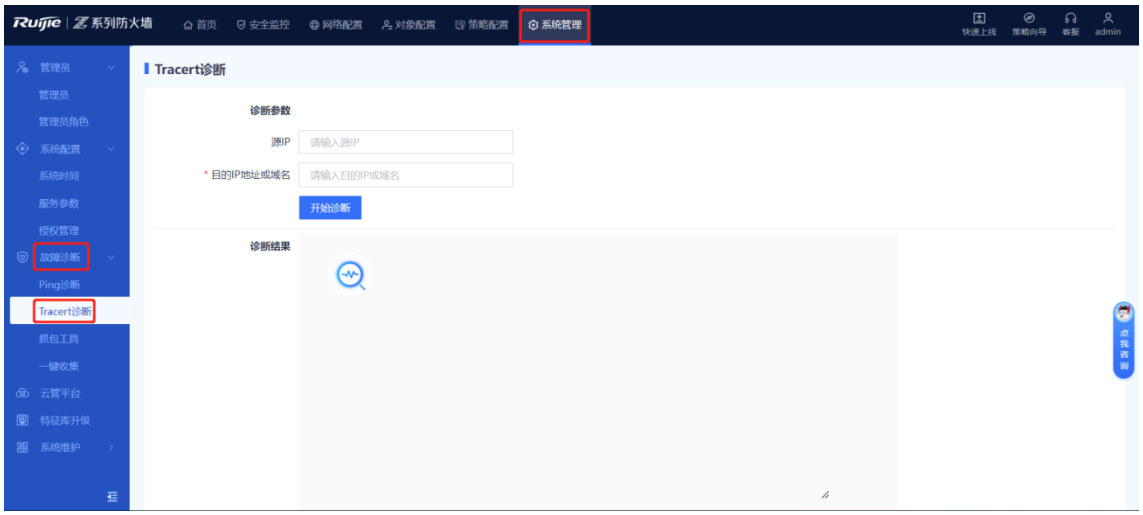
【应用场景】

通过使用Tracert诊断功能可以检测网络发生故障的位置。

【操作步骤】

(1) 进入[Tracert诊断]页面。

点击[系统管理]>>[故障诊断]>>[Tracert诊断]菜单项。



(2) 填写诊断参数，包括源IP，目的IP地址或域名。

(3) 点击<开始诊断>。

【后续处理】

诊断结果将显示在页面下方。

8.4.5 使用抓包工具

【应用场景】

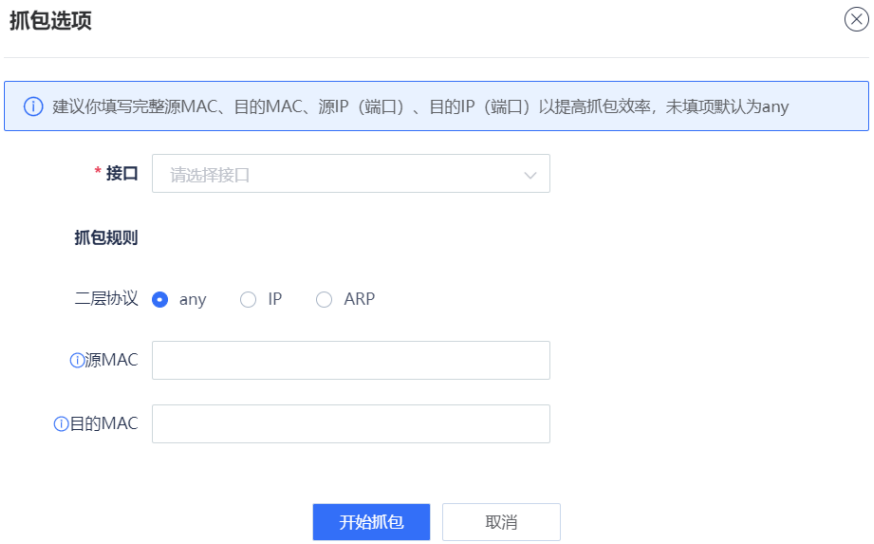
当软件出现故障时，管理员可以使用抓包工具帮助研发人员定位故障。抓包工具用于抓取网络数据包并保存到文件中，开发人员通过对抓获的数据包进行分析，可以较快地定位出软件故障。

【操作步骤】

(1) 进入[抓包工具]菜单项。

点击[系统管理]>>[故障诊断]>>[抓包工具]菜单项。

(2) 点击<开始抓包>，选择要抓包的接口，并填写抓包规则。



(3) 点击<开始抓包>，当前可以根据协议类型、IP地址、端口号和MAC地址进行过滤。

【后续处理】

- 生成抓包文件后，点击<查看>可在线查看、分析抓包文件。
- 生成抓包文件后，可以点击<下载>将对应的抓包文件下载到PC上，使用工具对抓包文件进行分析。
- 若抓包文件不再使用，管理员可以点击<删除>按钮，释放设备端的存储空间，支持批量删除。

8.4.6 一键收集故障信息

【应用场景】

当设备出现故障，可以通过一键收集把设备端的故障信息收集起来，供故障定位人员分析。

【操作步骤】

(1) 进入[一键收集]页面。

点击[系统管理]>>[故障诊断]>>[一键收集]菜单项。

(2) 点击<一键收集>，等待3~5分钟时间即可完成信息收集。

(3) 收集完成后，点击<下载>将收集到的故障信息下载到PC端，进行故障分析。

8.5 特征库升级

【应用场景】

通过定期升级特征库，可以持续为防火墙提供最新应用程序、威胁等特征，以便防火墙使用这些最新特征去保护网络，防止网络遭遇新型攻击。因此建议定期升级特征库，特征库升级后就可以在安全策略中生效，无需进行软件升级或更改防火墙的配置。特征库升级分为在线升级和本地升级。

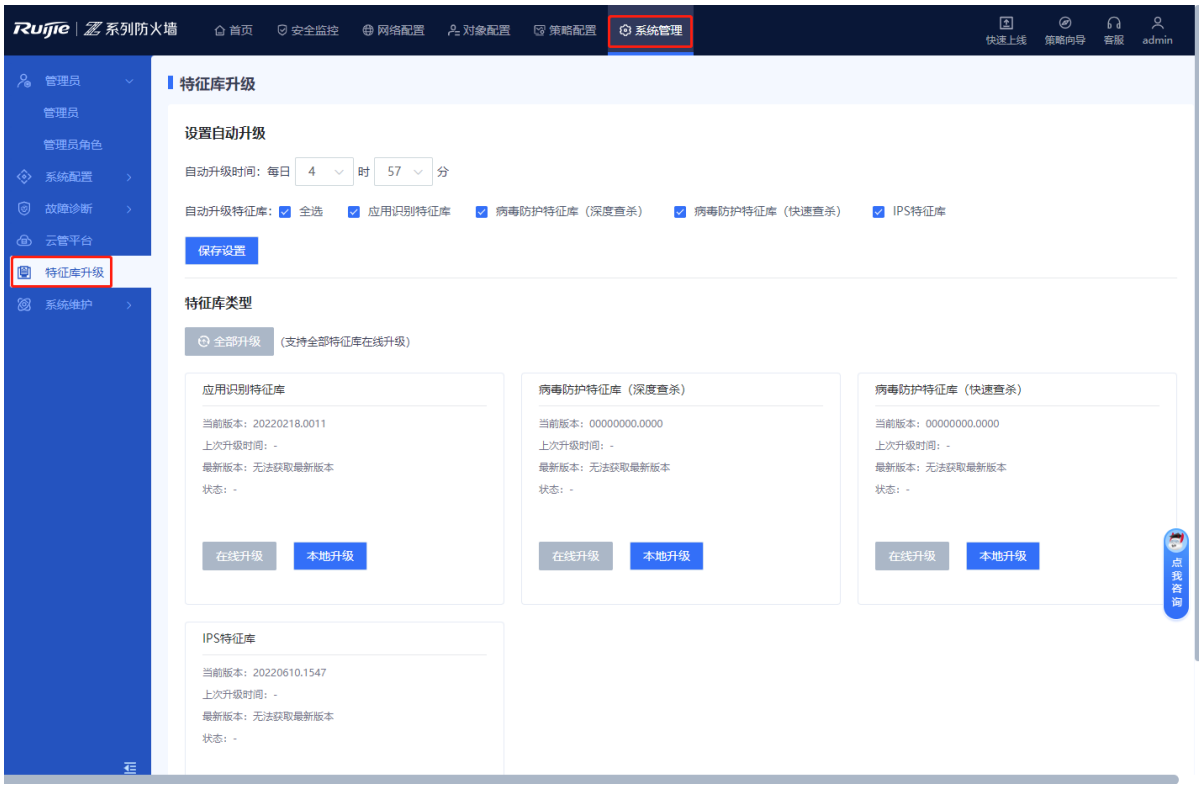
【前置条件】

- 特征库在线升级需要依赖设备信息包括软件版本号、设备序列号、设备产品类型、特征库版本等，通过设备信息在云服务平台获取更新的特征库版本。
- 所有的特征库版本需要通过云平台发布才是有效、合法的版本。云平台通过联动订单出货系统，录入所有设备出厂序列号。

【操作步骤】

(1) 进入[特征库升级]页面。

点击[系统管理]>>[特征库升级]菜单项。



系统显示当前特征库的相关信息：

- 上次升级时间：用户可以通过Web界面清晰地知晓，该特征库升级时间距离当前有多长时间。
- 最新版本：用户可以直观地了解最新的版本信息和功能，从而引导用户升级特征库。

(2) 根据需要，选择对应的特征库升级方式：

- 定时自动升级

  系统根据设置的时间计划，系统自动从云端下载、升级最新版本的特征库。

  a 设置自动升级时间。

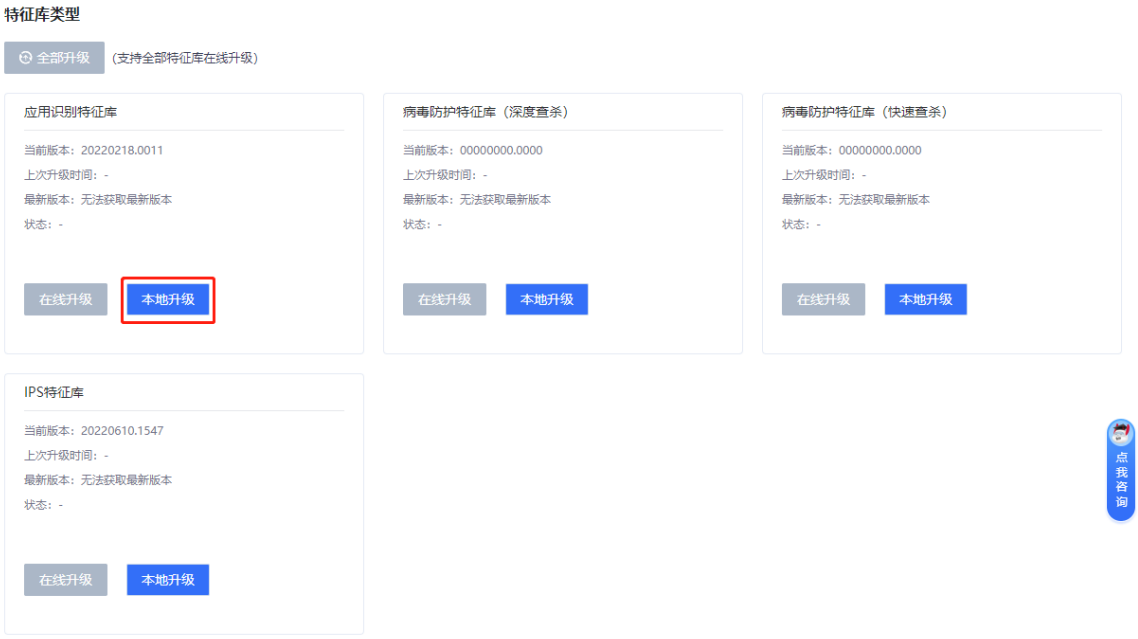
    建议将自动升级时间设置在业务不繁忙的时间段。

  b 选择需要升级的特征库类型。

  c 点击<保存设置>。

- 本地升级

  d 在需要升级的特征库区域，点击<本地升级>。



e （可选）如果未提前获取升级文件，可以点击“下载地址”链接，下载升级文件。

f 点击<浏览>，导入升级文件。

g 点击<开始升级>。

- 在线升级

当设备网络连接正常，且与版本服务器能够正常互通，如果系统自动监测到有最新的特征库版本需要升级，则可以点击<在线升级>一键式触发升级。

说明

当需要同时升级应用识别特征库和IPS特征库时，可以点击<全部升级>。

8.6 系统维护

8.6.1 查看设备信息

【应用场景】

通过该操作，可以查看防火墙设备的基本信息，包括：设备型号、设备信息等。

【操作步骤】

(1) 点击[系统管理]>>[系统维护]>>[设备信息]菜单项。

(2) 查看设备详细信息。

8.6.2 配置备份管理

1. 备份配置文件

【应用场景】

管理员使用配置备份功能可以手动备份当前配置或导出当前系统的配置文件，以便后续恢复或用于批量配置。

【操作步骤】

(1) 点击[系统管理]>>[系统维护]>>[配置备份]菜单项。

(2) 选择以下两种备份方式：

- 点击<导出当前配置>下载配置文件。

- 点击<手动备份配置>将当前配置文件保存到防火墙设备。

2. 恢复配置

【应用场景】

以下场景可以导入备份的配置文件，实现快速恢复及快速部署。

- 当设备故障恢复后，可以导入之前备份的配置文件，以便快速恢复配置。
- 新设备部署时，如果网络环境相同，则可以导入其他设备的配置文件，实现快速部署。

【操作步骤】

(1) 点击[系统管理]>>[系统维护]>>[配置备份]菜单项。

(2) 在“恢复配置”区域，可以选择从设备的备份文件中恢复，或点击<浏览>，选择已备份的配置文件进行恢复。

(3) 点击<导入配置>，将备份配置导入到当前设备。

8.6.3 系统升级

系统升级用于更新设备的软件版本，以获取最新的设备功能。

系统支持在线升级和本地升级。

1. 在线升级

【应用场景】

网络通信正常，且系统提示推荐版本时，可使用在线升级方式进行升级。

【前置条件】

设备升级前，请先确认升级版本。

【操作步骤】

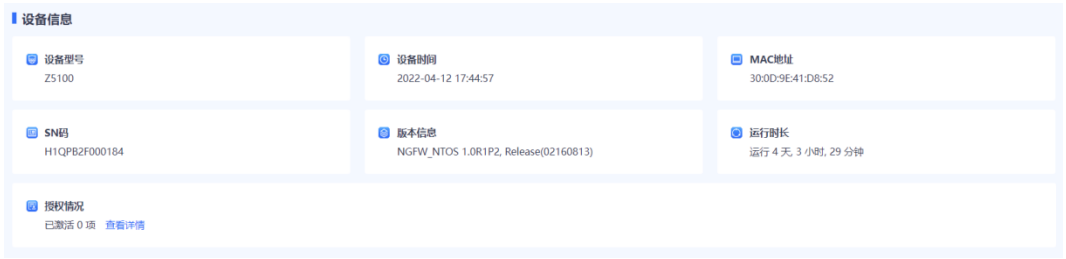
(1) 点击[系统管理]>>[系统维护]>>[系统升级]菜单项。

(2) 在"在线升级"区域，点击<立即升级>。

(3) 阅读提示信息，点击<确认>进行再次确认。

【后续处理】

点击[系统管理]>>[系统维护]>>[设备信息]菜单项，查看软件版本等信息，确认升级是否成功。



2. 离线升级

【应用场景】

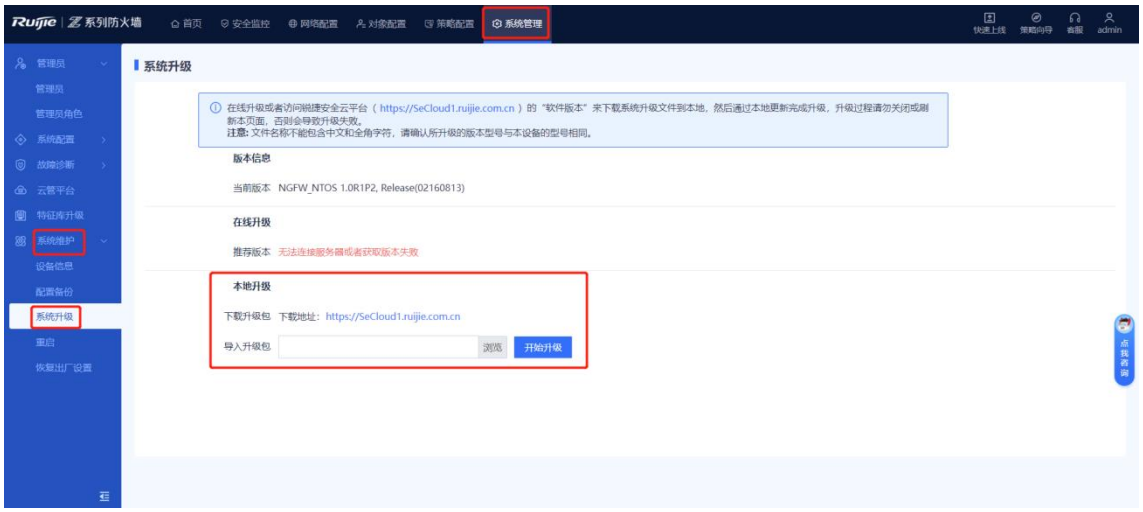
当网络异常，系统无法自动获取到最新版本；或执行升级回退时，可以使用离线升级方式进行升级。

【前置条件】

已提前获取升级文件。获取方法：访问锐捷安全云平台（https://secloud1.ruijie.com.cn/app/ops/no-login/home/userVersionUpdate ），在[版本升级] >> [升级包信息]页面可下载最新的补丁升级文件到本地。

【操作步骤】

(1) 点击[系统管理]>>[系统维护]>>[系统升级]菜单项。



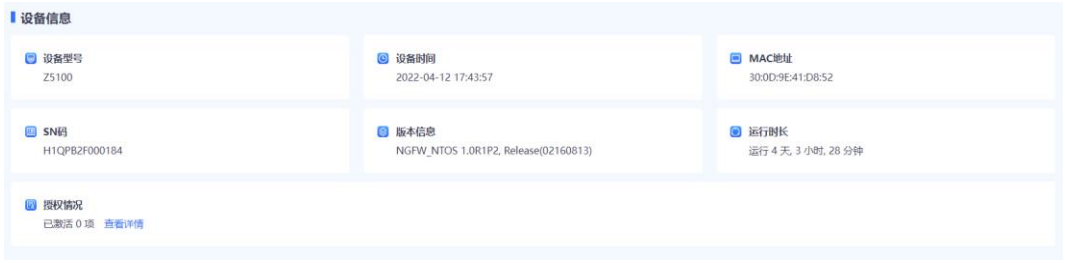
(2) 在“本地升级”区域，点击<浏览>，选择升级包文件。

(3) 点击<开始升级>，启动系统升级。

当升级成功时，根据提示，可选择立即重启生效，或者下次重启生效。

【后续处理】

点击[系统管理]>>[系统维护]>>[设备信息]菜单项，查看软件版本等信息，确认升级是否成功。



8.6.4 补丁升级

补丁升级用于修复设备运行过程中发生的故障。当系统存在未升级补丁时，首页会有弹窗告警；当需要安装的补丁包超过20个时，建议升级软件版本。

系统支持在线升级和本地升级。

1. 在线升级

【应用场景】

设备与锐捷云平台之间网络通信正常时，可使用在线升级方式进行升级。

【前置条件】

设备升级前，请先确认升级版本。

【操作步骤】

(1) 点击[系统管理]>>[系统维护]>>[补丁升级]菜单项。

(2) 在"在线升级"区域，打开自动升级开关，并设置不定信息同步时间，设备将在指定时间同步并升级补版本。

(3) 升级成功后，可以在页面下方查看信息的补丁升级记录。

2. 离线升级

【应用场景】

当设备与锐捷云平台之间网络异常，无法自动获取到最新版本时，可以使用离线升级方式进行升级。

【前置条件】

已提前获取升级文件。获取方法：访问锐捷安全云平台（ https://secloud1.ruijie.com.cn/app/ops/no-login/home/userVersionUpdate ），在[版本升级] >> [补丁包信息]页面可下载最新的补丁升级文件到本地。

【操作步骤】

(1) 点击[系统管理]>>[系统维护]>>[补丁升级]菜单项。

(2) 在“本地升级”区域，点击<浏览>，选择升级包文件。

(3) 点击<升级>，启动系统升级。

热补丁升级成功后不需要重启设备，冷补丁升级成功后需要重启设备。实际操作时，请根据提示选择是否重启。

8.6.5 重启设备

【应用场景】

当防火墙设备出现故障，无法恢复时，可以使用本功能重启设备。

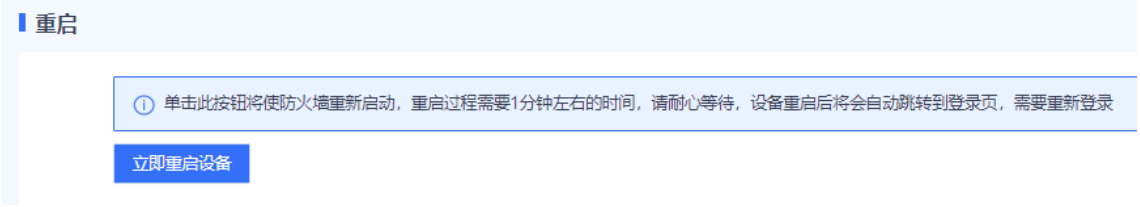
【前置条件】

- 防火墙设备工作不正常时，尽量排除故障，不要轻易重启系统，以免对业务造成影响。
- 如必须重启系统，非紧急情况请在对业务影响最小的时间（比如凌晨）进行。
- 重启会造成临时数据的丢失，重启前请确认配置文件已保存。

【操作步骤】

(1) 点击[系统管理]>>[系统维护]>>[重启]菜单项。

(2) 点击<立即重启设备>，确定后设备将立即重启。



8.6.6 恢复出厂设置

【应用场景】

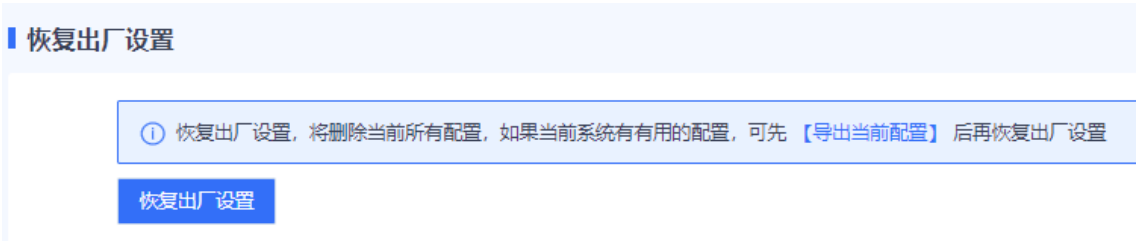
当需要删除设备的所有配置或重置超级管理员默认密码时，可进行恢复出厂操作。

> 注意
> 恢复出厂配置将清除所有的配置信息。在执行该操作前请及时备份配置信息。

【操作步骤】

(1) 点击[系统管理]>>[系统维护]>>[恢复出厂设置]菜单项。

(2) 点击<恢复出厂设置>。



【后续处理】

设备将会自动重启。重启完，设备的所有配置恢复为出厂设置。

- 管理口的IP地址恢复为192.168.1.200。
- 管理员用户和密码恢复为admin/firewall。

9 安全监控管理

9.1 安全驾驶舱

【应用场景】

安全驾驶舱功能即防火墙攻击统计功能，可以有效地帮助管理员发现最常发生的威胁类型、经常进行非法网络活动的攻击者以及经常遭受攻击的受害者等，从而制定相应的安全防护措施。

针对于检测到的攻击、事件类型、风险程度以及系统对攻击所执行的操作，防火墙在采集这些信息的基础上给出了攻击趋势、攻击类型Top 5等分布图以及攻击趋势图。

【操作步骤】

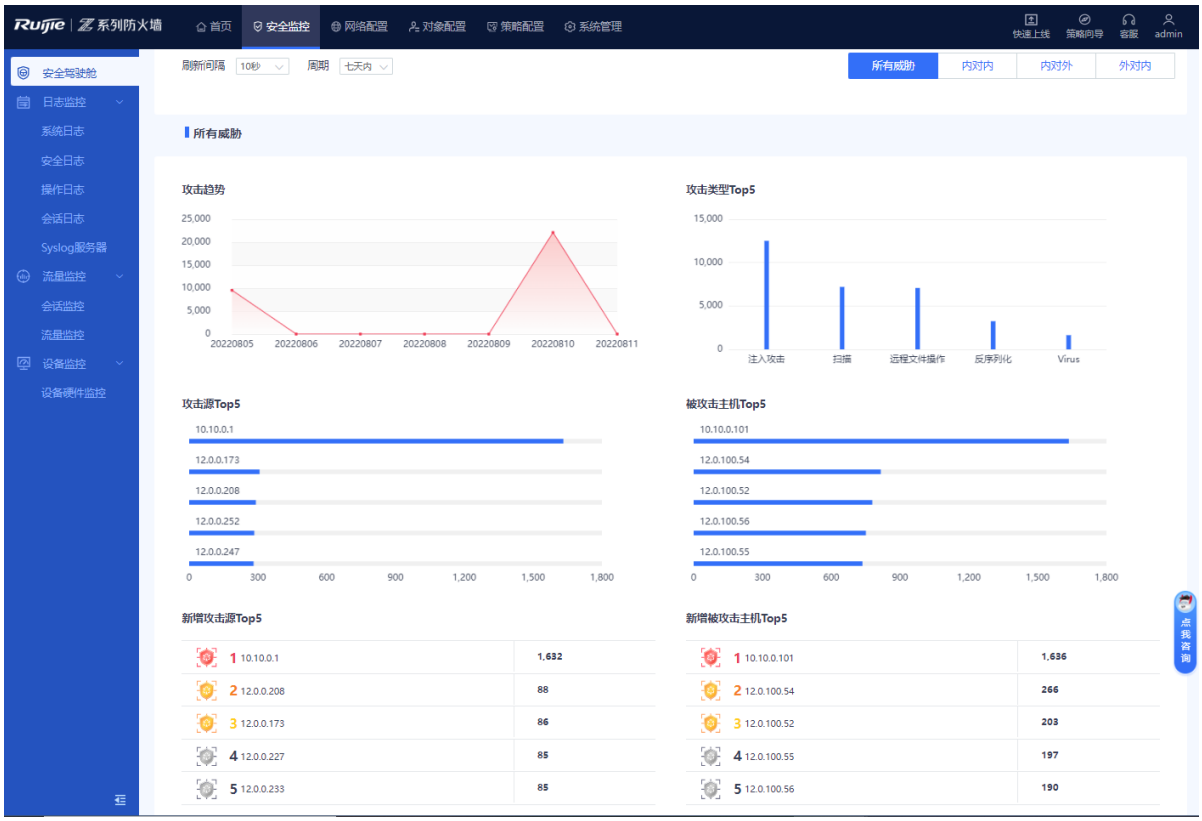
(1) 点击[安全监控]>>[安全驾驶舱]菜单项。

(2) 设置刷新时间、显示周期，并选择攻击类型。

攻击类型包括如下几类：

- 所有威胁
- 内对内
- 内对外
- 外对内

(3) 系统显示对应攻击类型的攻击趋势、攻击类型Top 5、攻击源Top 5等分布图。



9.2 日志监控管理

9.2.1 了解日志

日志信息是设备记录的对报文处理的相关信息。网络管理员利用这些信息即可以有效监控网络运行情况和诊断网络故障；也可以实时跟踪、记录、分析用户访问网络的情况，审计用户的上网行为。设备支持输出日志的方式包括：系统日志、安全日志、操作日志，并且可以通过Syslog协议将日志文件备份到第三方服务器上。

【日志格式】

【日志存储】

9.2.2 查询日志

1. 查询系统日志

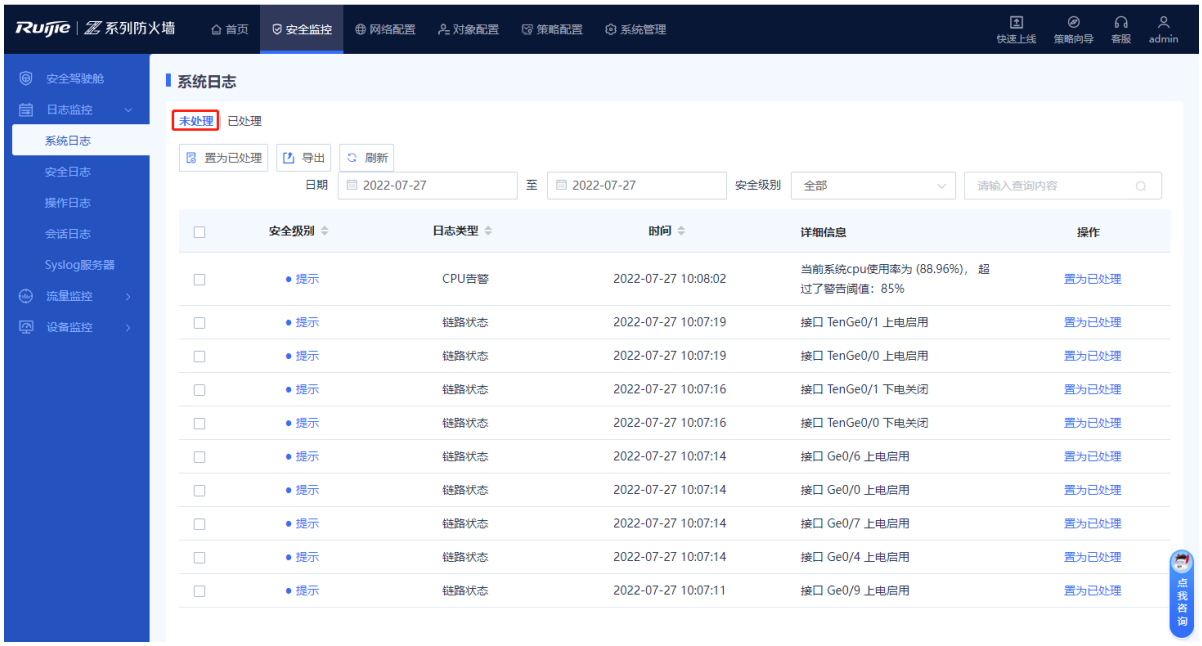
【应用场景】

通过查看系统日志，管理员可以查看系统运行过程中所产生的运行日志以及硬件环境的相关日志记录，了解设备是否一直正常运行，在发生问题时可以用于故障的定位和分析。

【操作步骤】

(1) 点击[安全监控]>>[日志监控]>>[系统日志]>>[未处理]菜单项。

(2) Web界面展示系统日志相关信息。



字段	说明
安全级别	系统日志的安全级别。
日志类型	系统日志的类型。
时间	系统日志产生的时间。
详细信息	系统该日志的详细信息。
操作	点击“置为已处理”可以将该条日志标记为已处理，切换到[已处理]页签，可查看已处理的日志信息。

说明

通过设置安全级别、日志、其他关键字进行模糊查询，界面只显示匹配的系统日志。

【后续处理】

- 勾选多条日志，点击<置为已处理>可以批量修改日志状态为已处理。
- 点击<导出>，可以将系统日志导出为Excel格式保存在本地，以方便后续阅读查询。
- 点击<刷新>，获取最新的系统日志。

2. 查询安全日志

【应用场景】

通过查看安全日志，管理员可以获知网络中的攻击流量，了解当前网络的带宽占用以及安全策略和带宽策略配置的生效情况。

【操作步骤】

(1) 点击[安全监控]>>[日志监控]>>[安全日志]菜单项。

(2) Web界面展示安全日志相关信息。

字段	说明
严重性	安全日志标识的问题严重程度。
安全事件	日志记录的安全事件描述。
日志类型	日志记录的安全事件类型。 [示例] IPS攻击
攻击类型	日志记录的攻击类型。 [示例] Heap Overflow
时间	安全日志产生的时间。
源安全区域	安全策略的源安全区域。
源地址	安全策略的源地址。
源端口	安全策略的源端口。
目的端口	安全策略的目的端口。
目的安全区域	安全策略的目的安全区域。
目的地址/地区	安全策略的目的地址。
动作	安全策略对流量的操作结果。
操作	点击<查看详情>，可获取操作日志的详细信息。

说明

点击<查询条件>设置查询条件关键信息，界面只显示匹配的系统日志。

【后续处理】

- 点击<导出>，可以将安全日志导出为Excel格式保存在本地，以方便后续阅读查询。

- 点击<刷新>，获取最新的安全日志。

3. 查询操作日志

【应用场景】

通过查看操作日志，管理员可以查看用户的在线记录，例如登录时所使用的IP地址、操作对象、具体操作、操作时间等信息，了解当前网络中的用户活动情况，发现异常的用户登录或网络访问行为，及时做出应对。

【操作步骤】

(1) 点击[安全监控]>>[日志监控]>>[操作日志]菜单项。

(2) Web界面展示操作日志相关信息。

字段	说明
管理员	执行操作的管理员名称。
主机IP	管理员登录设备使用的主机IP地址。
操作对象	管理员操作的对象类别。
操作	管理员执行的具体操作。
操作时间	管理员执行操作的时间
描述	操作日志的描述信息。
操作	点击<查看详情>，可获取操作日志的详细信息。

说明

点击<查询条件>设置查询条件关键信息，界面只显示匹配的操作日志。

[后续处理]

- 点击<导出>，可以将操作日志导出为Excel格式保存在本地，以方便后续阅读查询。
- 点击<刷新>，获取最新的操作日志。

4. 查询会话日志

【应用场景】

通过查看会话日志，管理员可以查看每条数据流的详细信息，包括数据流的五元组信息（源IP/端口号，目的IP/端口号及协议），以及该数据流命中的安全策略和承载的应用等。

【操作步骤】

(1) 点击[安全监控]>>[日志监控]>>[会话日志]菜单项。

(2) Web界面展示会话日志相关信息。

说明

点击<查询条件>设置查询条件关键信息，界面只显示匹配的操作日志。

[后续处理]

- 点击<导出>，可以将会话日志导出为Excel格式保存在本地，以方便后续阅读查询。
- 点击<自定义字段>，设置页面展示的字段信息。
- 点击<刷新>，获取最新的会话日志。

9.2.3 配置 Syslog 服务器

[应用场景]

设备出厂未配置硬盘，此时，只能依靠内存存储日志（存储时间不超过1天），且设备重启后，内存中日志将全部丢失。为了确保能获取更多的日志信息，可以利用Syslog协议将防火墙的系统日志和安全日志传输到第三方日志平台上进行存储和分析。

【背景信息】

系统最多支持配置3个Syslog服务器。

【操作步骤】

(1) 点击[安全监控]>>[日志监控]>>[Syslog服务器]菜单项。

(2) 配置Syslog服务器1。

a 在“Syslog服务器1”区域，点击<新增>。

b 设置Syslog服务器1相关配置。

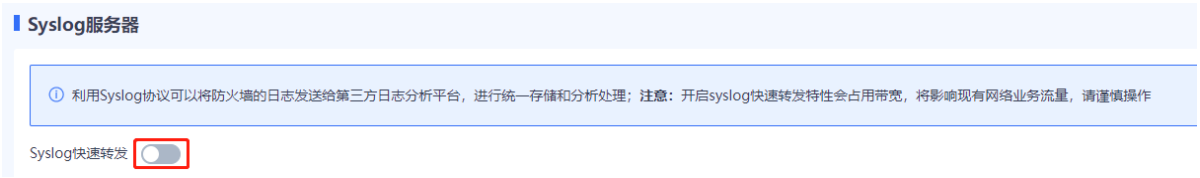
配置项	说明	配置方法
服务器IP	Syslog服务器的IP地址。	设置为Syslog服务器的IP地址。 [示例] 192.168.10.30
端口号	Syslog通知的端口号。	默认端口号为514。 需要与Syslog服务器的端口号设置一致。 [示例] 80
日志类型	Syslog通知的日志类型，包括：系统日志、安全日志。	选择需要发送syslog通知的日志类型。 [示例] 系统日志

c 点击<保存配置>。

(3) （可选）如果需要新增Syslog服务器2，在“Syslog服务器2”区域点击<新增>。

(4) （可选）如果需要新增Syslog服务器3，在“Syslog服务器3”区域点击<新增>。

(5) （可选）如果需要实时转发Syslog日志，可以点击 开启Syslog快速转发功能。



【后续处理】

设置Syslog服务器后，系统会将日志信息发送到指定的应用服务器或维护终端上。

9.3 流量监控

9.3.1 接口流量统计

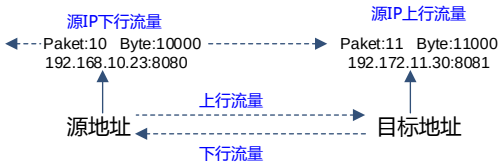
【应用场景】

接口流量监控功能用于展示接口的上行流向流量趋势和下行流量趋势，可以有效地帮助管理员了解当前网络的流量状态，从而制定相关的流量管理措施。

【背景信息】

- 上行流量：接口发出去的流量为上行流量。
- 下行流量：接口接收到的流量为下行流量。

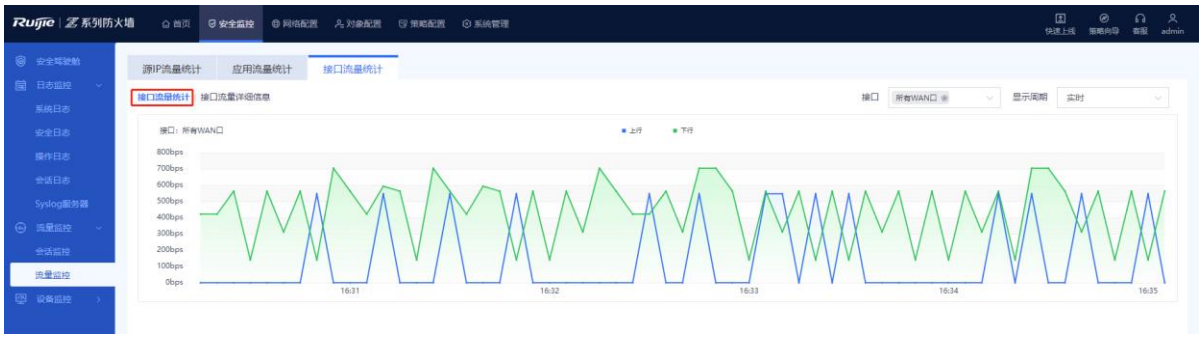
上行流量和下行流量的示意如图所示。



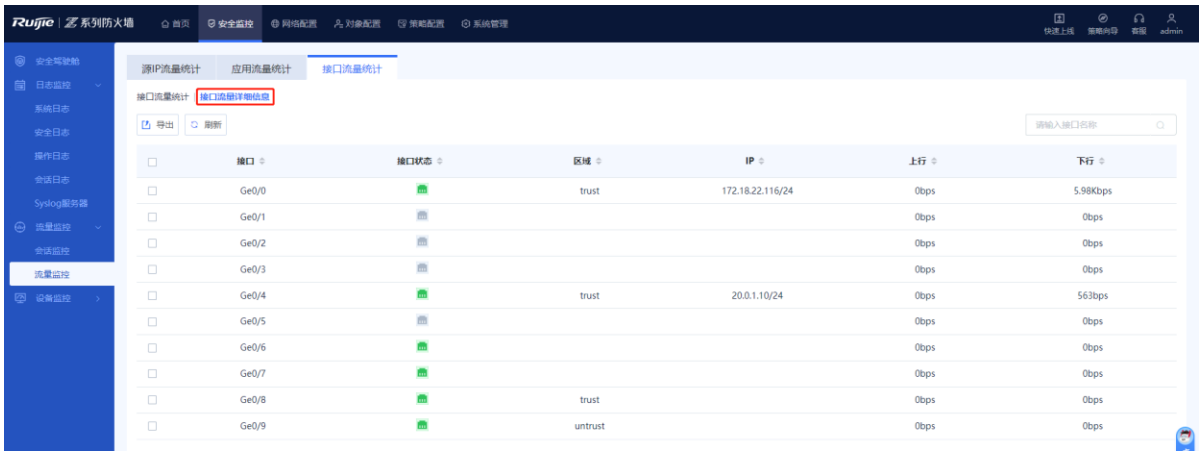
【操作步骤】

(1) 点击[安全监控]>>[流量监控]>>[接口流量统计]。

(2) 点击“接口流量统计”，选择待查看的接口并设置查询周期，系统显示接口流量趋势图。



(3) 点击“接口流量详细信息”，查看接口流量详细信息。



【后续处理】

- 点击<导出>，可以将接口流量信息导出为Excel格式保存在本地。
- 点击<刷新>，可以获取最新的接口流量信息。

9.3.2 源 IP 流量统计

【应用场景】

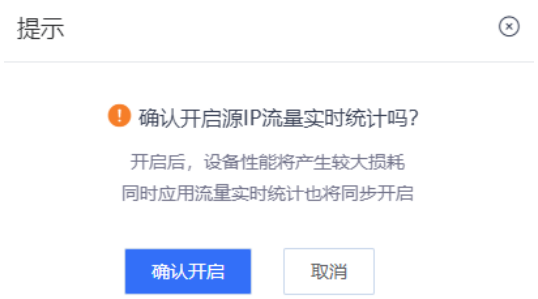
源IP流量统计功能用于展示基于源IP统计的上、下行流向流量及会话数。源IP流量统计功能默认关闭，开启该功能，应用流量实时统计也将同步开启，并且会消耗大部分设备性能，建议在业务不繁忙的时段开启。

【操作步骤】

(1) 点击[安全监控]>>[流量监控]>>[源IP流量统计]。

(2) 点击“流量实时统计”开关。

(3) 在弹出的提示框中点击<确认开启>。



(4) 页面将会展示总流量前10的源IP及其流量信息。点击排名可以设置展示前20的源IP流量。

(5) （可选）点击<导出全部>将实时流量统计结果导出并下载到本地。

9.3.3 应用流量统计

【应用场景】

应用流量统计功能用于展示基于应用统计的上、下行流向流量及会话数。本功能不能单独开启或关闭，随源IP流量统计功能联动开启或关闭。

【操作步骤】

(1) 点击[安全监控]>>[流量监控]>>[应用流量统计]。

(2) 页面将会展示总流量前10的应用及其流量信息。点击排名可以设置展示前20的应用流量。

(3) （可选）点击<导出全部>将实时流量统计结果导出并下载到本地。

9.4 会话监控

9.4.1 简介

设备通过会话展示网路中通信双方建立的连接状态，一条会话表示通信双方的一个连接。会话记录了连接的五元组信息（源地址，源端口号，目的地址，目的端口号和协议），五元组相同的报文即可认为属于同一连接，即同一个会话。

9.4.2 实时会话信息

【应用场景】

实时会话信息功能用于统计和展示当前会话数。用户可根据实际业务需求选择阻断某个会话，会话断开后，该会话的后续报文会被设备丢弃，页面也不再展示该会话信息。

【操作步骤】

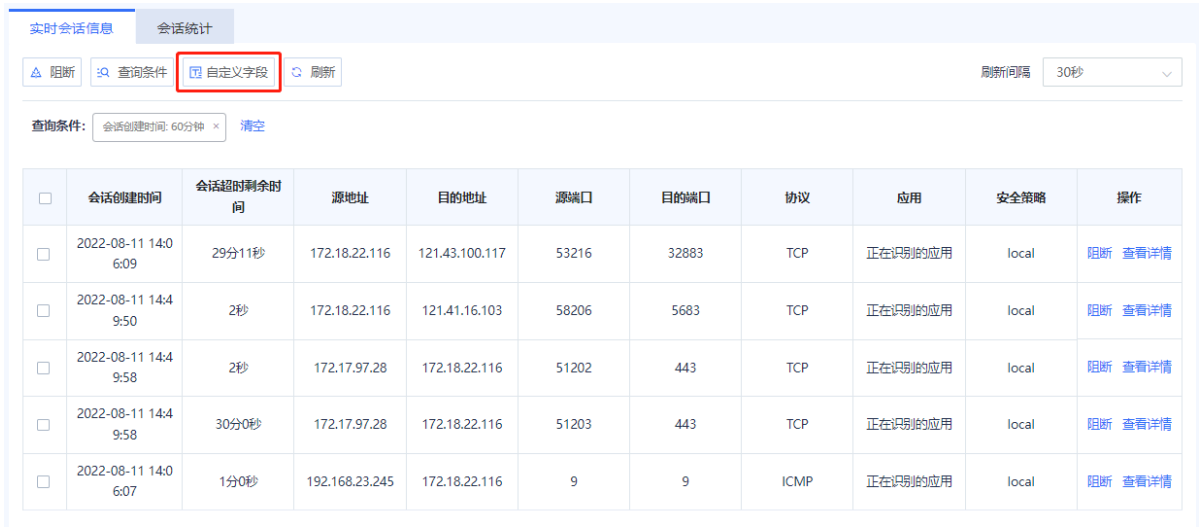
(1) 点击[安全监控]>>[流量监控]>>[会话监控]>>[实时会话信息]。

(2) 选择目标会话，点击“查看详情”可查看会话建立的时间，命中的安全策略、正反向报文数等信息。

(3) （可选）点击<查询条件>可以设置会话的筛选条件。

(4) （可选）勾选一个或多个会话，点击“阻断”可以断开选中的会话。

(5) （可选）点击<自定义字段>可以设置页面展示的会话字段。



9.4.3 会话统计

【应用场景】

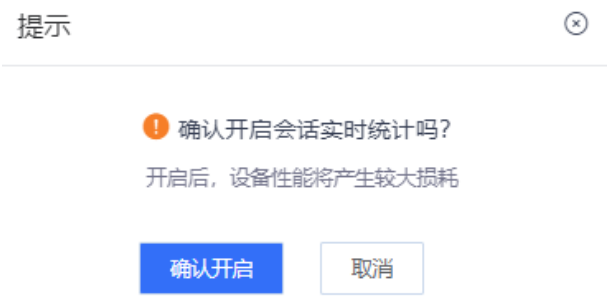
会话统计功能用于统计每个源IP建立的总会话数、TCP会话数、UDP会话及每秒新增会话数等信息。开启本功能会消耗大部分设备性能，建议在业务不繁忙的时段开启。

【操作步骤】

(1) 点击[安全监控]>>[流量监控]>>[源IP流量统计]。

(2) 点击“会话统计”开关。

(3) 在弹出的提示框中点击<确认开启>。



(4) 页面将会展示建立会话总数前10的源IP及其建立的会话信息。点击排名可以设置展示前20的源IP会话。

9.5 设备硬件监控

【应用场景】

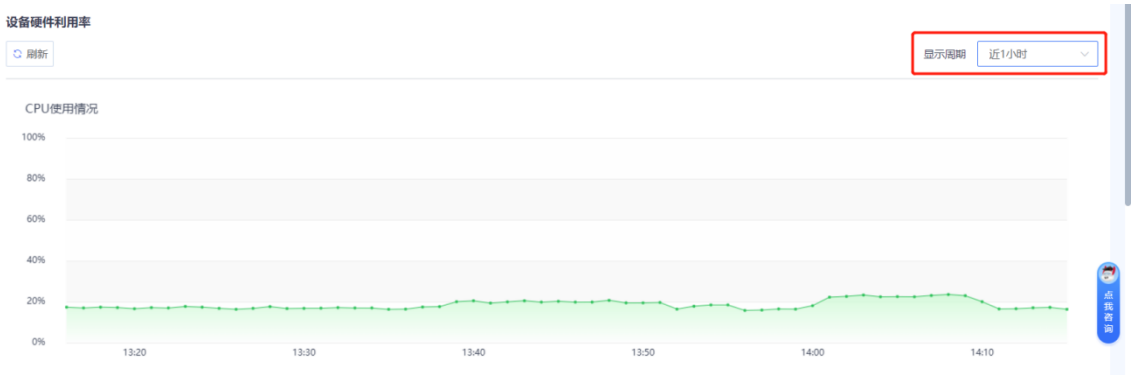
通过该操作，可以监控设备的CPU、内存、硬盘利用率，以便出现异常时及时进行处理。

系统支持设置显示周期为实时、近24小时、近7天，可查看利用率实时数据或近24小时、近7天的历史数据。

【操作步骤】

(1) 点击[安全监控]>>[设备监控]>>[设备硬件监控]菜单项。

(2) 设置显示周期。



显示周期包括：

- 近1小时：系统将展示1小时内的利用率，采样时间间隔为1分钟。
- 近24小时：系统将展示24小时内的利用率，采样时间间隔为5分钟。

- 近7天：系统将展示7天内的利用率，采样时间间隔为1小时。

(3) 界面分区域显示CPU、内存、硬盘利用率。

【后续处理】

检查项	说明
CPU	正常情况下，CPU的利用率应低于80%。如果CPU占用率长时间过高，应检查设备，分析原因。 CPU占用率过高的可能原因如下： ● 开启了应用防护功能或者DDOS防护功能。 ● 新建连接太多，大多是攻击引起。
内存	正常情况下，内存的利用率应低于80%。如果长时间过高，应检查设备，查询原因。
硬盘	正常情况下，硬盘的利用率应低于90%。如果长时间过高，硬盘剩余空间太小，应检查设备，清理硬盘空间。

10 对接诺客云

10.1 简介

诺客云管理平台是应用于SMB场景的管理全链路设备（网关、交换机、AP、防火墙等）的远程管理平台。管理员在诺客云管理平台添加设备后，即可随时随地管理设备。

使用诺客云管理平台前，请确保已获得防火墙通用版授权。

安全能力授权

序号	安全能力名称	描述	授权类型	状态
1	应用识别(APP/URL)	提供防火墙应用识别库和URL库的升级服务	-	未激活 (过期时间：-)
2	入侵防御(IPS)	提供防火墙IPS特征库的升级服务	-	未激活 (过期时间：-)
3	RG-WALL 1600-TY	防火墙通用版授权	正式授权	已激活 (过期时间：永久)

10.2 接入诺客云管

10.2.1 开启诺客云管

【应用场景】

通过诺客云管理平台，用户可以查看设备的基本信息（包括软件版本、硬件版本、MAC地址和产品型号等信息），能够升级设备、查看设备的接口信息、打反向隧道、通过设备的EWEB功能远程控制设备。

【操作步骤】

(1) 点击[系统管理]>>[云管平台]>>[诺客云管]菜单项。

(2) 开启“诺客云管开关”（此开关默认是开启状态），开启后管理员可以在诺客云管理平台管理防火墙设备。

10.2.2 绑定设备

【应用场景】

当管理员需要使用诺客云管理平台管理设备时，需要先绑定设备，绑定后才能在诺客云管理平台查看设备信息及维护设备。

【操作步骤】

(1) 登录防火墙设备的Web管理界面。

(2) 点击[系统管理]>>[云网平台]>>[诺客云]菜单项。

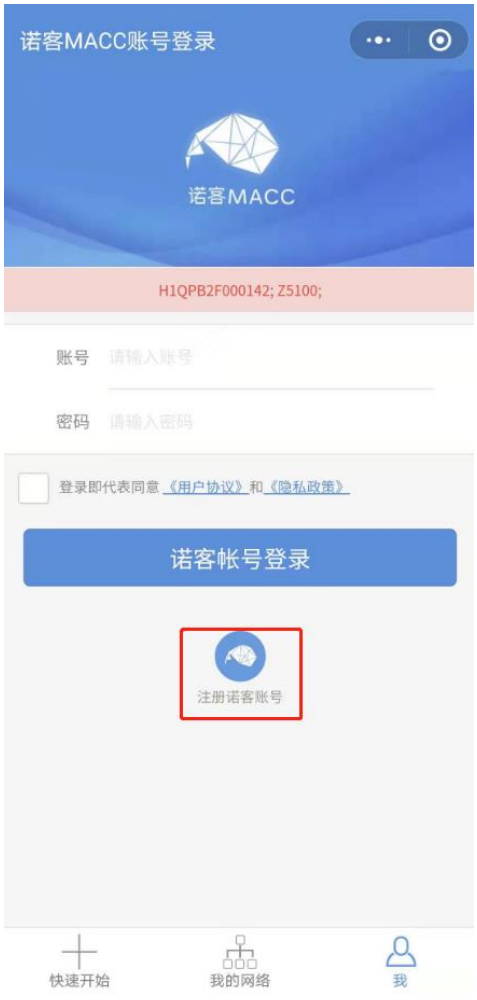
(3) 在“设备绑定”区域，根据页面提示扫描二维码进入小螺号界面，注册诺客云账号。

说明

您也直接在浏览器网址栏输入诺客云平台地址，注册诺客云账号。

(4) 注册诺客云管理平台的账号后，可以登录查看此设备的基本信息。

图10-1 注册账号



【后续处理】

绑定设备成功后，Web界面提示该设备已经绑定相关帐号。

10.3 诺客云管相关操作

10.3.1 查看设备信息

【应用场景】

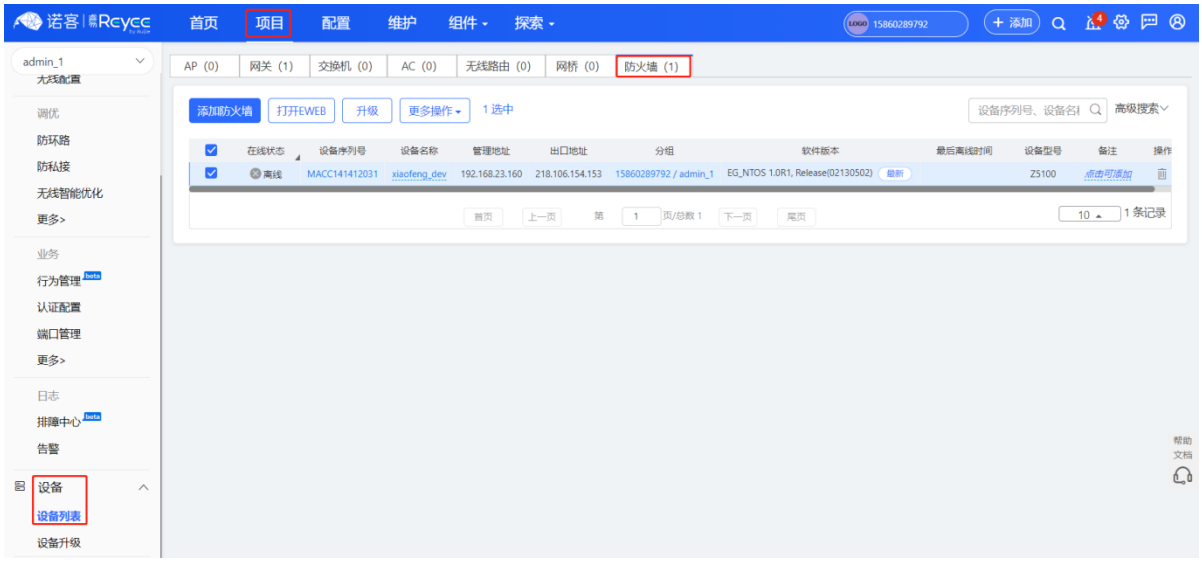
开启诺客云管后，在浏览器输入诺客云管平台网址：http://cloud.ruijie.com.cn/，并登录，可以查看设备信息、在线情况和接口等信息。

【操作步骤】

(1) 点击[项目]>>[设备]>>[设备列表]菜单项，进入设备列表页面。

(2) 点击[防火墙]标签页，查看设备详细信息。

图10-2 防火墙设备详细信息



系统显示设备的在线情况、序列号、设备名称、管理地址、软件版本、设备型号等基本设备信息。

(3) 点击“设备序列号”，进入设备管理界面，查看设备的基本信息、面板信息、接口信息和状态信息。

可通过依次点击相关的标题进行设备管理。

- **设备面板信息：**包括设备面板的接口分布等信息。
- **基本信息：**包括设备名称、设备型号、序列号、MAC地址、软件版本等信息。
- **状态信息：**包括CPU和内存利用率、离线状态、连通状态。
- **接口信息：**通过状态信息中的相应标题栏可查看详细的接口信息，如WAN/LAN口信息(端口号、模式、子网掩码等)。

图10-3 设备面板信息

图10-4 基本信息

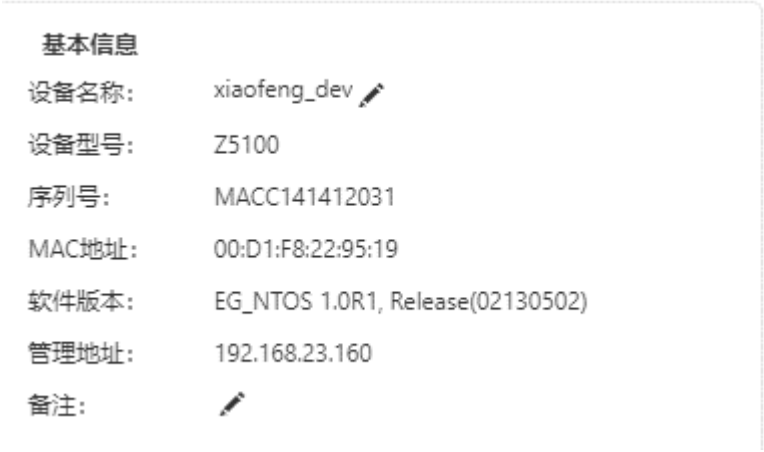


图10-5 状态信息

图10-6 端口信息

10.3.2 隧道管理

(1) 点击<隧道管理>或者直接点击<EWEB配置>访问设备的EWEB界面。

图10-7 隧道管理

(2) 若需要新增隧道，则点击<创建隧道>。

图10-8 创建隧道

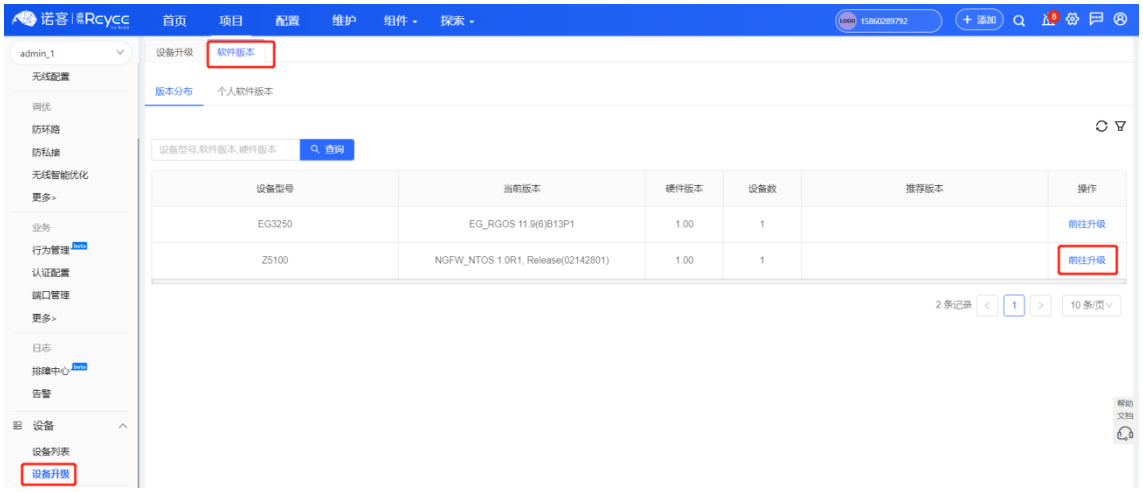
10.3.3 升级设备软件/固件

(1) 点击[设备]>>[设备升级]菜单项。

(2) 上传需要升级的软件版本/固件版本。

(3) 点击<升级>，升级设备的软件/固件。

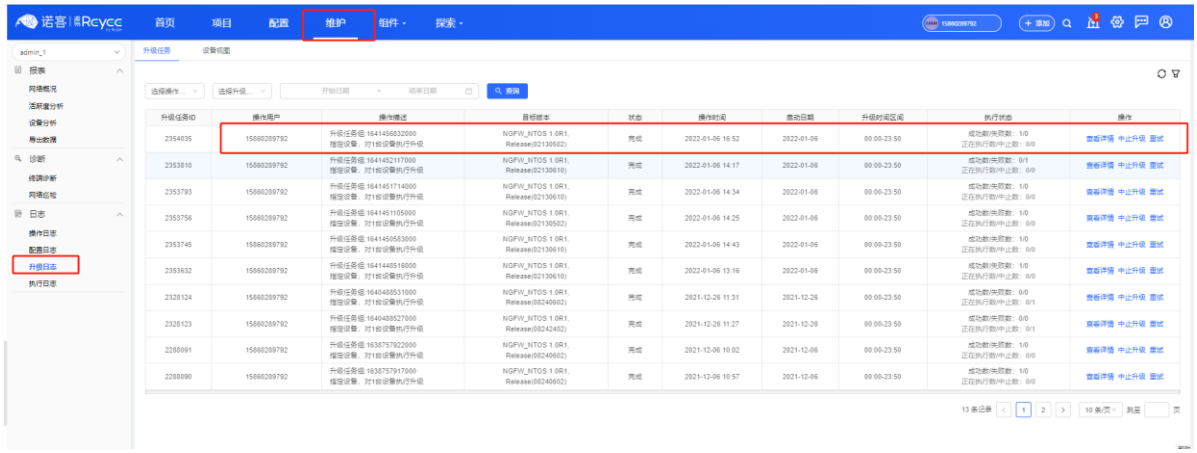
图10-9 升级设备软件版本



启动升级后，进入升级流程，等待设备升级完成后，设备会自动重启，耐心等待升级完成。

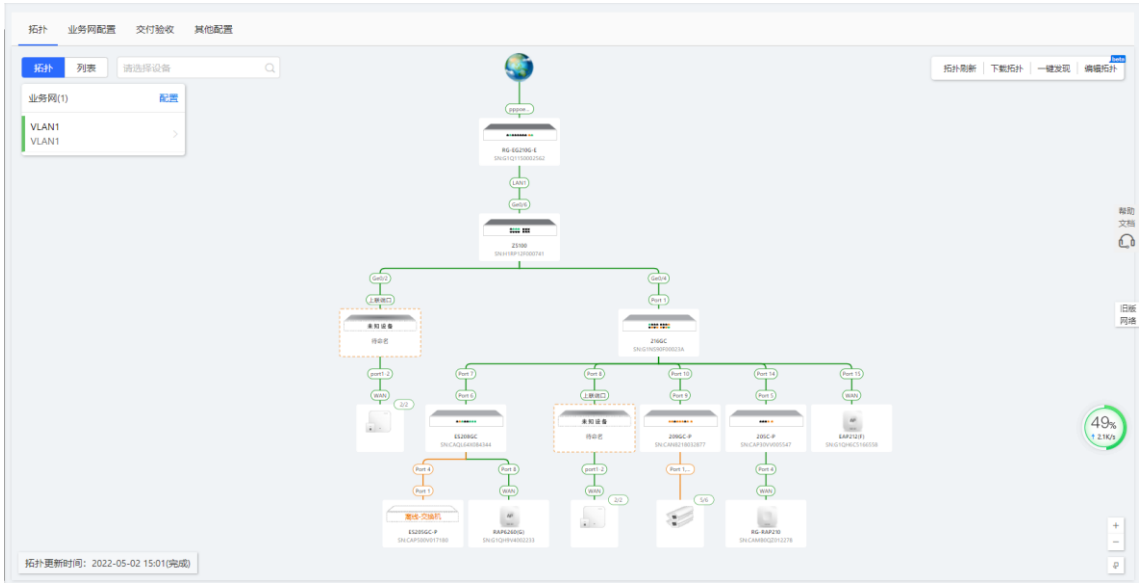
(4) 升级完成后，管理员可以点击[维护]>>[日志]>>[升级日志]页面项查看升级结果。

图10-10升级结果



10.3.4 查看网络拓扑

点击[项目]>>[概览]>>[拓扑]菜单项可以查看防火墙设备与其他网络设备的连接拓扑。



注意

- 当防火墙上存在多条默认路由，或者桥口和路由口混合使用时，在诺客云上查看拓扑连接异常。
- 使用透明部署时，0/MGMT口无需再单独接线。

【后续处理】

- 点击<拓扑刷新>，可以获取最新的拓扑信息。
- 点击<下载拓扑>，可以下载网络拓扑图。
- 点击<编辑拓扑>，可以编辑网络拓扑图，添加未自动识别的设备。

11 典型配置案例

11.1 配置外网用户访问内网服务器

介绍外网用户使用公网地址访问内部服务器的配置举例。

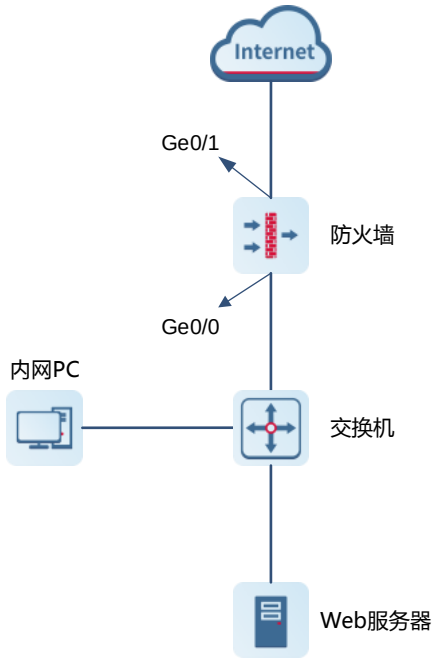
【组网需求】

某公司在网络边界处部署了防火墙作为安全网关。为了使内网Web服务器能够对外提供服务，需要在防火墙设备上配置目的NAT，将内网的Web服务器（192.168.1.2）全映射到外网口的地址（202.1.1.11），让外网的用户能访问到此服务器。公司希望内网用户可以使用公网地址访问这台内部Web服务器，因此还需要在防火墙设备上配置源NAT。

【网络拓扑】

该场景的组网拓扑如图11-1所示。

图11-1 组网拓扑示意



【配置要点】

(2) 配置基础上网。

(3) 配置安全策略。

(4) 配置静态NAT。

【操作步骤】

(5) 基础上网配置。

点击[网络配置]>>[接口]>>[物理接口]菜单项。

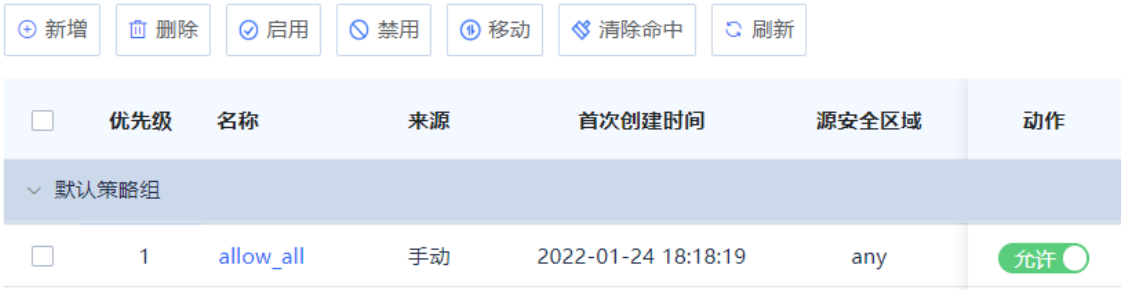
接口配置如下：

接口名称	描述	网口状态	模式	区域	链接类型	IP地址	MTU	操作
Ge0/0	-		路由	trust	静态IP	192.168.1.200/24	1500	编辑
Ge0/1	-		路由	untrust	DHCP	172.26.1.116/24	1500	编辑

(6) 配置安全策略。

点击[策略配置]>>[安全策略]>>[安全策略]菜单项。

策略配置如下：



(7) 配置目的NAT。

a 点击[策略配置]>>[NAT策略]>>[NAT转换]菜单项。

b 点击<新增>。

c 设置目的NAT相关配置项。

配置项	说明
基本信息	
名称	Web服务器策略
启用状态	启用
原始数据包	
源区域	untrust和trust
源地址	any
目的地址	any
服务	源端口：0~65535；目的端口18080（外部端口）
转换后数据包	
IP地址	192.168.1.2
端口	80（内部端口）

d 点击<保存>。

【验证效果】

从外部可以访问内网服务器http://172.26.1.116。

11.2 配置内网用户通过公网地址访问内部服务器

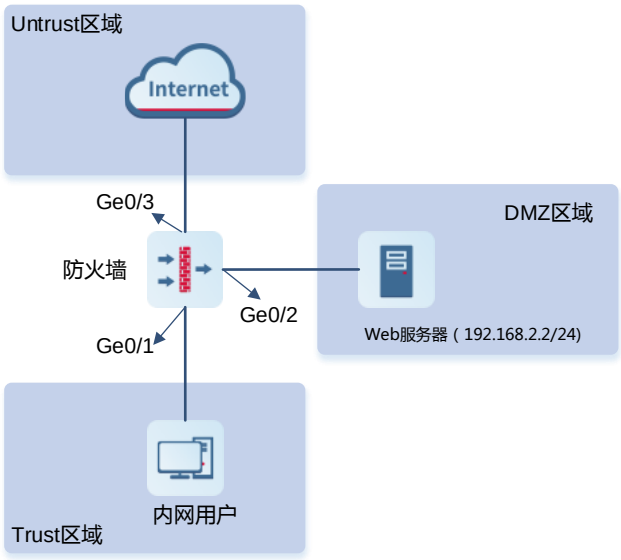
介绍内网户使用公网地址访问内部服务器的配置举例。

【组网需求】

某公司在网络边界处部署了防火墙作为安全网关，内网部署了一台Web服务器对外提供服务。现在需要将内网的WEB服务器（192.168.2.2）映射到外网口的地址（200.10.10.10），让内外网的用户能访问到此服务器：

- 内网服务器区存在WEB服务器（区域:DMZ, IP地址:192.168.2.2，服务：HTTPS）。
- 外网用户通过访问防火墙外网接口地址（区域:untrust, IP地址:200.10.10.10，端口50000）访问Web服务器。
- 内网用户(区域:trust)也能通过访问防火墙外网接口地址（区域:untrust, IP地址:200.10.10.10，端口50000）访问Web服务器，并且访问服务器时的源地址是防火墙的外网接口地址。

【网络拓扑】



【配置要点】

(1) 基础上网配置。

(2) 配置安全策略。

(3) 为外网用户访问配置目的NAT转换策略。

(4) 为内网用户访问配置双向NAT转换策略。

【操作步骤】

(5) 配置基础上网。

具体的操作请参见3 快速部署。

(6) 配置安全策略。

策略配置如下：

(7) 为外网用户配置目的NAT转换策略。

a 点击[策略配置]>>[NAT策略]>>[NAT转换]。

b 点击[新增]。

c 在[新增NAT转换]界面，设置目的NAT策略相关配置项。

配置项	说明
基本信息	
名称	策略1
启用状态	启用
原始数据包	
源区域	untrust
源地址	any

配置项	说明
目的地址	防火墙外网口IP地址（Ge0/3:200.10.10.10）
服务	创建一个自定义服务“服务器映射”（如TCP，源端口0-65535，目的端口50000）
转换后数据包	
IP地址	DMZ区域Web服务器的IP地址（192.168.2.2/24）
目的端口转换为	443（WEB服务器端口）

d 点击<保存>。

(8) 为内网用户配置双向NAT转换策略。

a 点击[策略配置]>>[NAT策略]>>[NAT转换]。

b 点击[新增]。

c 在[新增NAT转换]界面，设置双向NAT策略相关配置项。

配置项	说明
基本信息	
名称	策略2
启用状态	启用
原始数据包	
源区域	trust
源地址	any
目的地址	防火墙外网口IP地址（Ge0/3:200.10.10.10）

配置项	说明
服务	创建一个自定义服务“服务器映射”（如TCP，源端口0-65535，目的端口50000）
转换后数据包	
源地址转换为	指定IP：源地址转换配置指定IP为防火墙外网地址200.10.10.10。 如果防火墙有多个外网地址，可以选择将外网地址配置成地址组对象，然后应用该地址组对象。 说明：配置成出接口地址则会导致源IP被转换成192.168.2.1，不满足需求。
指定IP	防火墙外网口IP地址（Ge0/3:200.10.10.10）
目的地址转换为	DMZ区域web服务器的IP地址（192.168.2.2）
目的端口转换为	443（WEB服务器端口）

d 点击<保存>。

【配置验证】

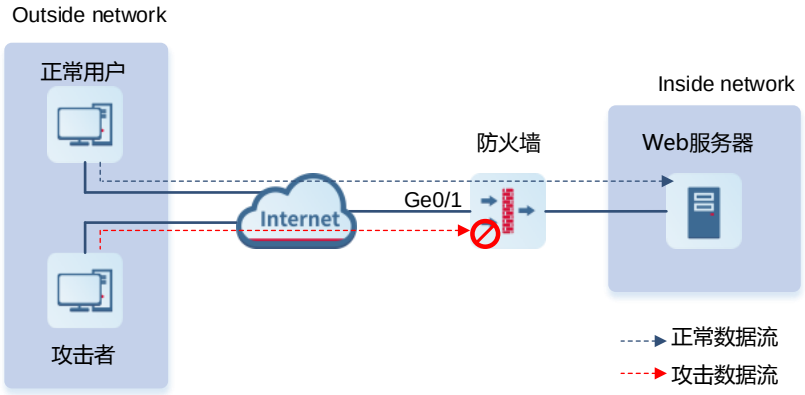
- 通过内网访问http://200.10.10.10:50000。
- 通过外网访问http://200.10.10.10:50000。

如果通过内网外均能访问，说明NAT策略配置成功。

11.3 配置 DDoS 攻击防护

【组网需求】

防火墙设备部署在内网出口处，企业内网部署了Web服务器。经检测，Web服务器经常受到SYN洪水攻击、UDP洪水攻击和ICMP洪水攻击，为了保障Web服务器的正常运行，需要在防火墙上配置攻击防范功能，用来防范以上三种类型的DDoS攻击。



【配置思路】

(1) 对于外网连接的端口Ge0/1启用流量学习功能，对外网访问企业内网的流量进行统计。

(2) 在防火墙上开启SYN Flood、UDP Flood和ICMP Flood攻击防护功能。各攻击防护对应的阈值先采用默认值。

【操作步骤】

(3) 为Ge0/1开启流量学习。

a 点击[策略配置]>>[流量学习]菜单项。

b 点击<流量学习地址>，设置流量学习地址。

在“添加自定义IP”中输入Ge0/1的IP地址，并点击<保存配置>。

c 点击<开启流量学习>。

(4) 将Ge0/1加入untrust区域。

a 点击[网络配置]>>[区域]菜单项。

b 选择untrust区域，点击<编辑>。

c 在“接口”区域，选择Ge0/1。

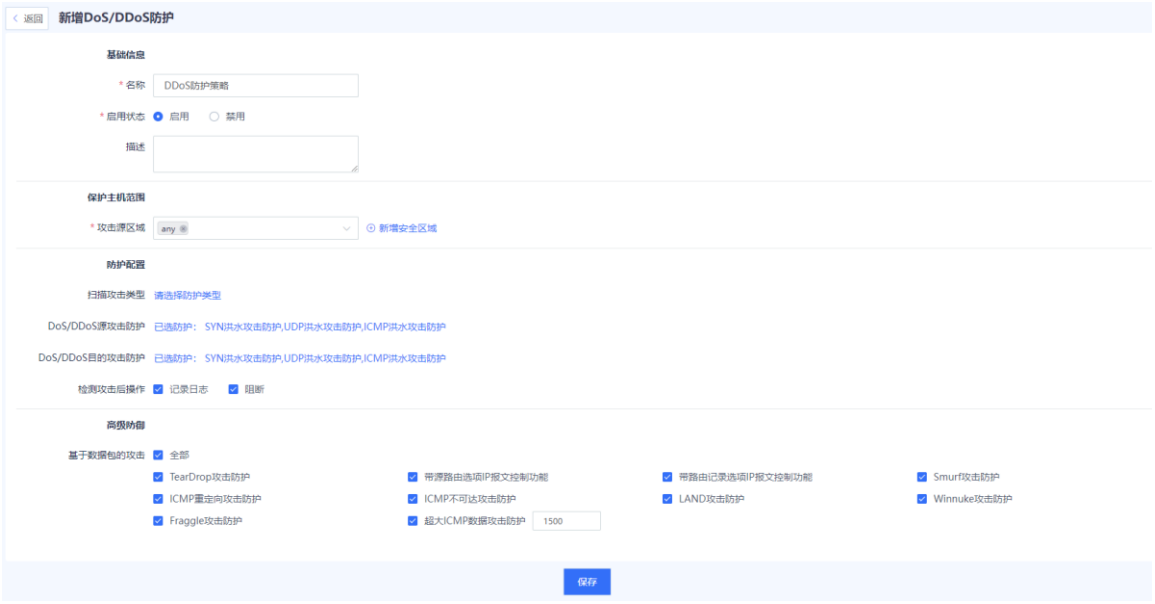
d 点击<保存>。

(5) 配置DOS/DDoS防护策略。

a 点击[策略配置]>>[安全防护]>>[DoS/DDoS防护]菜单项。

b 点击<新增>。

c 设置DoS/DDoS防护策略相关参数。



d 点击<保存>。

【结果验证】

- 配置完成后，DDoS攻击防范采用的阈值为默认阈值。流量学习结束后，可以查看攻击防范的效果。如果Web服务器继续受到攻击，可以调整对应的攻击阈值。

- 配置完成后，系统对检测到的攻击会记录安全日志。选择[安全监控]>>[日志监控]>>[安全日志]，可以查看详细的安全日志。

12 常见问题

12.1 无法登录 Web 页面

【可能原因】

该问题的可能原因包括：

- 设备连通性问题。
- 管理PC浏览器不兼容。
- 登录密码输入错误。

【排查步骤】

根据原因逐条排查：

- 设备连通性问题。

  登录管理PC，在命令行下运行Ping XXX.XXX.XXX.XXX（XXX.XXX.XXX.XXX为防火墙设备的管理口IP地址），检查防火墙设备和管理PC的连通性。

  - 如果能接收到防火墙设备返回的信息，则说明连通性正常。请排查其他原因。
  - 如果不能接收到防火墙设备返回的信息，则说明存在连通性问题。请重设设置防火墙设备的管理口IP地址。

- 管理PC浏览器不兼容。

(1) 检查管理PC上的浏览器是否满足兼容性要求。

  - 是->继续排查其他原因。
  - 否->重新安装满足兼容性的浏览器。

说明

兼容的浏览器包括：IE、Firefox、GoogleChrome或360浏览器。

- 登录密码输入错误。

(2) 重新输入密码。

(3) 如果多次输入错误，请重置登录密码为默认密码。

12.2 无法登录 SSH 页面

【可能原因】

SSH端口号错误。

【排查步骤】

(1) 检查网络连接。

(2) 如果网络正常，则点击[系统管理]>>[系统配置]>>[服务参数]>>[SSH]菜单项，修改SSH端口号。

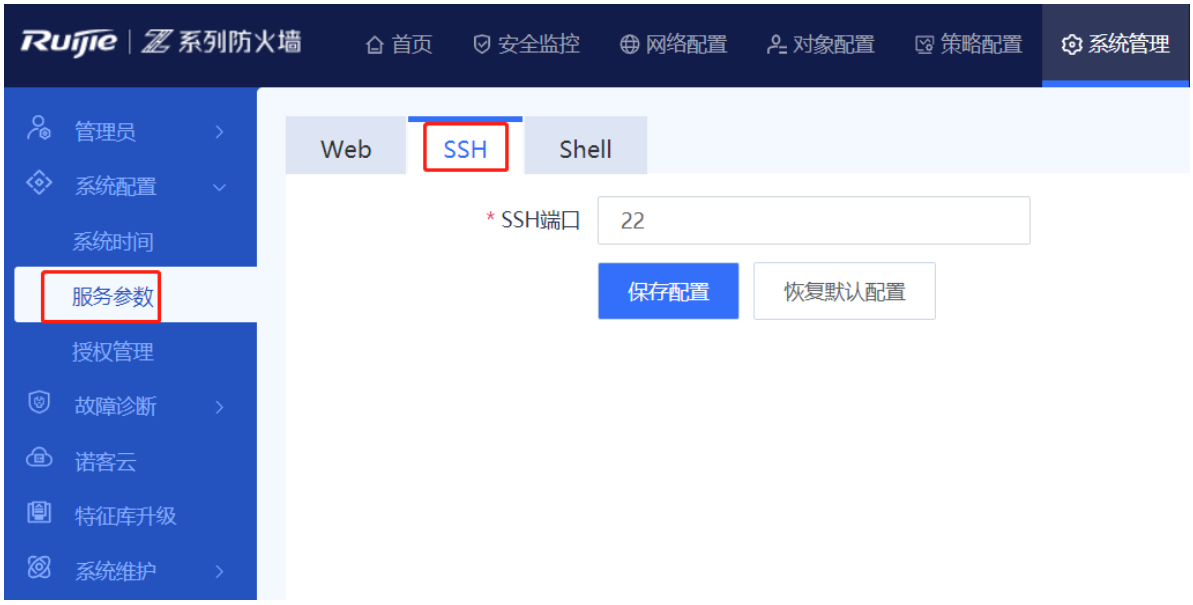



图12-1 修改 SSH 端口号