天清汉马 T 系列防火墙

配置管理手册

北京启明星辰信息安全技术有限公司

Beijing Venus Information Security Inc.

二零二一年六月

天清汉马T系列防火墙配置管理手册

手册版本	V5.0
产品版本	V5.0
资料状态	发行

版权声明

免责声明

本手册依据现有信息制作，其内容如有更改，恕不另行通知。启明星辰公司在编写该手册的时候已尽最大努力保证其内容准确可靠，但启明星辰公司不对本手册中的遗漏、不准确或错误导致的损失和损害承担责任。

User's Manual Copyright and Disclaimer

Copyright

Disclaimer

This document and the information contained herein is provided on an "AS IS" basis.Venus InfoTech Inc. may make improvement or changes in this document,at any time and without notice andas it sees fit.The information in this document was prepared by Venus Info Tech Inc.with reasonablecare and is believed to be accurate.However,Venus Info Tech Inc.shall not assume responsibility forlosses or damages resulting from any omissions,inaccuracies, or errors contained herein.

副本发布声明

启明星辰公司的天清汉马 T 系列防火墙产品正常运行时，包含 2 款 GPL 协议的软件（linux、zebra）。启明星辰公司愿意将 GPL 软件提供给已经购买产品的且愿意遵守 GPL 协议的客户，请需要 GPL 软件的客户提供（1）已经购买的产品的序列号，（2）有效送达 GPL 软件地址和联系人，包括但不限于姓名、公司、电话、电子邮箱、地址、邮编等；（3）人民币 100 元的光盘费和快递费，客户即可获得产品所包含的 GPL 软件。

内容介绍

本手册详细介绍 T 系列防火墙的功能特性，配置方法；用于指导用户对于 FW 产品的配置，使用。本书共分为六部分：

第一部分管理方式介绍

内容涵盖第 1 章；主要介绍 T 系列防火墙的 WEB 管理方法。

第二部分系统信息

内容涵盖第 2-14 章；主要介绍 T 系列防火墙的系统状态，历史数据统计，流量监控等功能的使用方法。

第三部分网络配置

内容涵盖第 16-41 章，主要介绍 T 系列防火墙网络相关功能配置方式。包括 VLAN，链路聚合，IP 地址，静态路由，策略路由，动态路由，静态 ARP，NAT，协议管理，网络调试的介绍。

第四部分安全特性

内容涵盖第 42-68 章；主要介绍 T 系列的安全相关策略的配置，包括安全策略，ARP 和 DoS 防护策略，流控策略，应用策略，会话控制策略等

第五部分模板与对象

内容涵盖第 69-79 章；T 系列防火墙为使配置更加灵活简便，引入了对象及模板的概念。对象建立好后，可以在多种业务功能中使用。该部分包括对地址对象，时间对象，服务对象，ISP 地址对象，健康检查模板的介绍。

第六部分系统管理

内容涵盖 80-90 章，主要介绍 T 系列防火墙安全特性的系统特性的配置方式。包括设备基本配置，时间配置，配置文件管理，操作系统升级管理，管理员，许可授权，高可靠性，VRRP ，日志管理和 SNMP。

目录

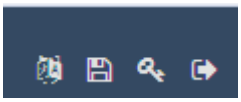
1 第1章 Web 管理介绍

1.1 Web管理概述

通过运行Internet浏览器的任何计算机使用HTTP或一个安全的HTTPS连接，便能够配置并管理T系列防火墙设备。在进行Web管理前，必须配置T系列防火墙设备使其能够接受来自指定接口的HTTP或HTTPS管理。

推荐使用IE10.0及以上版本、Mozilla50.0及以上版本、chrome54.0浏览器，推荐显示分辨率为1600×900。

1.2 工具条



 语言

 保存配置

 修改密码

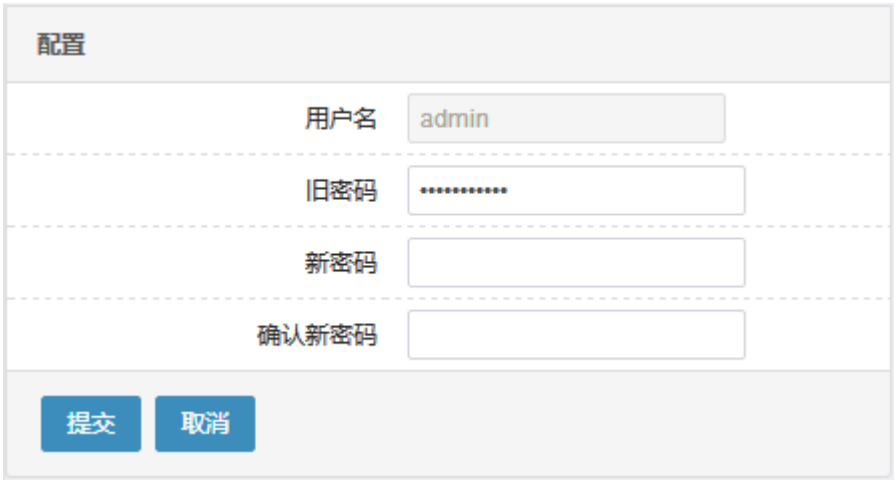
 注销

1.2.1 保存配置

保存配置按钮永久保存配置更改。设备默认不永久保存配置更改，如果进行配置更改后，不点击**保存配置**按钮，则设备下一次启动后会丢失上次所做的配置。

1.2.2 修改密码

修改密码按钮在新窗口中打开修改密码页面。



参数说明：

用户名：管理员名称。

旧密码：管理员的旧密码。

新密码：设置的新密码。

确认新密码：确认设置的新密码。

1.2.3 注销

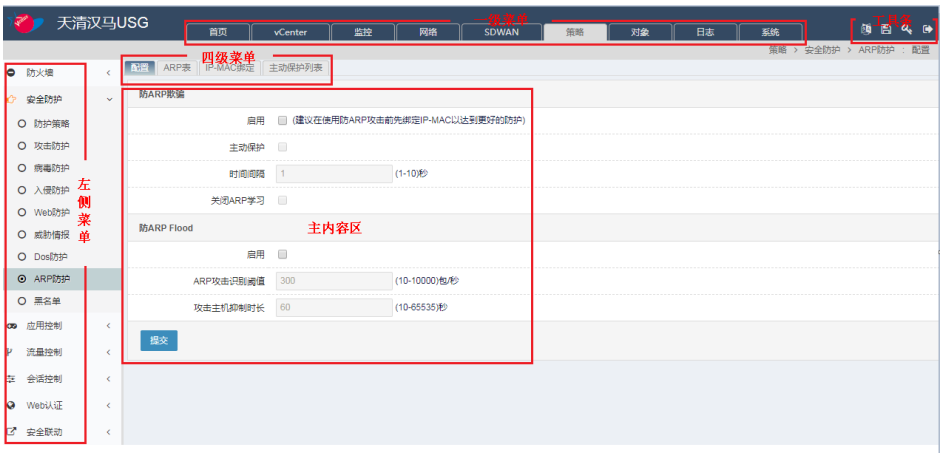
注销按钮立即注销当前登录用户，并跳转到用户登录页面。

1.3 Web管理

Web管理界面由顶部一级菜单、工具条、左侧二/三级菜单、四级菜单和主内容区组成；

除了首页外每个一级菜单有相应的一个或多个子级菜单，最多可能有四级菜单；

当点击一个一级菜单项，如“策略”时，左侧菜单内容会展示出策略功能下的二级子菜单：“防火墙”、“安全防护”、“应用控制”、“流量控制”、“会话控制”、“Web认证”“安全联动”，同时默认第一个二级菜单“防火墙”会自动展开，并选中该菜单第一个三级菜单“策略”。若此三级菜单下存在四级子菜单，如“安全防护”>“ARP防护”，则会在页面右侧主内容区上部分区域以“页签”的方式显示，并选中第一个四级子菜单项“配置”，该页面会在主内容区中显示。



1.3.1 菜单

菜单提供了 T 系列防火墙设备的主要配置选项。

首页：常用的业务信息趋势图、系统当前运行状态、高级别日志信息、系统信息和主要功能的配置概览。

vCenter：可视化中心，可查看整机及各业务功能相关的网络使用状态趋势，以及所监测到的有威胁的攻击事件信息。

监控：监控设备运行状况，从各个角度监控设备流量、会话的实时状况以及历史趋势。包括系统、接口、威胁、用户、应用、流控、URL、会话。

网络：网络相关配置。包括接口、安全域、ARP、DHCP、路由、NAT、VPN、系统参数、DNS 代理、DNS 服务、网络调试。

策略：策略相关配置。包括防火墙、安全防护、应用控制、流量控制、会话控制、Web 认证、安全联动。

对象：一些系统通用的配置项，可以供其他模块引用。包括各类对象管理、健康检查、CA 证书。

日志：各项功能日志的查看和日志功能的相关配置。包括系统日志、审计日志、安全日志、VPN 日志、日志管理。

系统：系统相关的配置。包括配置、管理员、版本管理、许可管理、高可用性、VRRP、SNMP。

1.3.2 列表

很多管理配置页面是列表的形式，例如管理员、接口、防火墙策略等。下图为 T 系列防火墙设备列表图。

列表中的条目显示项信息。列表中最右面的列一般为图标按钮列，可对该条目进行一些操作，例如**重置统计次数、移动、插入、删除**等。点击列表中的名称列或者 ID 列时，进入到编辑该条目的页面，这样的列一般显示为蓝色。例如这里的#列，即 ID 列。

通过列表上方的**新建**按钮，可以增加条目。**新建**和编辑操作的页面是基本一致的。

1.3.3 图标

页面中有一些图标按钮辅助进行配置管理操作。鼠标停留在图标上时，会出现提示信息，以描述图标的含义。常见图标有如下几种：

图标	名称	说明
	移动	移动当前条目到指定位置
	插入	在当前条目前面插入一个新条目
	重命名	给当前条目重命名
	删除	删除一个条目

1.4 设备默认配置

出厂的 T 系列防火墙设备有默认的配置。这些默认配置让用户不需要进行额外配置就能够通过 Web 浏览器登录设备进行管理和配置。

1.4.1 管理接口的默认配置

管理接口（MGT）的默认地址配置为 192.168.1.250/24。允许对该接口进行 PING 和 HTTPS 操作。注意：有些类型的设备是没有管理口的，默认地址配置在第一个业务口上，一般是 ge0/0。

1.4.2 默认管理员用户

系统默认的管理员用户为 admin，密码为 FW.admin@4.1。用户可以使用这个管理员账号从任何地址登录设备，并且使用设备的所有功能。

系统默认的审计员用户为 audit，密码为 FW.audit@4.1。用户可以使用这

个账号对日志系统进行审计。

系统默认的用户管理员用户为 useradmin，密码为 FW.user@4.1。用户可以使用这个账号来配置系统管理员。

2 第2章 首页

2.1 首页

通过 Web 登录设备后默认进入首页，该页面显示设备当前整体的运行状态，包括设备用户流量排行 Top10 趋势、应用流量排行 Top10 趋势、设备上下行流量趋势、网络连接数趋势、高级别日志信息、物理接口信息表、设备基本信息、常用配置概览。

在每个小面板的右上角有 

和 

两个图标，分别能刷新和展开/折叠当前面板。

可以通过首页的接口信息，和版本信息、cpu 和内存使用率来观察设备是否正常加载：

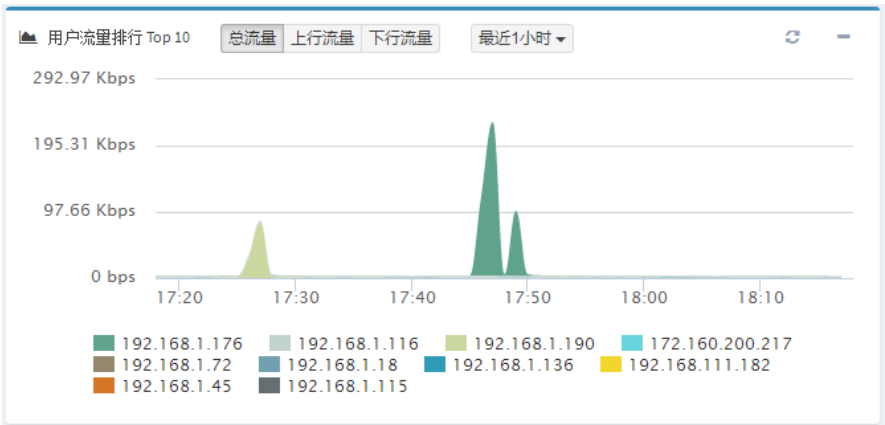
1、接口信息和物理接口数量和类型一致，如不一致请检查序列号或者硬件。

2、版本信息和发布版本信息一致或提供的临时版本信息一致，如不一致请检查升级包。

3、cpu 和内存使用率可以正常显示。

4、硬盘信息是否正确，如显示 N/A，说明设备没有配置硬盘。如设备配置硬盘，未正常加载，请联系厂家。

2.1.1 用户流量排行Top10



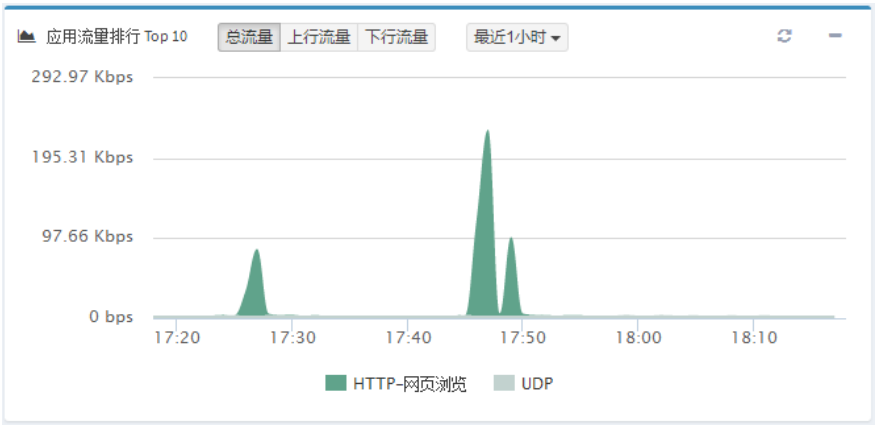
统计指定时间段内流量排行前 10 的用户（IP）流量速率的变化趋势。

统计内容默认的时间范围是最近 1 小时，按总流量排序；

排序内容可选“总流量/上行流量/下行流量”做为排序标准；

时间范围可选“最近 1 小时/最近 1 天/最近 7 天/最近 30 天”。

2.1.2 应用流量排行 Top 10



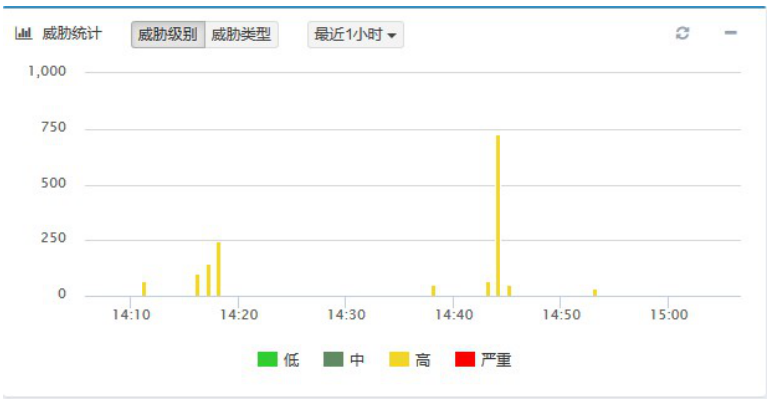
统计指定时间段内流量排行前 10 的应用流量速率的变化趋势。

统计内容默认的时间范围是最近 1 小时，按总流量排序；

排序内容可选“总流量/上行流量/下行流量”做为排序标准；

时间范围可选“最近 1 小时/最近 1 天/最近 7 天/最近 30 天”。

2.1.3 威胁统计

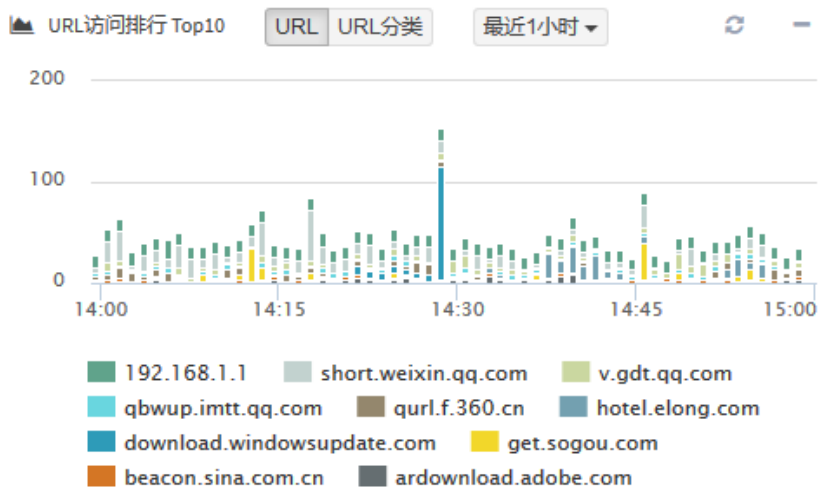


统计指定时间段内威胁级别和威胁类型的变化趋势。

统计内容默认的时间范围是最近 1 小时；

时间范围可选“最近 1 小时/最近 1 天/最近 7 天/最近 30 天”。

2.1.4 URL访问排行Top10

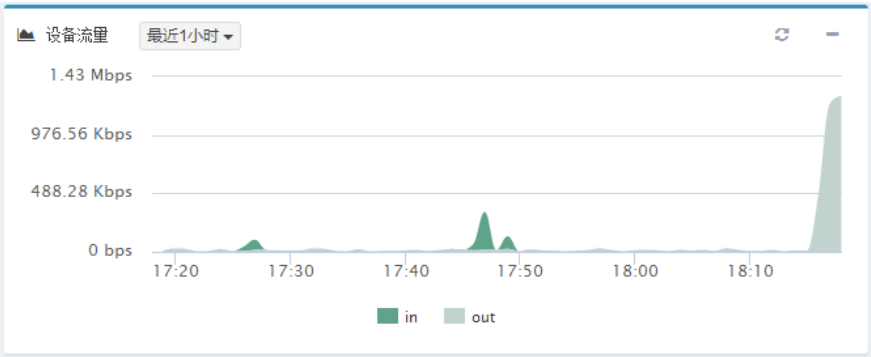


统计指定时间段内 URL 和 URL 分类访问量的变化趋势。

统计内容默认的时间范围是最近 1 小时；

时间范围可选“最近 1 小时/最近 1 天/最近 7 天/最近 30 天”。

2.1.5 设备流量

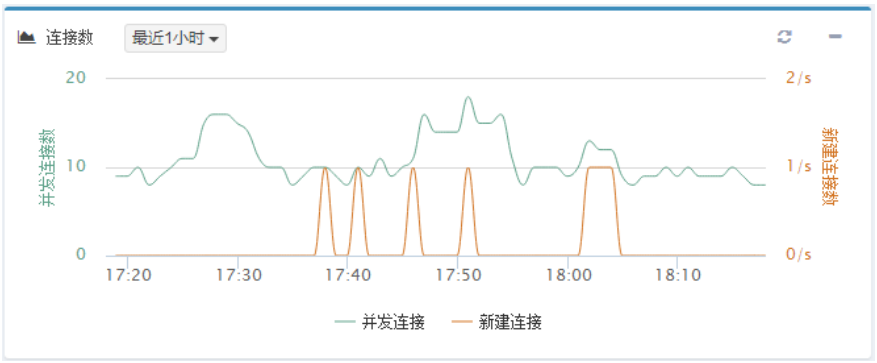


统计指定时间段内设备整机 in/out 流量速率的变化趋势。

统计内容默认的时间范围是最近 1 小时；

时间范围可选“最近 1 小时/最近 1 天/最近 7 天/最近 30 天”。

2.1.6 连接数



统计指定时间段内“并发连接”和“新建连接”的均值变化趋势。

统计内容默认的时间范围是最近 1 小时；

时间范围可选“最近 1 小时/最近 1 天/最近 7 天/最近 30 天”。

2.1.7 高级别日志

查看最新高级别日志数据。

首页的高级别日志列表中，包含了所有类型日志里的高级别记录；

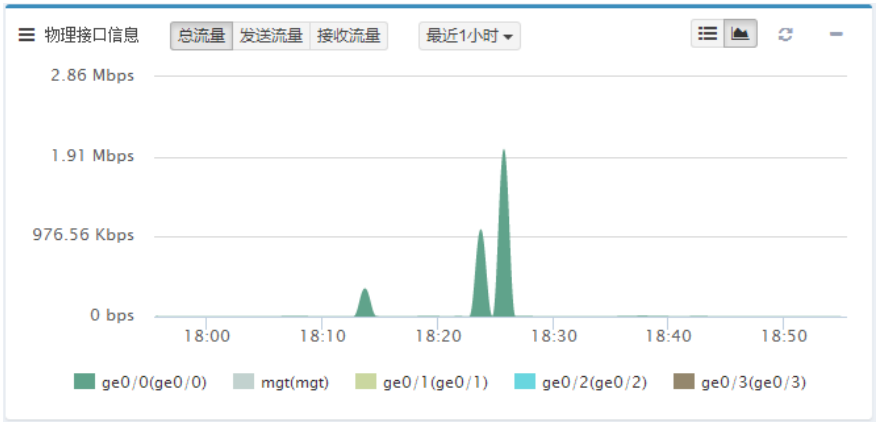
点击“详情”连接，可跳转到日志菜单下，即可浏览各类型日志的详细内容。

2.1.8 物理接口信息

查看设备中物理接口实时信息和历史趋势，默认显示实时信息。

点击此面板右上角的“表格/线图”切换按钮如下图：

即可将物理接口信息表格切换为曲线图的形式来展示，如下图：



统计指定时间段内物理口流量速率的变化趋势。

统计内容默认的时间范围是最近 1 小时，按总流量排序；

排序内容可选“总流量/上行流量/下行流量”做为排序标准；

时间范围可选“最近 1 小时/最近 1 天/最近 7 天/最近 30 天”。

2.1.9 系统信息

查看设备基本信息。

主机名称：可以由管理员用户配置，可以通过主机名称区分设备。

序列号：当前设备的唯一标识，是设备出厂时设定好的。

软件版本：当前设备运行的系统软件的版本号。

Release：售后服务时使用的编码。

入侵防护特征库版本：最新入侵防护特征库更新时间和特征数量。

病毒防护特征库版本：最新病毒防护特征库更新时间和特征数量。

应用分类特征库版本：最新应用分类特征库更新时间和特征数量。

URL 分类特征库版本：最新 URL 分类特征库更新时间和特征数量。

系统时间：当前系统时间。

系统运行时间：系统从上次启动到现在已经运行的时间。

HA 状态：设备 HA 状态（单机状态、主状态、备状态、主 A 状态、主 N 状态）。

CPU 使用率：当前设备 CPU 使用率。

内存使用率：当前设备内存使用率。

设备温度：当前设备的温度。

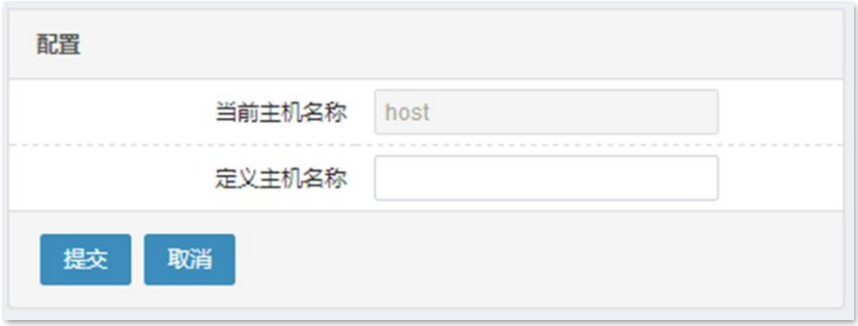
磁盘信息：表示设备上存储磁盘的容量信息。

基础授权：设备基础授权时间。

修改主机名称

为了方便区分设备，有时候需要修改主机名。

首页>系统信息，点击主机名称一栏中的**图标**，跳转到修改名称页面：



当前主机名： 设备当前主机名。

定义主机名： 修改后的主机名。

在定义主机名中输入新的主机名称，点击**提交**按钮。

2.1.10 常用配置概览

查看常用功能配置的基本情况，包括：

物理接口、VLAN、透明桥、聚合链路、安全域、静态路由、策略路由、NAT、防火墙策略、攻击防护策略、应用控制策略、Web 控制策略、流量控制策略、会话控制策略、Web 认证策略、HA；

点击各项配置对应的数字连接，页面可跳转至相应的配置页面。

3 第3章 vCenter

3.1 vCenter概述

通过 vCenter 功能，可监控防火墙设备的整机流量情况和捕获威胁情况，并可以调整最近 1 小时、最近 1 天、最近 7 天、最近 30 天监控周期。

3.2 流量

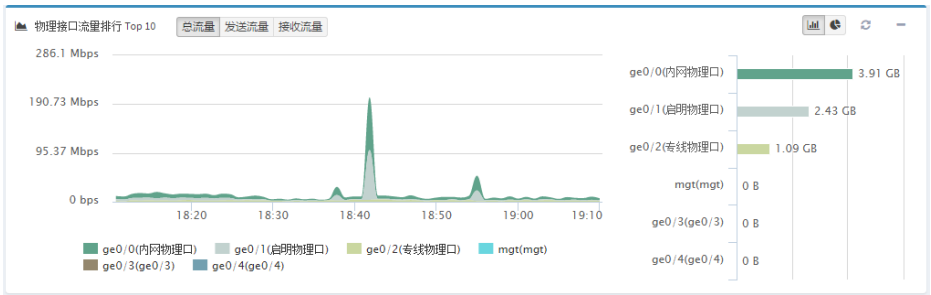
查看步骤：

点击 **vCenter>流量**进入流量可视化页面，可以查看防火墙设备最近 1 小时、最近 1 天、最近 7 天、最近 30 天的各时间段流量信息。

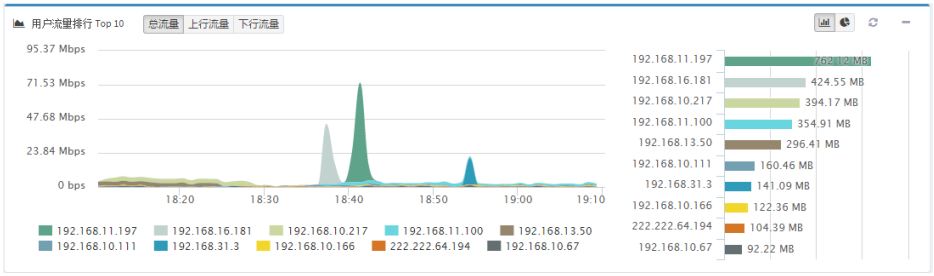
查看内容包括设备流量、连接数、物理接口流量排行 Top 10、用户流量排行 Top 10、应用分类流量排行 Top 10、应用流量排行 Top 10、URL 访问分类 Top 10、URL 访问 Top 10。

设备流量和连接数 统计展示：

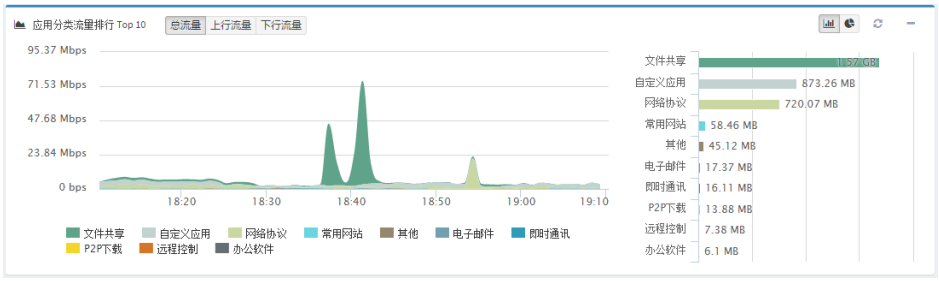
物理接口流量排行 Top 10 统计展示：



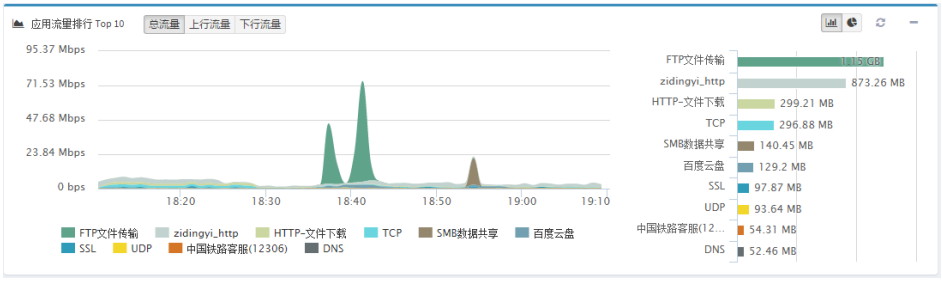
用户流量排行 Top 10 统计展示：



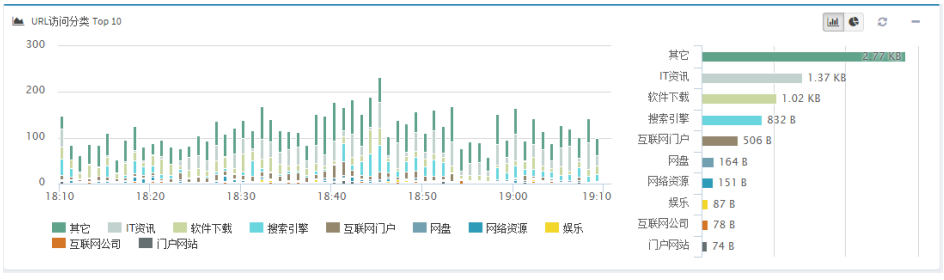
应用分类流量排行 Top 10 统计展示：



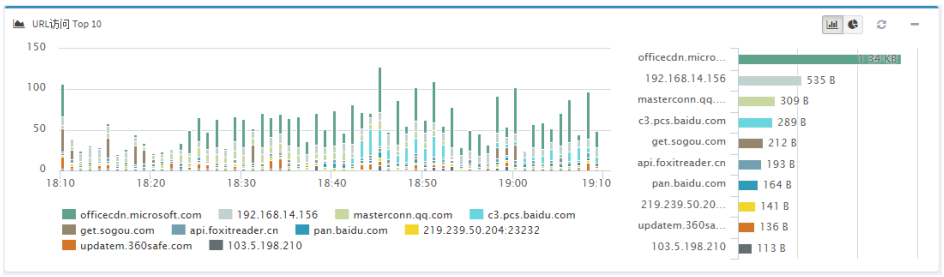
应用流量排行 Top 10 统计展示：



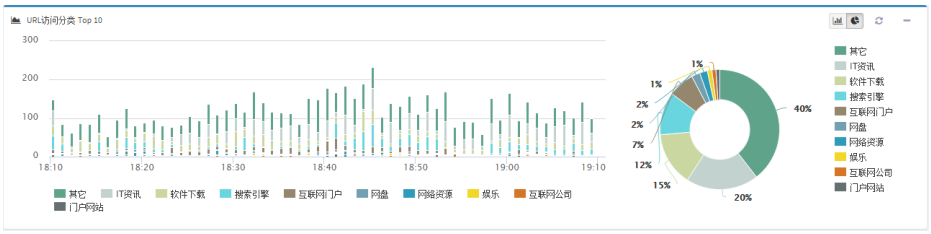
URL 访问分类 Top 10 统计展示：



URL 访问 Top 10 统计展示：



右侧的统计柱形图还可以切换为饼图来查看，以“URL 访问分类 Top 10”为例：



点击**最近 1 小时、最近一天、最近 7 天、最近 30 天**切换监控周期。

点击“导出本页到 PDF”可将整页内容导出成为 PDF 文件，生成的 PDF 文档与当前所看到的统计内容一致，若折叠某一个统计使之在页面不可展示，生成的文件该统计也是折叠状态。

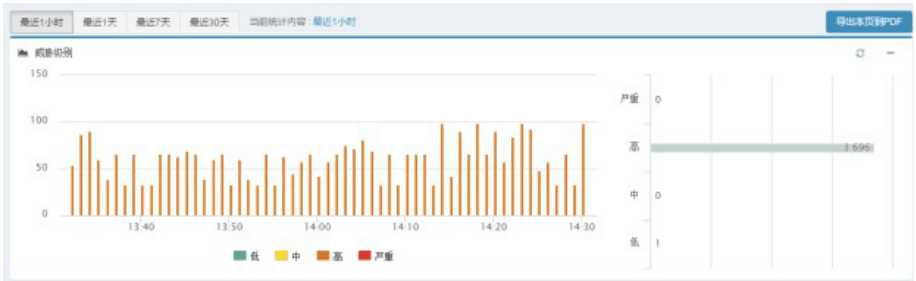
3.3 威胁

查看步骤：

点击 **vCenter>威胁**进入威胁可视化页面，可以查看防火墙设备最近 1 小时、最近 1 天、最近 7 天、最近 30 天的各时间段威胁信息。

统计内容包括威胁级别、威胁类型排行、威胁地图、威胁事件排行 Top 10、威胁源主机排行 Top 10 表格与柱形图、威胁目的主机排行 Top 10 表格与柱形图。

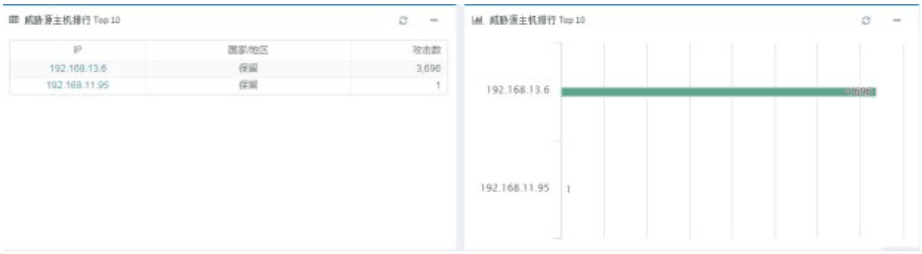
威胁级别 统计展示：



威胁类型排行 统计展示：

威胁地图和威胁事件排行 Top 10 统计展示：

威胁源主机排行 Top 10 表格与柱形图 统计展示：



威胁目的主机排行 Top 10 表格与柱形图 统计展示：

点击**最近 1 小时、最近一天、最近 7 天、最近 30 天**切换监控周期。

点击“导出本页到 PDF”可将整页内容导出成为 PDF 文件，生成的 PDF 文档与当前所看到的统计内容一致，若折叠某一个统计使之在页面不可展示，生成的文件该统计也是折叠状态。

3.4 VCloud

3.4.1 VCloud概述

VCloud 功能主要是通过扫描二维码进行付费，并取得公有云服务器的授权之后，将本地产生的 syslog 日志通过加密或者非加密方式发送到云服务器进行存储。

3.4.2 配置VCloud

进入 **vCenter >VCloud 云日志**

启用：VCloud 开关。

授权状态： 表示没有授权， 表示有授权。

日志类型：发送到服务器的日志类型。

服务器域名：配置了 DNS 服务器地址后，可以通过服务器域名解析出服务器的 IP。

首选 DNS 服务器：**首选** DNS 服务器地址。

备选 DNS 服务器：**备选** DNS 服务器地址。

3.4.3 获取服务器授权

第一步：微信端扫描该二维码或者在小程序端添加设备界面扫描该二维码，如下图：

第二步：扫描该二维码后，会进入添加设备的界面，根据实际情况填写设备名称、设备 sn 号、推荐人手机号，信息填写完毕之后点击提交按钮，如下图：

第三步：提交之后，会在提交成功页面停留 5s，展示添加的设备信息，之后自动返回首页，添加成功的设备会在首页展示

第四步：授权激活的操作，第二步添加设备时，根据填写的推荐人信息，

登陆该小程序，在“推荐人”列表页，找到刚刚添加的 sn 号码，点击“发放试用”按钮，即可完成该设备的激活操作，如下图：

第五步：在小程序端首页，即可查看激活成功的设备，如有日志信息，将在该页面展示该设备的日志数据，如下图：

3.4.4 配置案例

案例描述：

配置 VCloud，使本地产生的系统日志发送到云服务器。

配置步骤：

1. 进入 **vCenter >VCloud 云日志，**

2. 开启 VCloud 开关。
3. 勾选系统和安全选项。
4. 配置服务器域名 t.log.venuscloud.cn。
5. 配置 DNS 服务器地址 114.114.114.114。
6. 点击提交。

3.4.5 常见故障

	日志发送失败，Vcloud配置成功，显示有授权，云服务器收不到日志
	● 本地是否正常生成日志 ● 服务器ip是否可达

4 第4章 系统监控

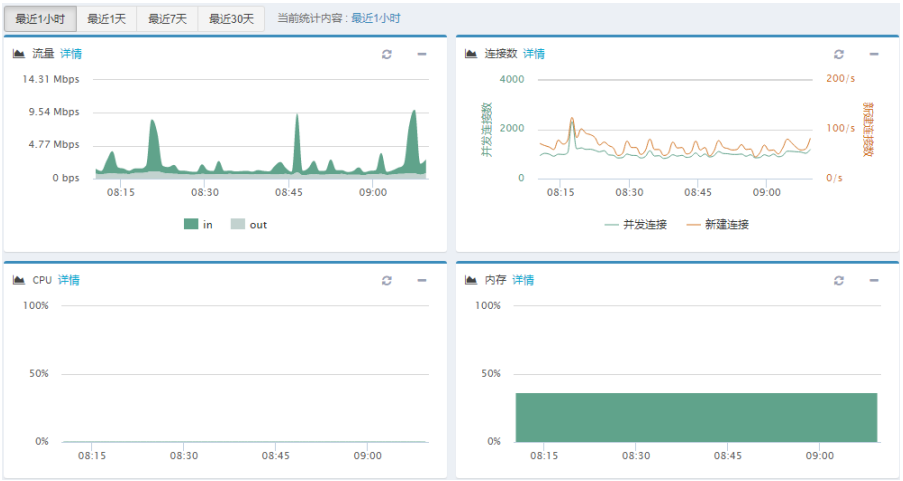
4.1 系统监控概述

通过系统监控功能，可监控防火墙设备的整机流量速率、并发连接与新建连接、CPU 与内存利用率等信息。并可以调整最近 1 小时、最近 1 天、最近 7 天、最近 30 天监控周期以及查看过去 24 小时内的详细数据。

4.2 系统监控

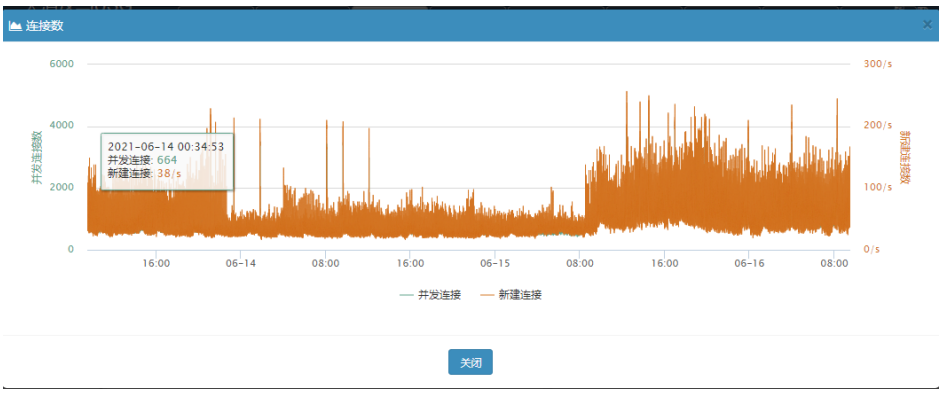
配置步骤：

1. 点击**监控>系统**，进入系统监控页面，可以查看防火墙设备，最近 1 小时、最近 1 天、最近 7 天、最近 30 天的流量、连接数、CPU 利用率、内存利用率信息。



点击**最近 1 小时**、**最近一天**、**最近 7 天**、**最近 30 天**切换监控周期。

分别点击流量、连接数、CPU、内存的**详情**按钮，可以查看过去 24 小时内该信息的详细数据。



5 第5章 接口监控

5.1 接口监控概述

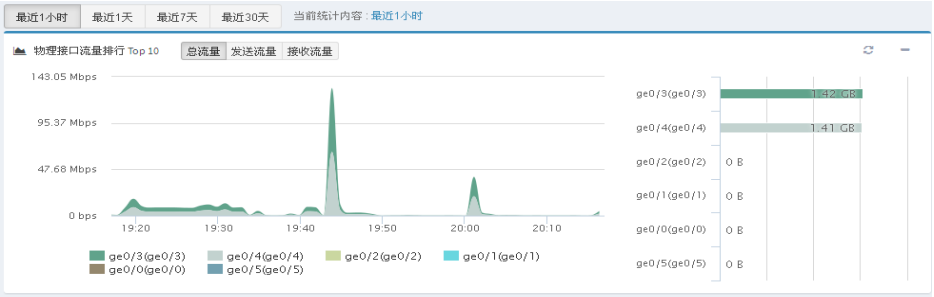
通过接口监控功能，可监控统计防火墙设备的接口流量变化趋势。接口类型包括物理接口、vlan 接口、链路聚合接口，gre 接口，可分别查看这些接口不同历史周期的流量变化情况，在接口详情也可查看接口的实时速率情况。

5.2 接口概览

查看步骤：

1. 点击**监控>接口>概览**，进入接口概览页面，可以查看在统计周期时间内，总流量 Top 10 的十个接口的流量统计，曲线图表示监控周期内的接口流量速率变化，柱状图表示接口监控周期总流量排行。可分别查看“总流量”，“发送流量”，“接收流量”的统计。

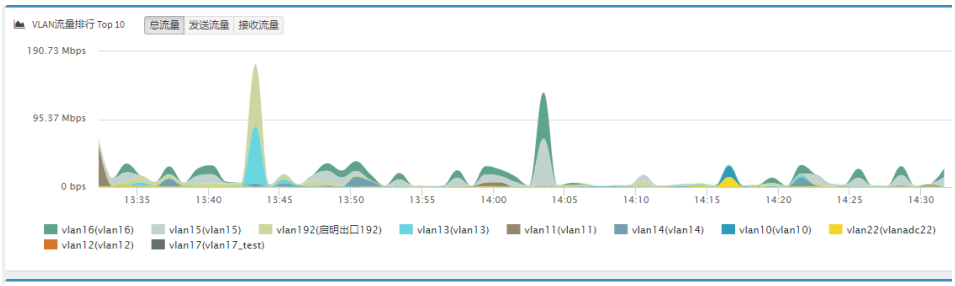
2. 物理接口流量排行 Top 10 统计展示：



点击**最近 1 小时**、**最近一天**、**最近 7 天**、**最近 30 天**切换监控周期。

点击**总流量**、**发送流量**、**接收流量**，切换接口流量流向。

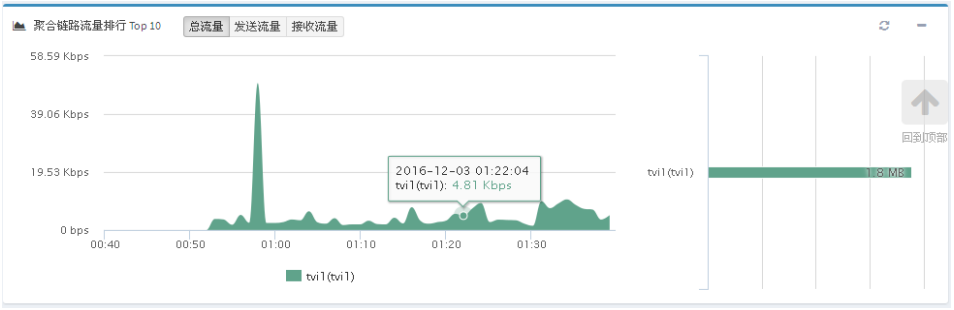
3. VLAN 流量排行 Top 10 统计展示：



点击**最近 1 小时**、**最近一天**、**最近 7 天**、**最近 30 天**切换监控周期。

点击**总流量**、**发送流量**、**接收流量**，切换接口流量流向。

4. 聚合链路流量排行 Top 10 统计展示：



点击**最近 1 小时**、**最近一天**、**最近 7 天**、**最近 30 天**切换监控周期。

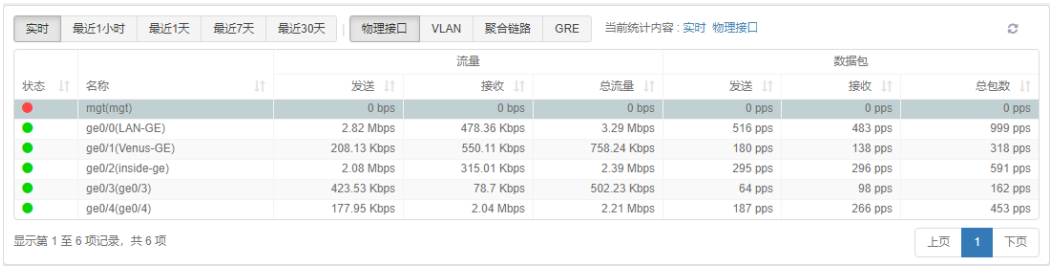
点击**总流量**、**发送流量**、**接收流量**，切换接口流量流向。

5.3 接口详情

查看步骤：

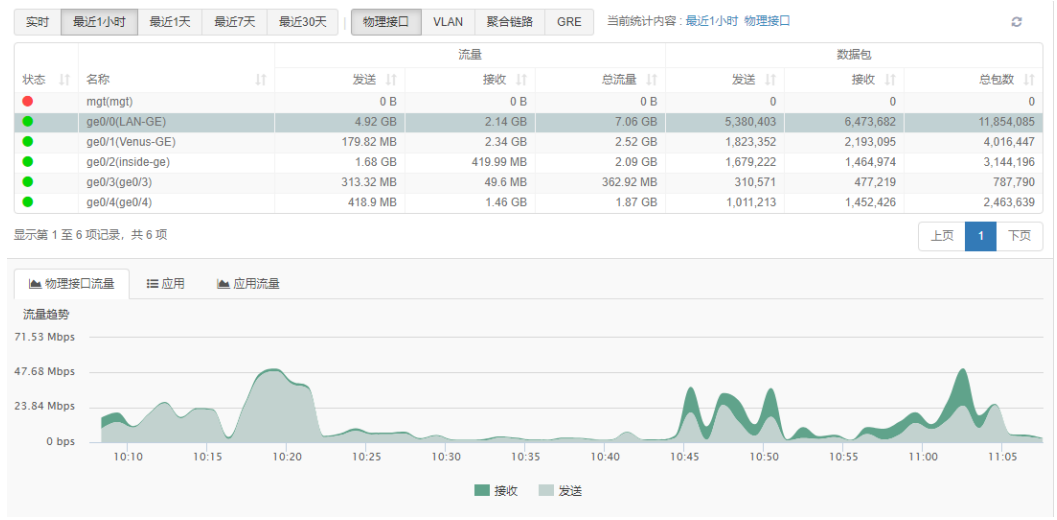
1. 点击**监控>接口>接口详情**，进入接口详情页面，可以查看物理接口、VLAN 接口、聚合链路接口的流量详情，时间周期分别为实时、最近 1 小时、最近 1 天、最近 7 天、最近 30 天。

2. 接口实时速率：



点击**物理接口**、**VLAN**、**聚合链路**，**GRE** 切换不同类型接口的实时速率。

3. 接口历史周期流量：



点击**最近 1 小时**、**最近一天**、**最近 7 天**、**最近 30 天**切换监控周期。

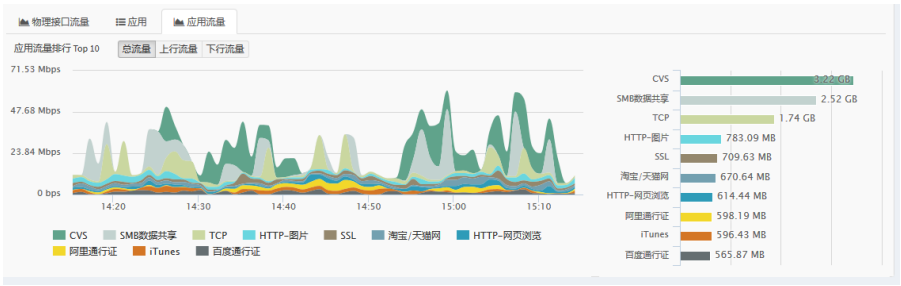
点击**物理接口**、**VLAN**、**聚合链路**，**GRE** 切换接口类型。

点击某一具体接口，查看该接口在统计时间周期内的流量速率曲线和应用流量情况。

4. 选择具体接口进行查询，在下方将会显示该接口的应用流量分布情况。

应用流量列表：

应用流量排行 Top 10 的曲线图和柱形图：



6 第6章 威胁监控

6.1 威胁监控概述

通过威胁监控功能，可监控用户受到威胁的信息。根据最近 1 小时、最近 1 天、最近 7 天、最近 30 天监控周期，监控周期内用户受到威胁的信息，并对攻击信息的级别、类型、事件以及地理分布做了全方位的分析检测，以图表和分布图的方式更直观让用户对威胁源头有了了解。

6.2 威胁概览

查看步骤：

1. 点击**监控>威胁>概览**，进入用户概览页面，可以查看最近 1 小时、最近 1 天、最近 7 天、最近 30 天的威胁统计、威胁地图、威胁主机 Top10 和威胁 Top10 的统计信息，其中包含威胁级别、类型、事件、以及中国地图、世界地图的威胁分布。

2. 威胁级别统计：

点击**最近 1 小时、最近一天、最近 7 天、最近 30 天**切换监控周期。

3. 威胁类型统计：

点击**最近 1 小时**、**最近一天**、**最近 7 天**、**最近 30 天**切换监控周期。

点击**威胁级别**、**威胁类型**，切换统计内容。

4. 威胁主机 Top10 表格展示方式：

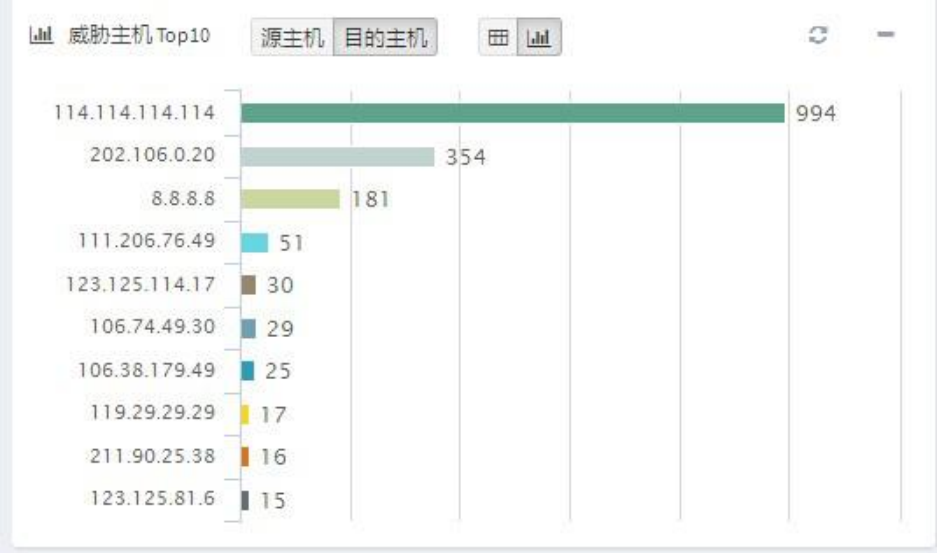
IP	国家/城市	攻击数
114.114.114.114	中国江苏	994
202.106.0.20	中国北京	354
8.8.8.8	美国	181
111.206.76.49	中国北京	51
123.125.114.17	中国北京	30
106.74.49.30	中国内蒙古	29
106.38.179.49	中国北京	25
119.29.29.29	中国广东	17
211.90.25.38	中国河北	16
123.125.81.6	中国北京	15

点击**最近 1 小时**、**最近一天**、**最近 7 天**、**最近 30 天**切换监控周期。

点击源主机、目的主机，切换攻击主机和被攻击主机的统计。

表/图按钮可切换统计展示方式。

5. 威胁主机 Top10 柱形图展示方式：

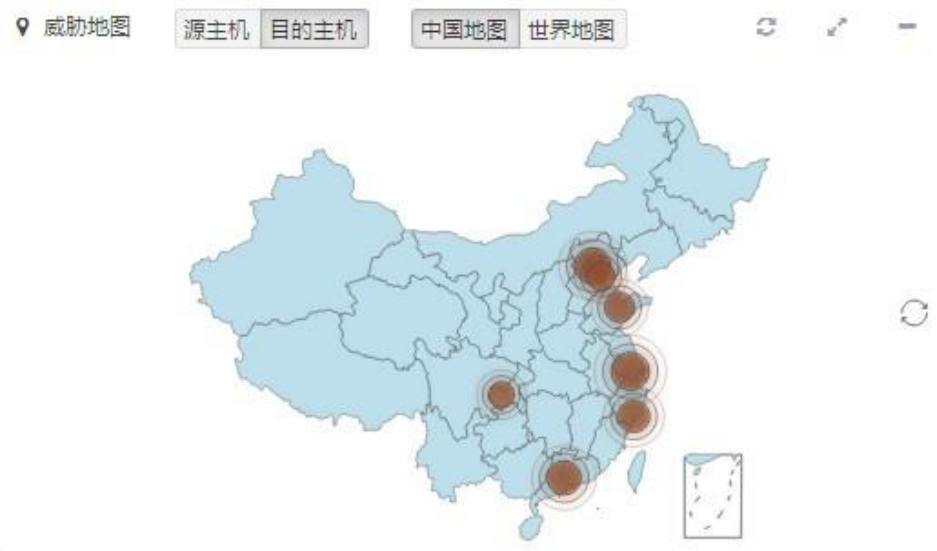


点击**最近 1 小时**、**最近一天**、**最近 7 天**、**最近 30 天**切换监控周期。

点击源主机、目的主机，切换攻击主机和被攻击主机的统计。

表/图按钮可切换统计展示方式。

6. 中国地图威胁目的主机分布：

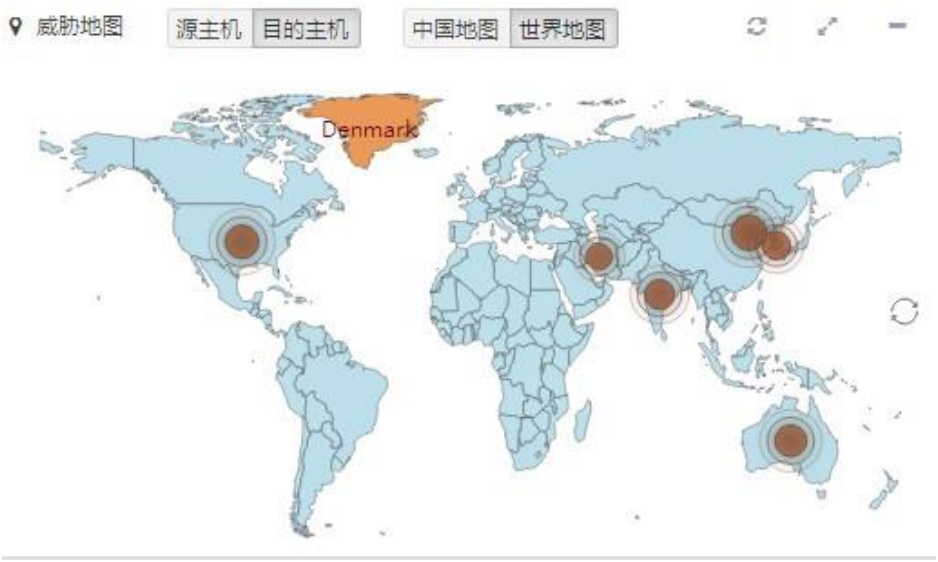


点击**最近 1 小时**、**最近一天**、**最近 7 天**、**最近 30 天**切换监控周期。

点击源主机、目的主机，切换攻击主机和被攻击主机的统计。

中国地图、世界地图页签切换可从不同的地理范围查看攻击情况。

7. 世界地图威胁目的主机分布：

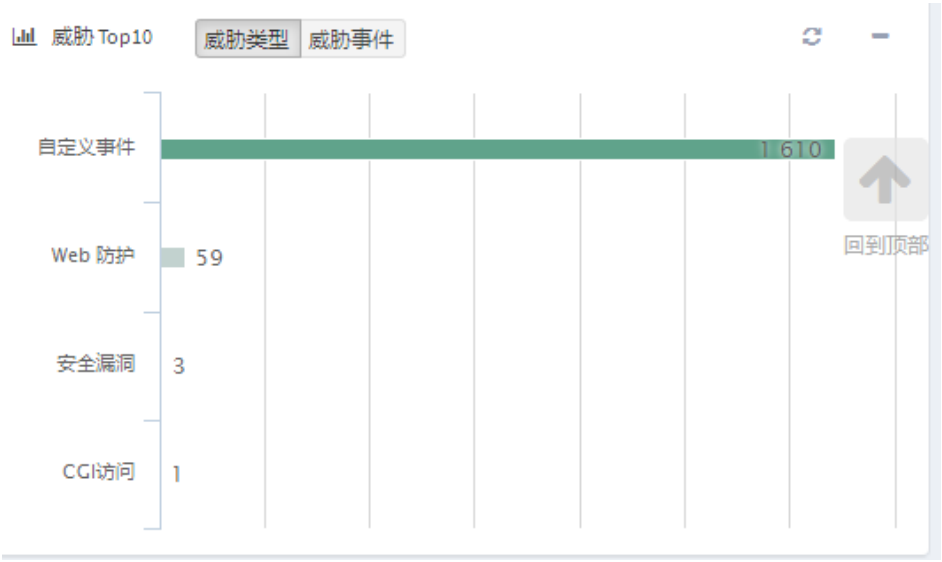


点击**最近 1 小时**、**最近一天**、**最近 7 天**、**最近 30 天**切换监控周期。

点击源主机、目的主机，切换攻击主机和被攻击主机的统计。

中国地图、世界地图页签切换可从不同的地理范围查看攻击情况。

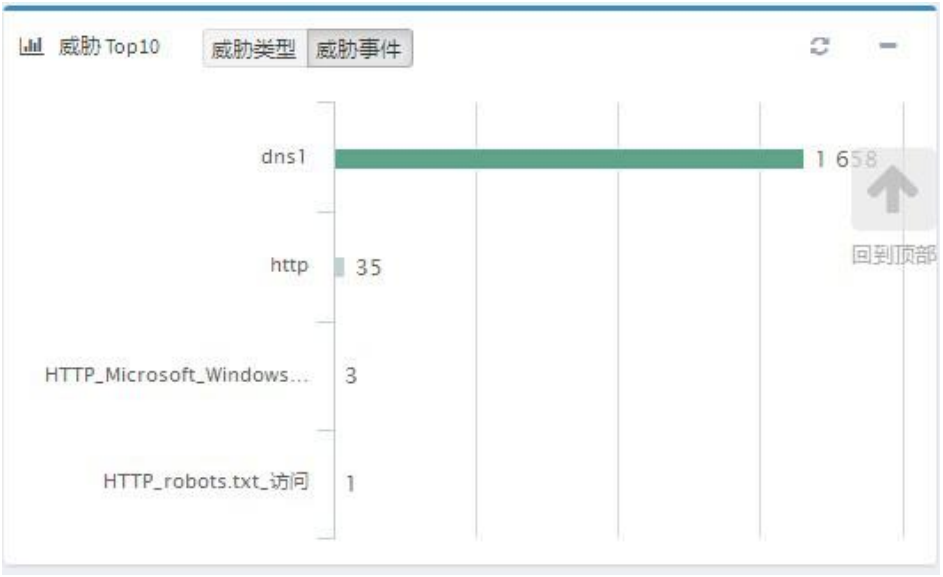
8. 威胁类型 Top10：



点击**最近 1 小时、最近一天、最近 7 天、最近 30 天**切换监控周期。

威胁类型、威胁事件页签切换可切换统计内容。

9. 威胁事件 Top10：



点击**最近 1 小时、最近一天、最近 7 天、最近 30 天**切换监控周期。

威胁类型、威胁事件页签切换可切换统计内容。

6.3 威胁详情

查看步骤：

1. 点击**监控>威胁>威胁详情**，进入**威胁**详情页面，可以查看威胁详细信息。

2. 威胁详情统计：

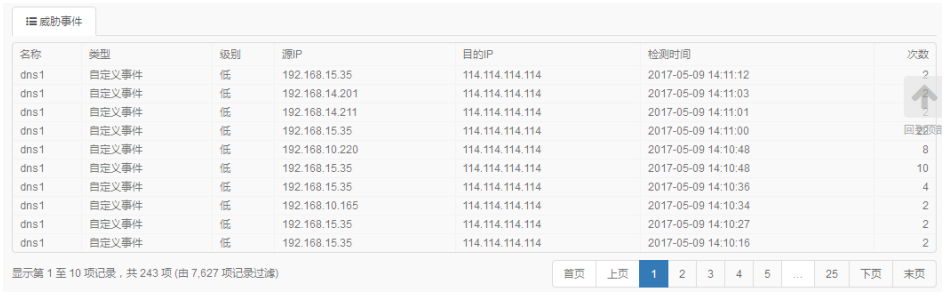
上图是威胁 IP 统计，可以看到威胁 IP 所在地理位置，和威胁级别分布情况。

上图是威胁类型统计，可以看到威胁类型的威胁级别分布情况。

上图是威胁级别统计，可分别查看各威胁级别的威胁总数。

3. 除此之外，点击以上各统计项，在下方都可以查看到符合该统计具体的威胁事件。

威胁事件详情：



上述统计中可查看到，威胁事件所属类型，威胁级别，源 IP，目的 IP 以及检测到威胁的时间，还有这次检测同时检测到的同类事件的次数。


注意

威胁事件的内容是保存在硬盘里的，保存数量的多少取决于硬盘的大小，当威胁数量过多时，会删除最早的数据，所以会出现比较靠前的数据无法查询到的情况。

7 第7章 用户监控

7.1 用户监控概述

通过用户监控功能，可监控用户的流量和会话信息。根据最近 1 小时、最近 1 天、最近 7 天、最近 30 天监控周期，监控周期内总流量的 Top10 用户、并发连接 Top10 用户 IP，并可以分别查看总流量、上行流量、下行流量的 Top10 用户，“用户详情”可以监控用户 IP 的流量 Top100 信息。通过指定用户可以监控不在 topN 中但需要监控的用户 IP。

7.2 用户概览

配置步骤：

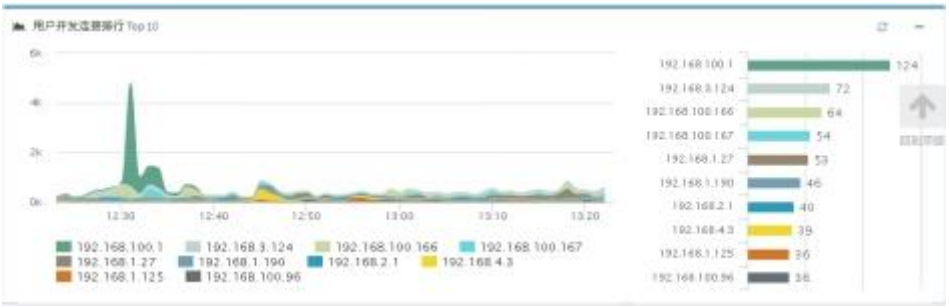
1. 点击**监控>用户>概览**，进入用户概览页面，可以查看经过防火墙的流量，最近 1 小时、最近 1 天、最近 7 天、最近 30 天的流量 Top10 用户 IP，曲线图表示监控周期内的用户 IP 的总流量、发送流量、接收流量速率，柱状图表示用户 IP 总流量、发送流量、接收流量排行。

2. 用户流量排行 Top10：

点击**最近 1 小时**、**最近一天**、**最近 7 天**、**最近 30 天**切换监控周期。

点击**总流量**、**上行流量**、**下行流量**，切换流量类型。

3. 用户并发连接数排行 Top10：



点击**最近 1 小时、最近一天、最近 7 天、最近 30 天**切换监控周期。

7.3 用户详情

配置步骤：

1. 点击**监控>用户>用户详情**，进入用户详情页面，可以查看全部用户或者指定用户 IP 的实时流量速率，最近 1 小时、最近 1 天、最近 7 天、最近 30 天的总流量 Top10 用户 IP 详情。

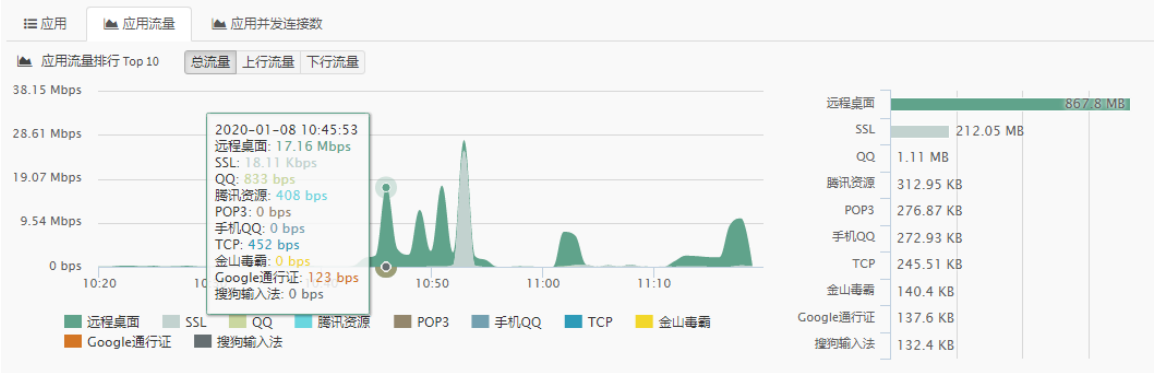
点击**实时、最近 1 小时、最近一天、最近 7 天、最近 30 天**切换监控周期。

点击**全部用户**或者**指定用户**切换监控用户类型

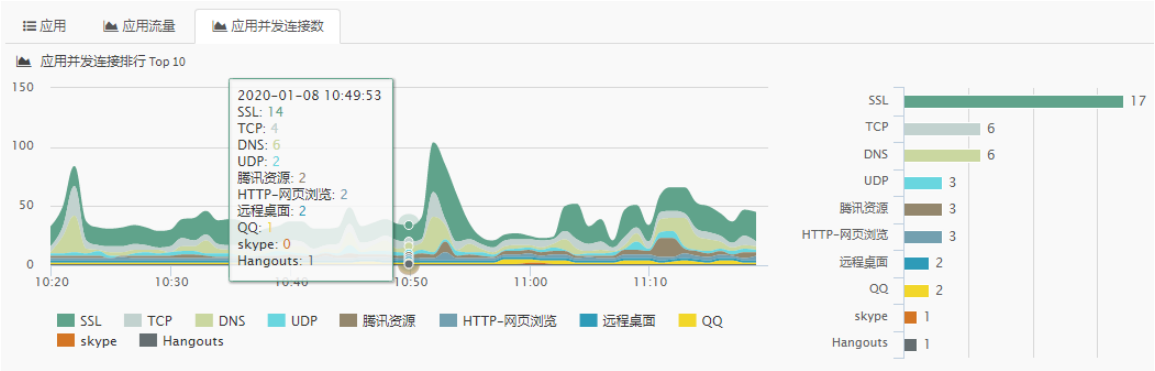
2. 选择具体用户进行查询：在用户的流量排行列表中，点击某用户，在下方将会显示该用户的流量在所有应用上的分布情况。

应用流量列表：

应用流量曲线图和柱形图：



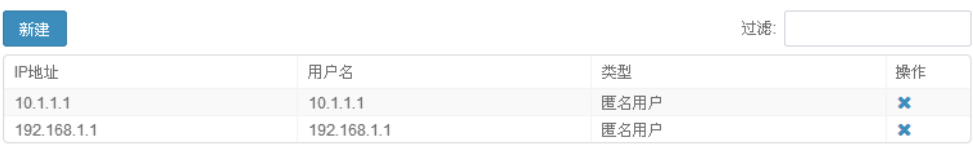
应用并发连接数曲线图和柱形图：



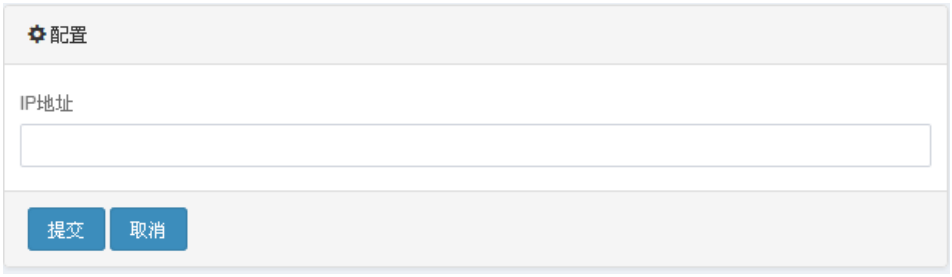
7.4 指定用户

配置步骤：

1. 点击**监控>用户>指定用户**，进入指定用户页面，可以指定用户 IP 流量监控，最多可以添加 50 个指定用户 IP。



2. 点击**新建**添加需要监控流量的指定用户 IP 地址。



3. 填写需要监控的用户 IP，点击**提交**按钮。返回用户详情查看。

8 第8章 应用监控

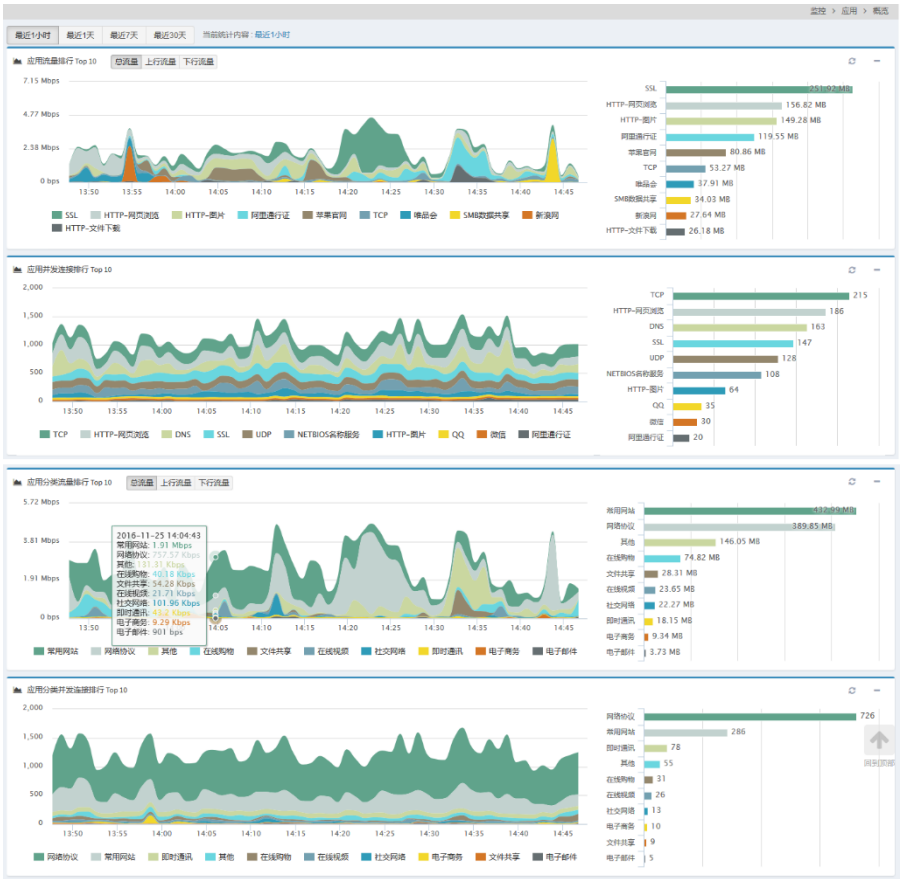
8.1 应用监控概述

通过应用监控功能，可监控统计通过防火墙设备应用的流量信息。根据最近 1 小时、最近 1 天、最近 7 天、最近 30 天监控周期，监控周期内总流量的 top10 应用、并发连接 top10 应用，并可以分别查看总流量、上行流量、下行流量的 top10 应用，以及监控应用的流量 top100 信息。

8.2 应用监控概览

查看步骤：

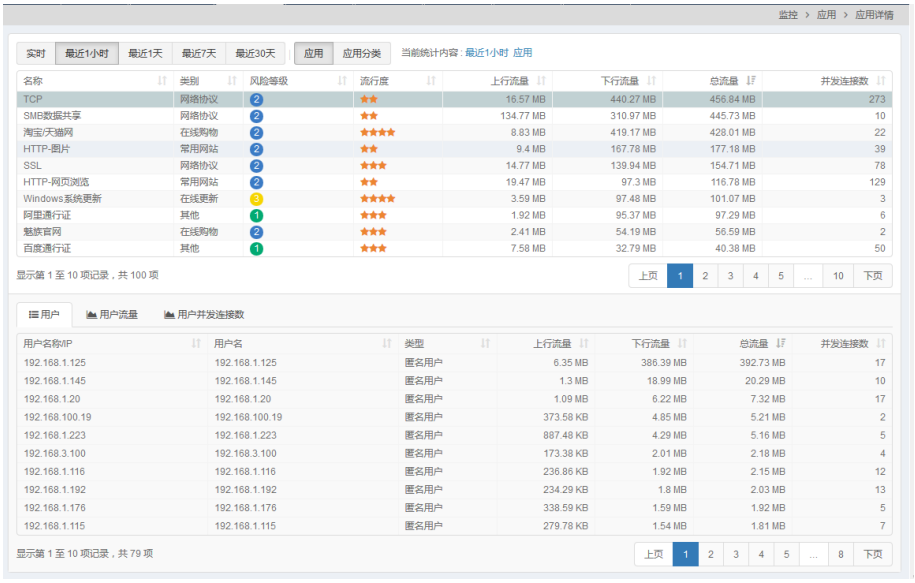
1. 点击**监控>应用>概览**，进入应用监控概览页面，该页面可分别查看应用和应用分类的流量排行和并发连接数排行，可查看最近 1 小时、最近 1 天、最近 7 天、最近 30 天的统计结果。曲线图表示监控周期内的应用的总流量、发送流量、接收流量速率，柱状图表示应用总流量、发送流量、接收流量排行。



8.3 应用统计详情

查看步骤：

1. 点击**监控>应用>应用详情**，进入应用统计详情页面，该页面可查看应用和应用分类最近 1 小时、最近 1 天、最近 7 天、最近 30 天的统计结果以及实时的流量和并发连接数情况，最多显示 100 条记录。



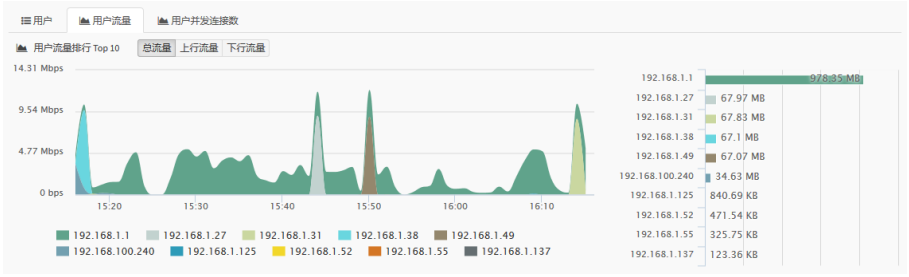
2. 选择类型：包括应用和应用分类。

3. 选择统计时间间隔，其中包括最近 1 小时、最近 1 天、最近 7 天、最近 30 天。

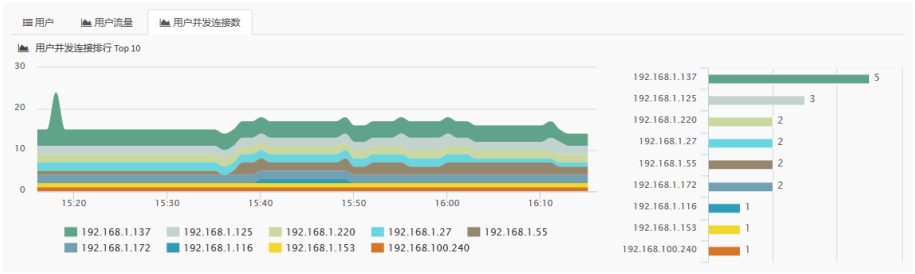
4. 选择具体应用进行查询：在应用或者应用分类的流量排行列表中，点击某应用，在下方将会显示该应用的流量在所有用户 IP 上的分布情况。

   用户流量列表：

   用户流量曲线图和柱形图：



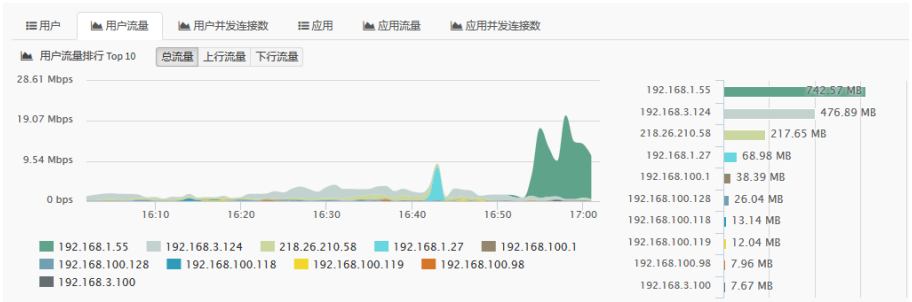
用户并发连接数曲线图和柱形图：



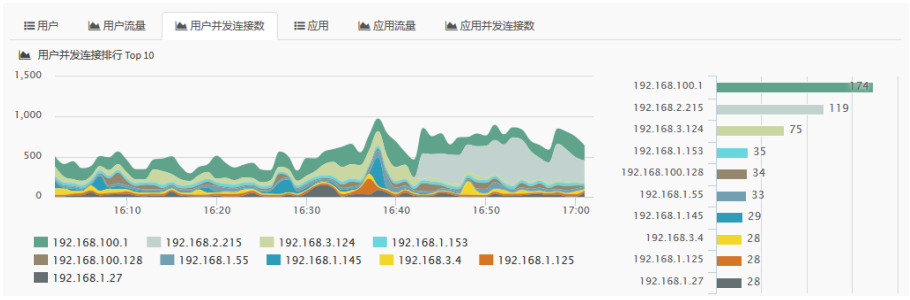
4. 选择具体应用分类进行查询：在应用分类的流量排行列表中，点击某应用分类，在下方将会显示该应用分类的流量和并发连接数分别在所有用户 IP 和该应用分类下具体应用上的分布情况。

用户流量列表：

用户流量曲线图和柱形图：

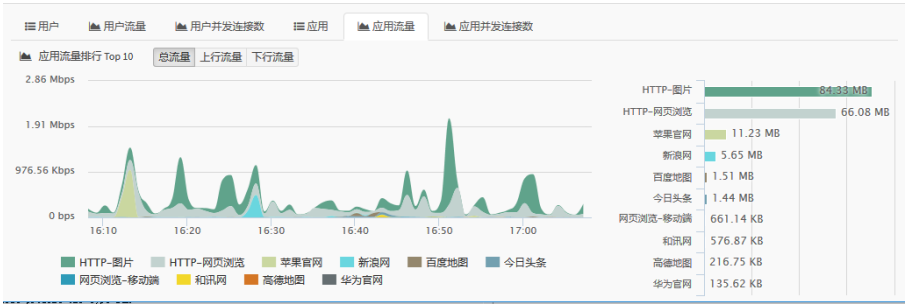


用户并发连接数曲线图和柱形图：

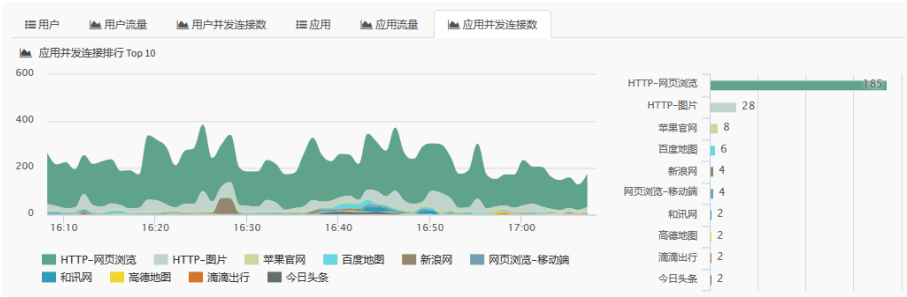


应用流量列表：

应用流量曲线图和柱形图：



应用并发连接数曲线图和柱形图：



5. 查看应用流量实时信息。

在应用详情中选择“实时”，将进入应用流量实时显示页面。该页面显示的是应用或者应用分类的实时流量和并发连接数。


监控 › 应用 › 应用详情
实时
最近1小时
最近1天
最近7天
最近30天
应用
应用分类
当前统计内容：实时 应用
名称 类别 风险等级 流行度 上行流量 下行流量 总流量 并发连接数
TCP 网络协议 2 12.15 Kbps 108.89 Kbps 121.04 Kbps 148
HTTP-网页浏览 常用网站 2 12.41 Kbps 11.6 Kbps 24.02 Kbps 109
QQ 即时通讯 3 2.2 Kbps 16.54 Kbps 18.73 Kbps 31
SSL 网络协议 2 4.3 Kbps 2.58 Kbps 6.88 Kbps 95
DNS 网络协议 2 2.17 Kbps 4.31 Kbps 6.48 Kbps 42
UDP 网络协议 2 3.4 Kbps 952 bps 4.33 Kbps 108
爱奇艺 在线视频 3 928 bps 0 bps 928 bps 23
阿里旺旺 即时通讯 2 0 bps 0 bps 0 bps 1
显示第 1 至 8 项记录，共 8 项
上页 1 下页

9 第9章 流量监控

9.1 流量监控概述

通过流量监控功能，可监控流量控制策略的生效情况。

9.2 流量监控详情

查看步骤：

1. 点击**监控>流控**，进入流控详情页面，该页面可查看在流控策略的作用下，各线路上的实时速率和带宽分配情况。

10 第10章 URL 监控

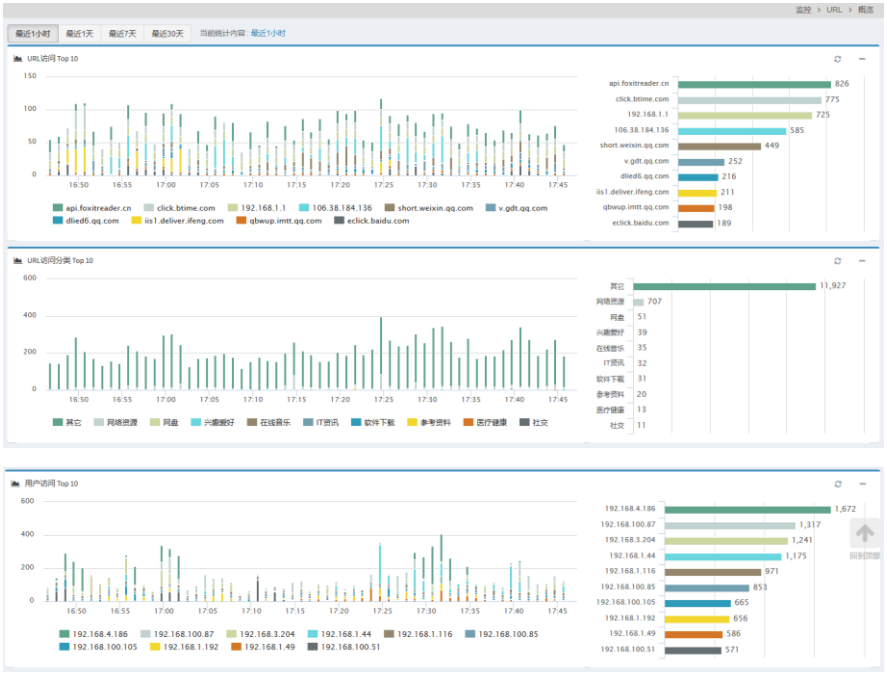
10.1 URL监控概述

通过 URL 监控功能，可监控统计通过防火墙设备访问 URL 的信息。根据最近 1 小时、最近 1 天、最近 7 天、最近 30 天监控周期，监控周期内总访问量 top10 的 URL 和 URL 分类，并可以分别监控 URL、URL 分类、用户访问量 top100 信息。

10.2 URL监控概览

查看步骤：

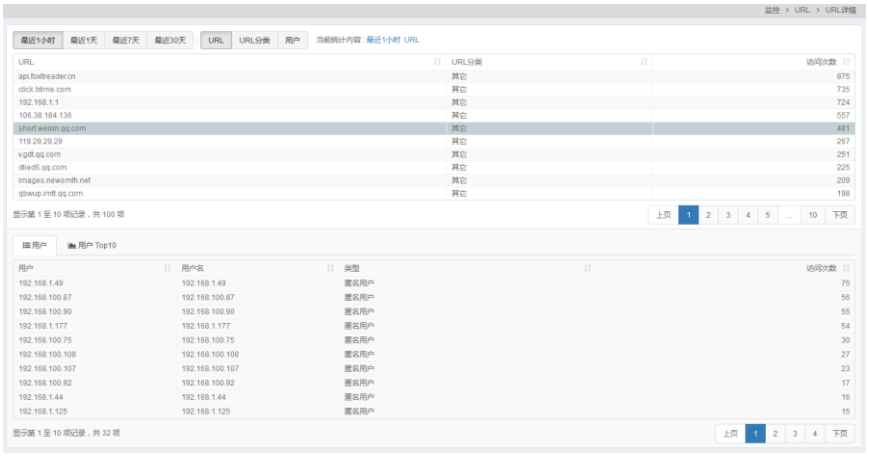
1. 点击**监控>URL>概览**，进入 URL 监控概览页面，该页面可分别查看 URL、URL 分类和用户的 URL 访问排行，可查看最近 1 小时、最近 1 天、最近 7 天、最近 30 天的统计结果。直方图表示监控周期内的 URL 的访问情况，柱状图表示 URL 访问量排行。



10.3 URL统计详情

查看步骤：

1. 点击**监控>URL>URL 详情**，进入 URL 统计详情页面，该页面可查看 URL、URL 分类和用户的 URL 访问最近 1 小时、最近 1 天、最近 7 天、最近 30 天的统计结果，最多显示 100 条记录。



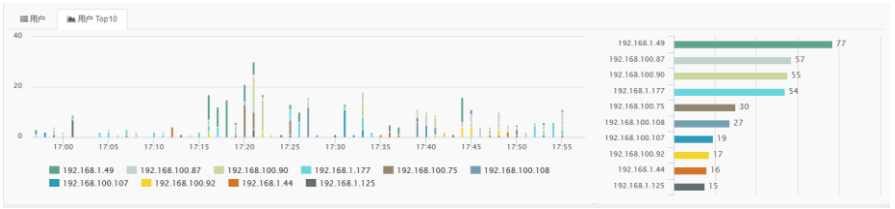
2. 选择类型：包括 URL、URL 分类和用户。

3. 选择统计时间间隔，其中包括最近 1 小时、最近 1 天、最近 7 天、最近 30 天。

4. 选择具体 URL 进行查询：在 URL 的访问量排行列表中，点击某 URL，在下方将会显示该 URL 的访问量在所有用户 IP 上的分布情况。

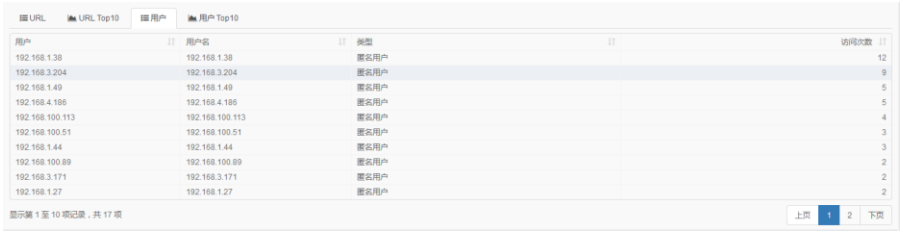
   用户访问量列表：

用户访问量直方图和柱形图：

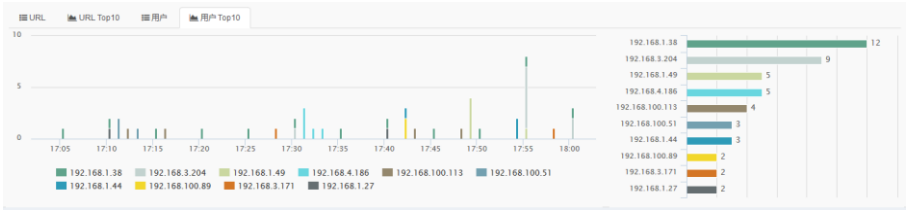


5. 选择具体 URL 分类进行查询：在 URL 分类的访问量排行列表中，点击某 URL 分类，在下方将会显示该 URL 分类的访问量分别在所有用户 IP 和该 URL 分类下具体 URL 上的分布情况。

   用户访问量列表：



用户访问量直方图和柱形图：



URL 访问量列表：

URL 访问量直方图和柱形图：

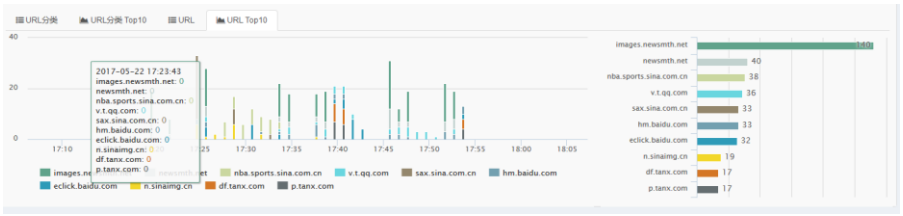
6. 选择具体用户进行查询：在用户的访问量排行列表中，点击某用户，在下方将会显示该用户的访问量分别在 URL 和 URL 分类上的分布情况。

   URL 分类访问量列表：

URL 分类访问量直方图和柱形图：

URL 访问量列表：

URL 访问量直方图和柱形图：



11 第11章 SDWAN 监控

11.1 SDWAN监控概述

通过 SDWAN 控功能，可监控统计基于 SDWAN 策略的各统计数据，包括 SDWAN 链路的链路质量、链路收发速率、WOC 加速统计等。如链路检查获取的延时、抖动、丢包的实时状态和历史统计数据，SDWAN 链路上的实时接收、发送速率等。

11.2 链路质量

配置步骤：

1. 点击**监控>SDWAN>链路质量**，进入 SDW**AN 链路质量**页面。

2. 策略状态：-策略可用，-没有可用下一跳，策略不可用。

3. 下一跳状态：-链路状态可调度，下一跳可用-链路状态不可调度，下一跳不可用。

4. 点击即可对下一跳进行展开和收缩操作。

5. 点击 可以立即刷新显示策略下的隧道信息。

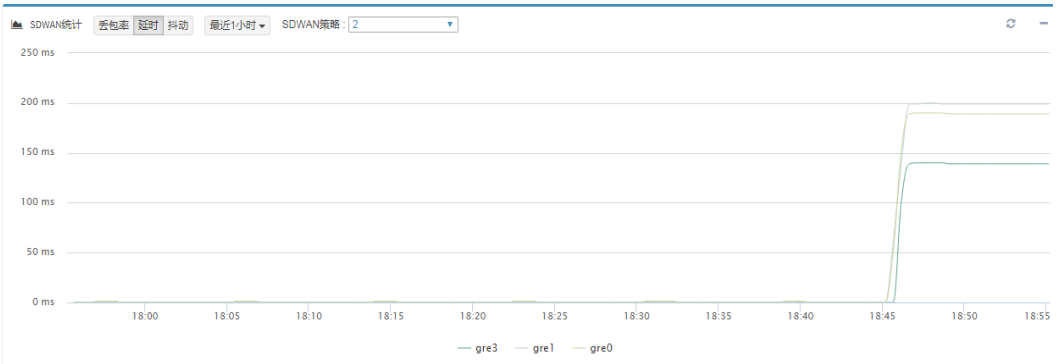
11.3 SDWAN统计

配置步骤：

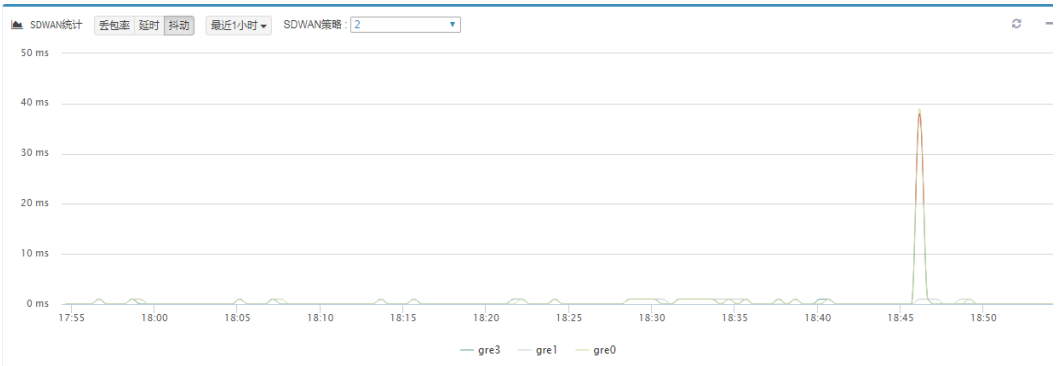
1. 点击**监控>SDWAN>SDWAN 统计**，进入 **SDWAN 统计**页面，该页面根据 SDWAN 策略 ID、统计类型、统计周期展示指定 SDWAN 策略的链路质量统计信息。

2. 统计类型可以选择：丢包率，延时，抖动。

统计类型选择**延时**，如下图：



统计类型选择**抖动**，如下图：



3. 统计周期可以选择：最近 1 小时，最新 1 天，最近 7 天，最近 30 天。

11.4 WOC加速统计

进入**监控>SDWAN>WOC 加速统计**，查看相关的统计数据。


压缩统计
策略名称
原始字节数
压缩字节数
woc
15,112
2,430
显示第 1 至 1 项记录，共 1 项

12 第12章 会话监控

12.1 会话监控概述

通过会话监控功能，可监控统计防火墙设备内所有连接状况;并可根据参数定制查询。会话监控将连接区分为全连接和半连接：当有新建连接长时间未得到应答就会一直处于半连接状态，直至得到正确应答才会转成全连接状态。

12.2 会话统计

配置步骤：

1. 点击**监控>会话>会话统计**，进入会话统计页面，该页面根据下拉菜单中的选项统计系统当前连接数，可根据**源 IPv4 统计、源 IPv6 统计、目的 IPv4 统计、目的 IPv6 统计、目的端口统计**，还可指定详细条件，统计出的连接数按数量降序排列，最多显示前 50 项。

2. 在类型下拉菜单中选择排序条件：**源 IPv4 统计、源 IPv6 统计、目的 IPv4 统计、目的 IPv6 统计、目的端口统计**，默认为按源 IPv4 统计。

3. 在输入框中填写详细的**端口**或 **IP** 匹配条件，可输入 IP 地址/范围/掩码或端口号/范围，如果不输入，默认为全部统计。

4. 点击 搜索 进行统计。

5. 结果显示后，若想查看详细信息，点击 进入标准会话页面查看连接详细信息。

6. 点击  ，配置基于“源 IP”的黑名单阻断。

12.3 标准会话

配置步骤：

1. 点击**监控>会话>标准会话**，进入**标准会话**页面，该页面根据输入的协议、连接类型、地址类型、源/目的 IP、业务端口等条件进行组合查询，显示匹配条件的连接。

2. 在下拉菜单中选择想要监控连接的类型和协议，输入源 IP，目的 IP，业务端口等条件，默认为所有。

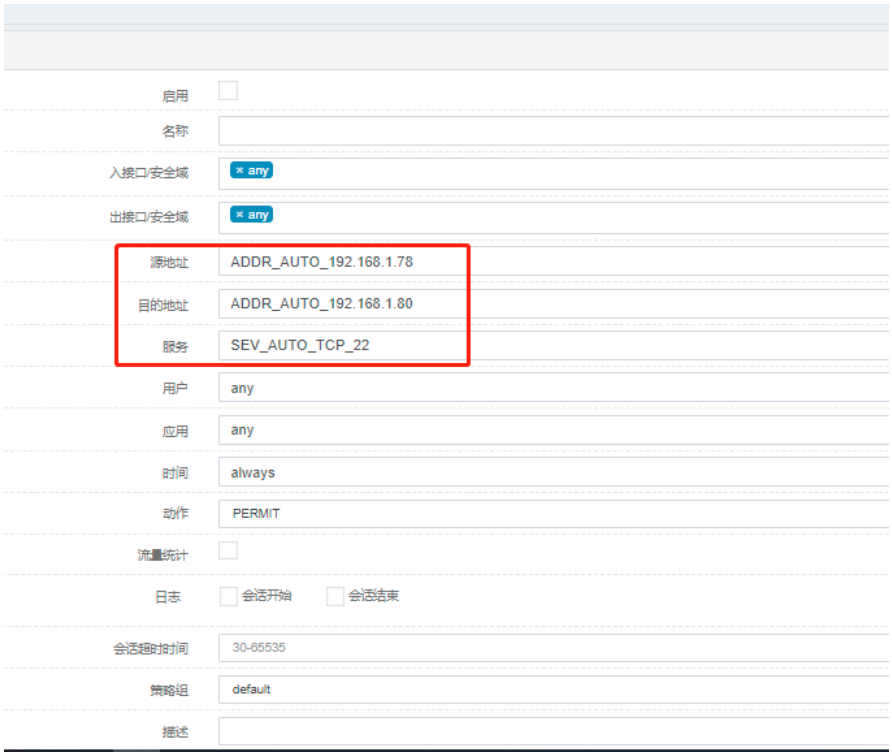
3. 点击  进行查询。

【注】发送源 IP/掩码指过设备做源 nat 以后的地址

4. 点击  ，可以删除当前连接。

5. 点击  按钮，跳转到安全策略新建页面，会根据“源 IP”自动生成源地址对象，“目的 IP”自动生成目的地址对象，“协议和目的端

口” 自动生成服务对象。



配置好其他选项，点击提交即可。

12.4 配置案例

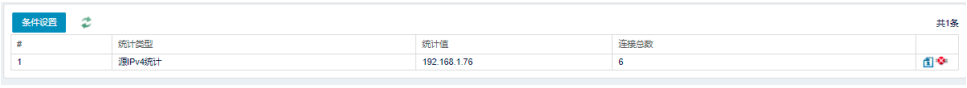
案例 1：源主机连接数

案例描述：

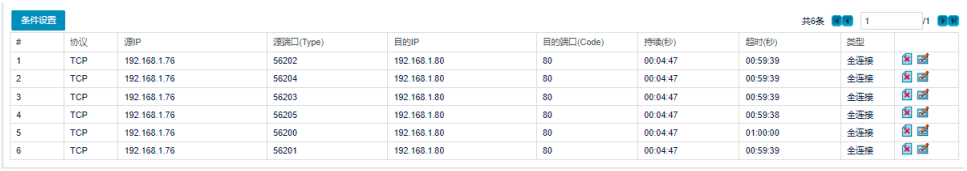
查看源 IP 的连接数量。

配置步骤：

1. 选择类型，源 IPv4 统计。
2. 输入具体 IP 地址。
3. 点击 搜索，查看结果。



4. 点击 按钮，查看详细信息



5. 点击  ，配置基于“源 IP”的黑名单阻断。

案例 2：标准会话连接数

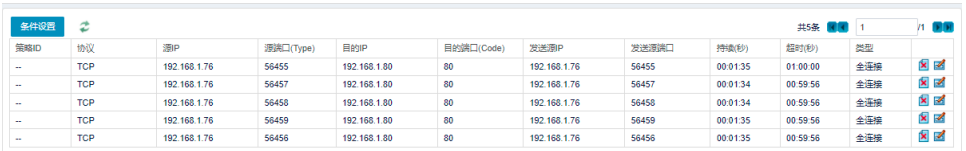
案例描述：

查看源 IP 是 192.168.1.76 的标准会话连接数。

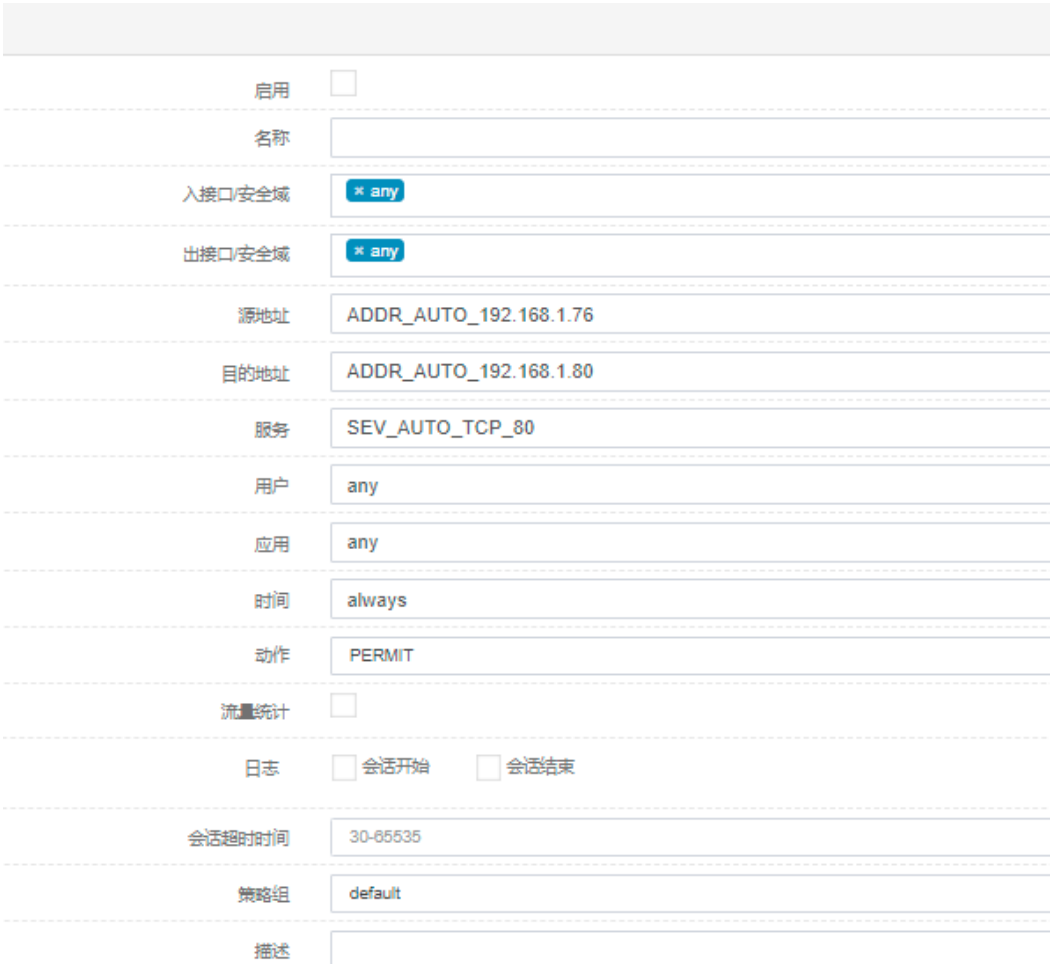
配置步骤：

1. 协议选择 any
2. 连接类型选择所有
3. 地址类型选择 IPv4
4. 源 IP/掩码填 192.168.1.76
5. 发送源 IP/掩码默认
6. 目的 IP/掩码默认
7. 目的端口/范围默认
8. 点击 

按钮



9. 点击  ，生成安全策略


启用
名称
入接口/安全域
any
出接口/安全域
any
源地址
ADDR_AUTO_192.168.1.76
目的地址
ADDR_AUTO_192.168.1.80
服务
SEV_AUTO_TCP_80
用户
any
应用
any
时间
always
动作
PERMIT
流量统计
日志
会话开始
会话结束
会话超时时间
30-65535
策略组
default
描述

13 第13章 流量统计

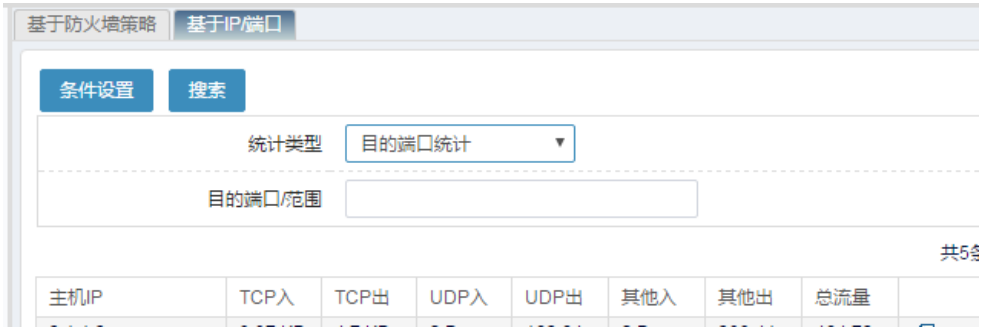
13.1 基于IP/端口流量统计查询

通过 IP/端口，检索查看流量统计。显示结果为基于源 IP 的流量大小排名。

进入**监控>会话>流量统计>基于 IP/端口**，可看到如下界面。输入检索条件，查询流量统计结果。

统计类型：包括主机统计和目的端口统计

地址类型：IPv4/IPv6 地址



目的端口或范围：统计的目的端口或者端口范围，如 100-2410

列表显示关键字释义：

主机 IP：统计的主机地址

TCP 入：TCP 协议流量，反向流量

TCP 出：TCP 协议流量，正向流量

UDP 入：UDP 协议流量，反向流量

UDP 出：UDP 协议流量，正向流量

其他入：其他协议流量，反向流量

其他出：其他协议流量，正向流量

总流量：所有协议双方向流量总和

13.2 配置案例

案例描述

配置过滤条件，查看流量统计。

配置步骤：

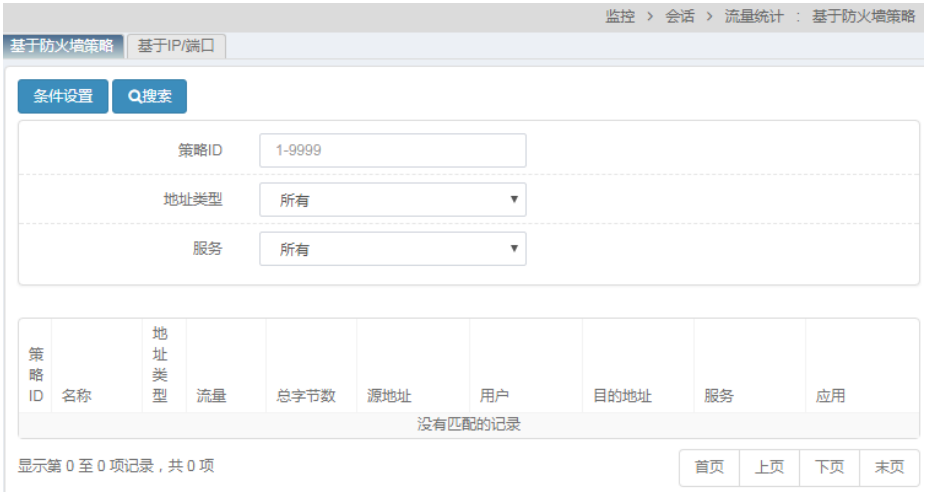
1. 进入**监控>会话>流量统计>基于 IP/端口**，进行过滤条件的设置：

2. 点击搜索，可查看主机的流量统计结果：

13.3 基于策略流量统计

该功能是对配置开启了流量统计的防火墙策略进行流量统计的。

进入**监控>会话>流量统计>基于防火墙策略**，可看到如下界面。可输入检索条件，查询流量统计结果。



策略 ID：需要过滤的策略的 ID 号。

地址类型：IPv4/IPv6 地址。

源地址：填写源地址或者源地址对象的名称关键字。

目的地址：填写目的地址或者目的地址对象的名称关键字。

服务：策略服务类型。

列表显示关键字释义：

策略 ID：显示该项策略的 ID 号。

名称：显示该项策略的名称。

地址类型：显示该项策略的地址类型。

流量：显示通过该项策略的实时流量速率。

总字节数：显示通过该项策略总流量，字节数。

源地址：显示该项策略配置的源地址对象。

用户：显示该项策略配置的用户对象。

目的地址：显示该项策略的目的地址对象。

服务：显示该项策略配置的服务对象。

应用：显示该项策略配置的应用对象。

注意

1. 在需要统计的策略下，开启流量统计，否则无流量统计。
2. 输入检索条件同策略配置保持一致，否则，无流量统计结果。

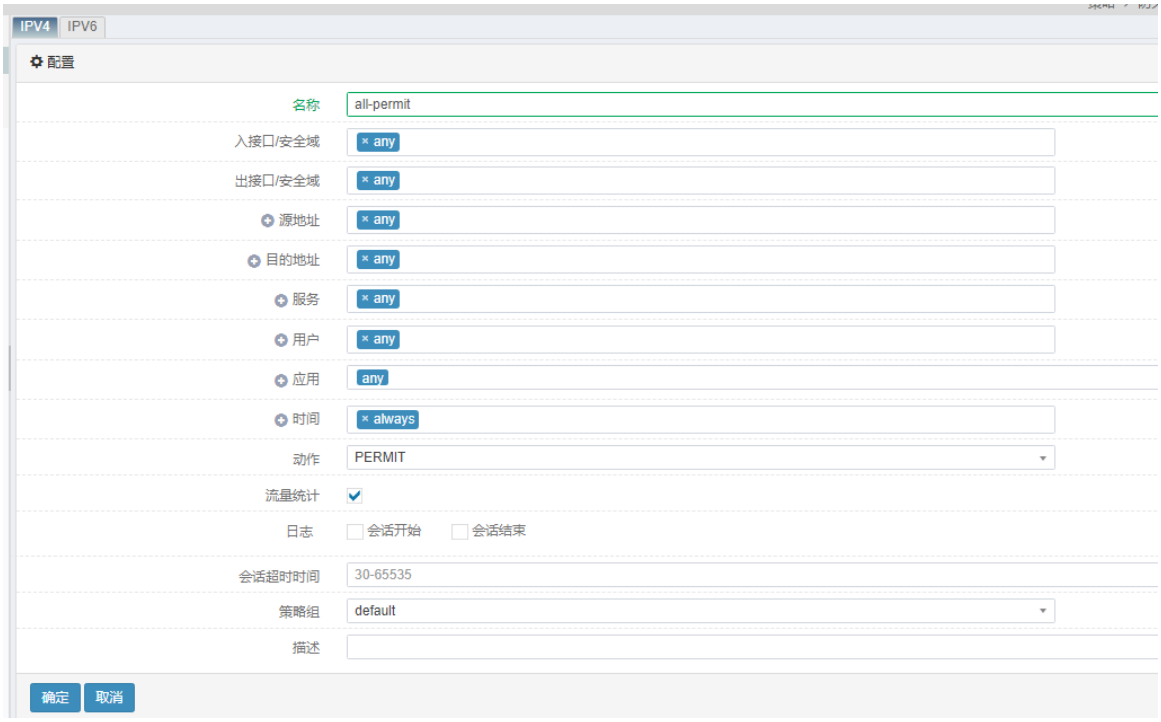
13.4 配置案例

案例描述

配置防火墙策略流量统计，查看统计结果。

配置步骤：

1. 进入**策略>防火墙>策略**，开启策略流量统计功能：



注：只有 PERMIT 类型的防火墙策略可以进行流量统计。

2.进入**监控>会话>流量统计>基于防火墙策略**，输入检索条件，查看策略流量统计结果：

14 第14章 主机监控

14.1 主机监控概述

通过主机监控功能，可监控指定网段的风险信息。根据最近 1 小时、最近 1 天、最近 7 天、最近 30 天监控周期，监控周期内指定网段的主机受威胁事件或非威胁事件的攻击情况，威胁主机页面展示已经受到威胁事件攻击的主机，风险主机页面展示之后可能受到威胁事件攻击的主机。

14.2 威胁主机

配置步骤：

4. 点击**监控>主机>威胁主机**，进入威胁主机展示页面，可以查看关注网段中，最近 1 小时、最近 1 天、最近 7 天、最近 30 天受威胁事件攻击的主机情况。

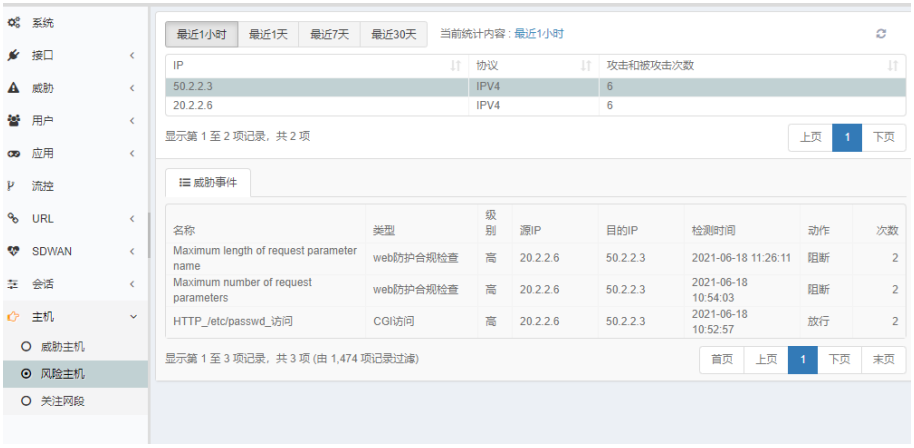
点击**最近 1 小时、最近一天、最近 7 天、最近 30 天**切换监控周期。

5. 选择具体主机进行查询：在主机的受攻击次数排行列表中，点击某主机，在下方将会显示该主机受到的威胁事件攻击的情况。

14.3 风险主机

配置步骤：

3. 点击**监控>用户>风险主机**，进入风险主机展示页面，可以查看关注网段中，最近 1 小时、最近 1 天、最近 7 天、最近 30 未受威胁事件攻击，但有非威胁事件攻击的主机情况。



点击**最近 1 小时、最近一天、最近 7 天、最近 30 天**切换监控周期。

4. 选择具体主机进行查询：在主机的受攻击次数排行列表中，点击某主机，在下方将会显示该主机受到的非威胁事件攻击的情况。

14.4 关注网段

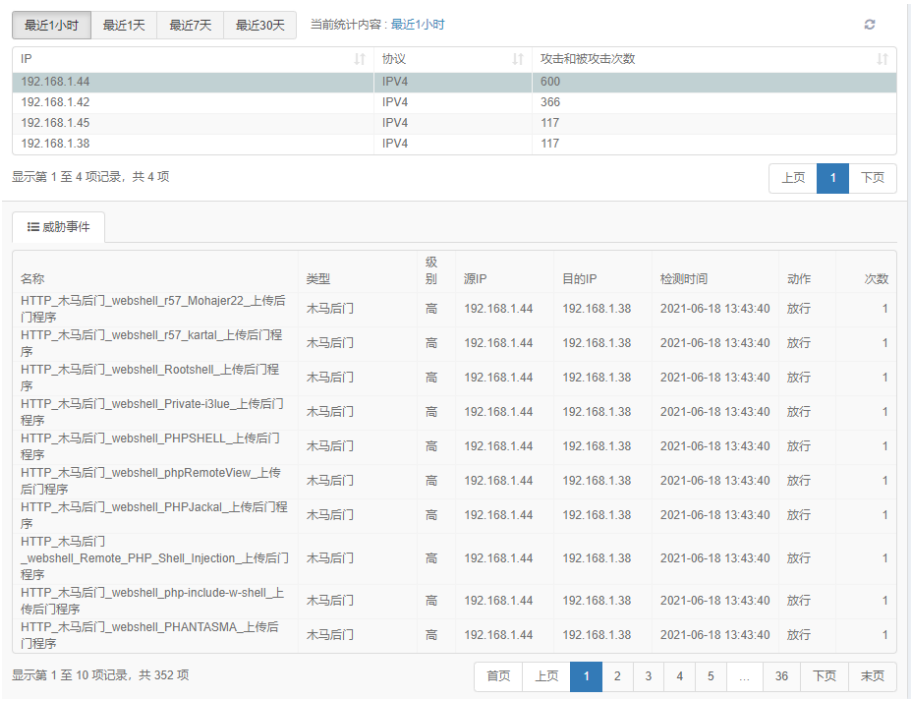
配置步骤：

4. 点击**监控>主机>关注网段**，进入关注网段页面，可以配置需要关注的网段信息，最多可以添加 20 个关注网段。

5. 选择需要监控主机的关注网段类型。

6. 输入需要监控主机的关注网段地址/掩码，点击**添加**。

7. 返回威胁主机或风险主机页面查看。


最近1小时
最近1天
最近7天
最近30天
当前统计内容：最近1小时
IP
协议
攻击和被攻击次数
192.168.1.44 IPV4 600
192.168.1.42 IPV4 366
192.168.1.45 IPV4 117
192.168.1.38 IPV4 117
显示第 1 至 4 项记录，共 4 项
上页 1 下页
威胁事件
名称 类型 级别 源IP 目的IP 检测时间 动作 次数
HTTP_木马后门_webshell_r57_Mohajer22_上传后门程序 木马后门 高 192.168.1.44 192.168.1.38 2021-06-18 13:43:40 放行 1
HTTP_木马后门_webshell_r57_kartal_上传后门程序 木马后门 高 192.168.1.44 192.168.1.38 2021-06-18 13:43:40 放行 1
HTTP_木马后门_webshell_Rootshell_上传后门程序 木马后门 高 192.168.1.44 192.168.1.38 2021-06-18 13:43:40 放行 1
HTTP_木马后门_webshell_Private-i3lue_上传后门程序 木马后门 高 192.168.1.44 192.168.1.38 2021-06-18 13:43:40 放行 1
HTTP_木马后门_webshell_PHPSHELL_上传后门程序 木马后门 高 192.168.1.44 192.168.1.38 2021-06-18 13:43:40 放行 1
HTTP_木马后门_webshell_phpRemoteView_上传后门程序 木马后门 高 192.168.1.44 192.168.1.38 2021-06-18 13:43:40 放行 1
HTTP_木马后门_webshell_PHPJackal_上传后门程序 木马后门 高 192.168.1.44 192.168.1.38 2021-06-18 13:43:40 放行 1
HTTP_木马后门_webshell_Remote_PHP_Shell_Injection_上传后门程序 木马后门 高 192.168.1.44 192.168.1.38 2021-06-18 13:43:40 放行 1
HTTP_木马后门_webshell_php-include-w-shell_上传后门程序 木马后门 高 192.168.1.44 192.168.1.38 2021-06-18 13:43:40 放行 1
HTTP_木马后门_webshell_PHANTASMA_上传后门程序 木马后门 高 192.168.1.44 192.168.1.38 2021-06-18 13:43:40 放行 1
显示第 1 至 10 项记录，共 352 项
首页 上页 1 2 3 4 5 ... 36 下页 末页

15 第15章 资产防护

15.1 资产防护概述

资产防护的目的是探测网络中的 IP 设备或者叫资产（主要是 IOT 设备，比如打印机、摄像头等），并对这些资产起到保护作用。此类设备一般网络防护能力比较差，容易遭受攻击，通过定期去探测此类设备的指纹信息，并对比前后扫描的结果，如果发现指纹信息发生明显改变，说明 IOT 设备可能遭受到网络攻击，此时把这个设备的 IP 加入黑名单，从而保证网络的安全。

资产防护还包括交换机联动、指纹管理、行为学习功能。

通过配置交换机联动能通过 SNMP 协议获取指定交换机的 IP-MAC 对应关系，并添加到自己的 IP-MAC 表中。

通过配置指纹管理可以通过扫描资产列表中的资产，获取到资产的类型、厂商和操作系统。

指纹管理分为预定义指纹库和自定义指纹两种配置方式

通过行为学习功能，可以展示在一段时间内经过设备的并且是设备所关注的连接，可以根据协议或主机进行查看，还可以对某条连接进行抓包和生成策略等操作。

15.2 配置资产防护

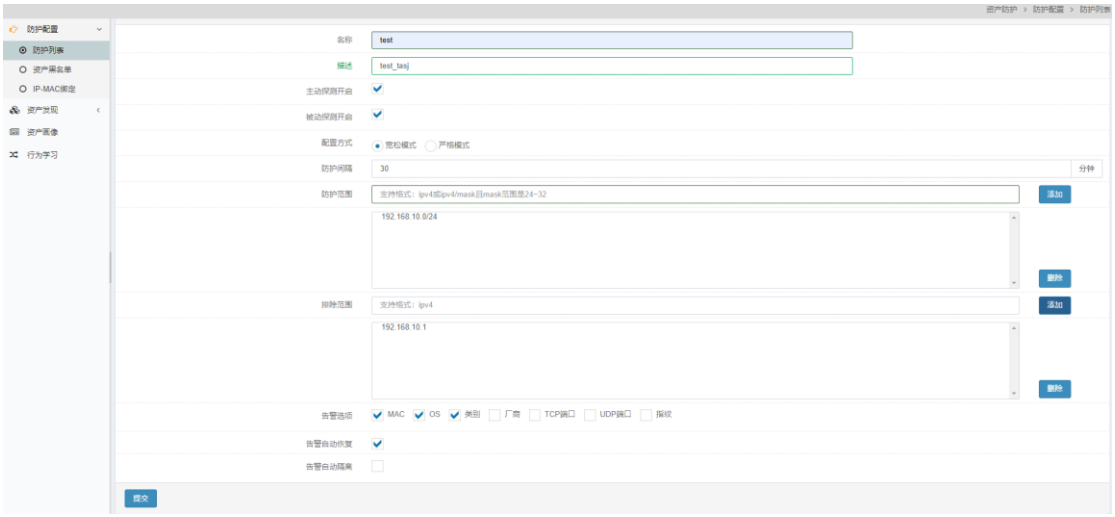
15.2.1 防护配置

1. 防护列表

防护列表是对网络中的资产进行防护的一种策略配置，包括防护模式、防护网段和告警模式等相关配置。通过防护模式和防护网段的配置，达到灵活的资产管理和防护目的。防护列表的配置如下图所示：

防护列表可以新建（最多配置 8 个防护任务）、修改和删除，当删除防护列

表某个任务时，相应防护网段的资产也将删除，其中新建页面如下图所示：



名称：防护任务的名称；

描述：防护任务的描述；

主动探测开启：主动探测开关；

被动探测开启：被动探测开关；

配置方式：可选宽松模式（资产缺省放行，审批后如检测到状态变更，则产生告警）或者严格模式（资产缺省隔离，审批后放行，如检测到状态变更则产生告警并隔离）；

防护间隔：主动探测时间间隔，5-30000 分钟；

防护范围：防护资产的 IP 网段，最多配置 8 个网段，最小配置 24 位掩码；

排除范围：不被探测的资产 IP，最多添加 32 个；

告警选项：能产生告警的资产指纹信息；勾选后的指纹信息发生变更会产生告警；

告警自动恢复：指纹信息变更后告警，又变更回审批时的状态，则解除告警；

告警自动隔离：告警后是否自动加入黑名单。如果是严格模式，只能选择自动隔离。

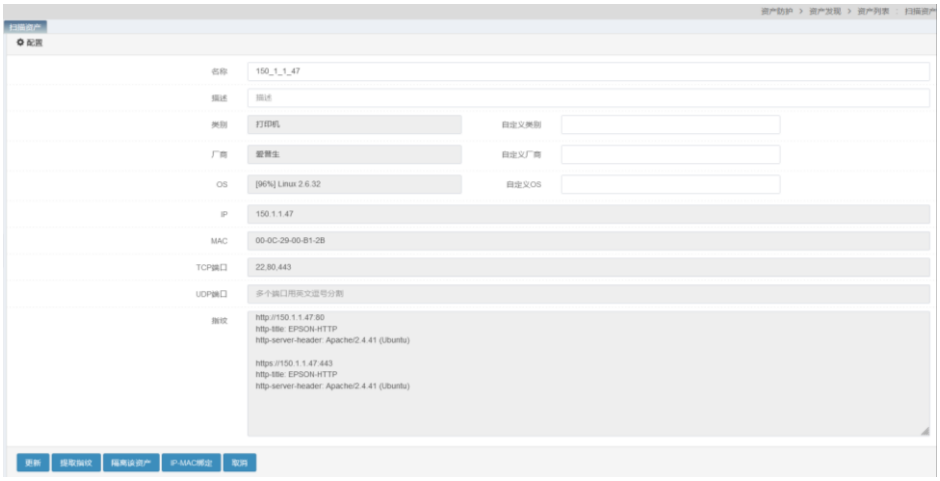
15.3 配置资产黑名单

15.3.1 配置资产黑名单

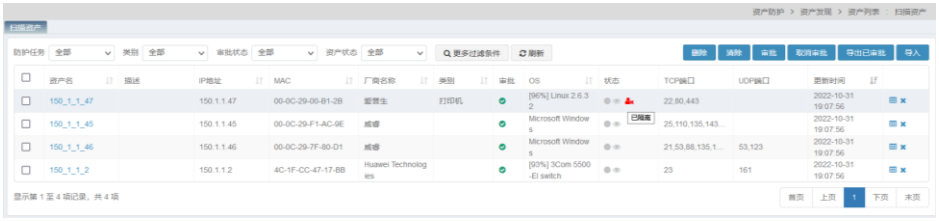
配置步骤：

1. 进入**资产防护>资产发现>资产列表**，在**扫描资产**的显示列表下通过点击

资产名进入资产修改页面，如下图：



2. 点击**隔离该资产**后，如下图：



此时对应资产名的**状态**列会显示 已隔离图标。

3. 进入**资产防护>防护配置>资产黑名单，**选择**配置，**显示对应生成的黑名单，如下图：

地址：通过隔离生成黑名单的资产 IP。

开始时间 ：黑名单配置创建时的系统时间。资产防护阻断方式添加的黑名单有效时间为永久，因此资产黑名单中显示为永久。

结束时间 ：黑名单生效周期结束的时间。资产防护阻断方式添加的黑名单有效时间为永久，因此资产黑名单中显示为永久。

剩余生效时间：黑名单剩余的生效时间。资产防护阻断方式添加的黑名单有效时间为永久，因此资产黑名单中显示为永久。

添加方式：黑名单的添加方式。资产黑名单的添加方式显示为资产防护阻断。

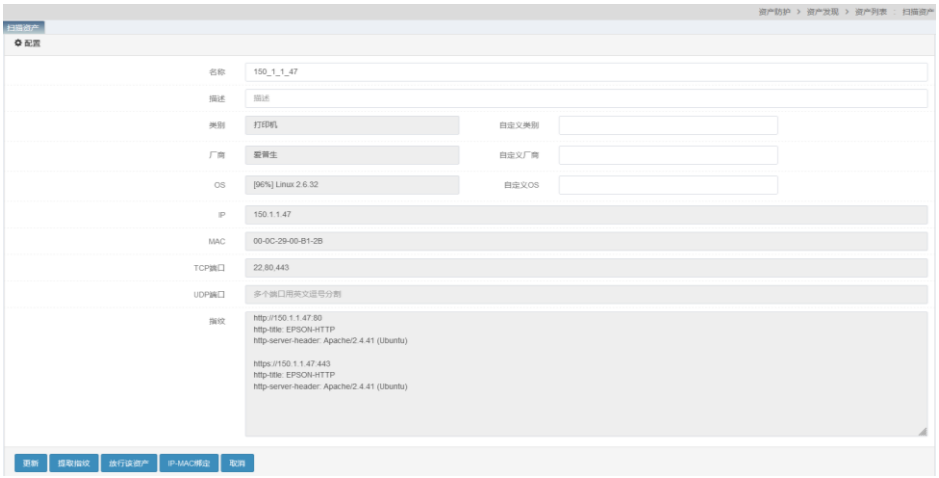
所在组：黑名单所属组的名称。资产黑名单创建后固定加入至黑名单内置组，组名为”abnormal_assets_block”。

命中：匹配黑名单 IP 地址的命中数。

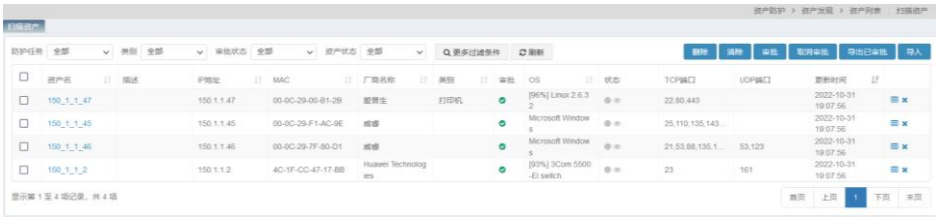
15.3.2 放行删除资产黑名单

配置步骤：

1. 进入**资产防护>资产发现>资产列表**，在**扫描资产**的显示列表下通过点击资产名进入资产修改页面，如下图：



2. 点击**放行该资产**后，如下图：



此时对应资产名的**状态**列的隔离状态已消失。

3. 进入**资产防护>防护配置>资产黑名单**，选择**配置，**显示相应的黑名单在放行资产操作后被随之删除。

15.3.3 手动删除资产黑名单

配置步骤：

1. 进入**资产防护>防护配置>资产黑名单**，选择**配置，**如下图：

2. 点击 删除某条资产黑名单配置，或者点击 删除全部资产黑名单配置。

3. 进入**资产防护>资产发现>资产列表**，在**扫描资产**的显示列表，显示相应资产黑名单所对应的资产在手动删除黑名单后，对应资产名的**状态**列的隔离状态已消失。

15.3.4 重置资产黑名单命中数

配置步骤：

1. 进入**资产防护>防护配置>资产黑名单**，选择**配置**，如下图：

2. 点击 重置某条资产黑名单已有命中数，或者点击 清除命中 重置全部资产黑名单列表下黑名单命中数。

15.3.5 查询资产黑名单配置

配置步骤：

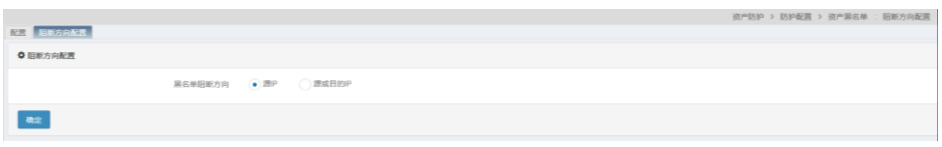
1. 进入**资产防护>防护配置>资产黑名单，**选择**配置**，如下图：

2. 在查询输入框输入需要查找的资产黑名单的 IP 地址，点击 进行查找。

15.3.6 设置资产黑名单阻断方向

配置步骤：

1. 进入**资产防护>防护配置>资产黑名单，**选择**阻断方向配置**，设置黑名单的阻断方向，如下图：



源 IP：选择流经报文的源 IP 进行资产黑名单匹配命中。

源或目的 IP：对流经报文先进行源 IP 的黑名单匹配，若未命中，再进行目的 IP 的资产黑名单匹配。

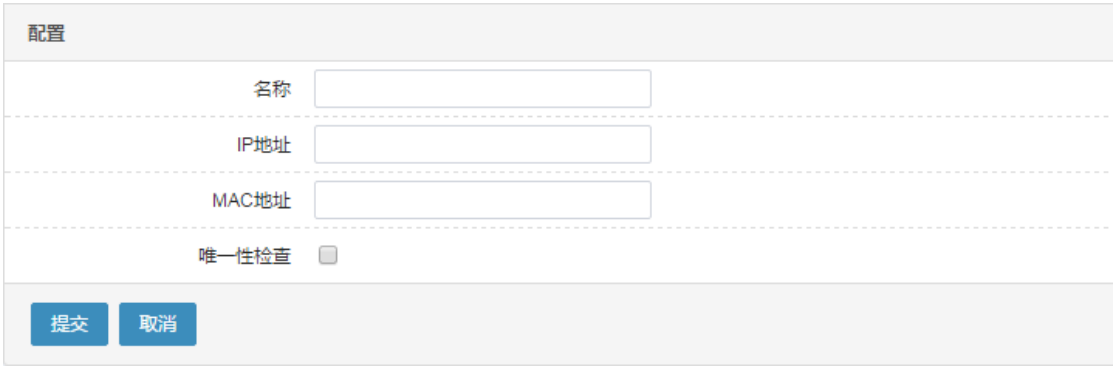
15.4 配置IP-MAC绑定

15.4.1 配置IP-MAC绑定

配置步骤：

1. 进入防护配置**>IP-MAC 绑定**

点击**新建**：



参数说明：

名称：IP-MAC 绑定的名称

IP 地址：IP-MAC 中的 IP 地址

MAC 地址：IP-MAC 中的 MAC 地址

唯一性检查：选定后，一个 MAC 只能与一个 IP 地址绑定

2. 点击**提交**：完成设置

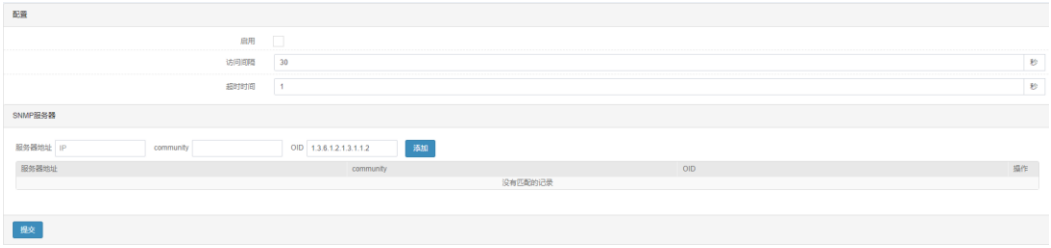
15.5 配置交换机联动

15.5.1 配置的基本要素

交换机联动的基本要素有访问间隔、超时时间、SNMP 服务器和动作。SNMP 服务器包括服务器地址、community 和 OID。

配置步骤：

1. 进入**资产防护>资产发现>交换机联动**。



参数说明：

启用：启用交换机联动。

访问间隔：交换机联动发送 SNMP 查询数据包的间隔时间，单位为秒。

超时时间：发送的 SNMP 查询数据包在此时间内没收到回应包，则此次交换机联动查询失败，单位为秒。

服务器地址：要进行联动的交换机的 IP 地址。

community：SNMP 代理认证的密码。

OID：对象标识符，是 SNMP 代理提供的具有唯一标识的键值。

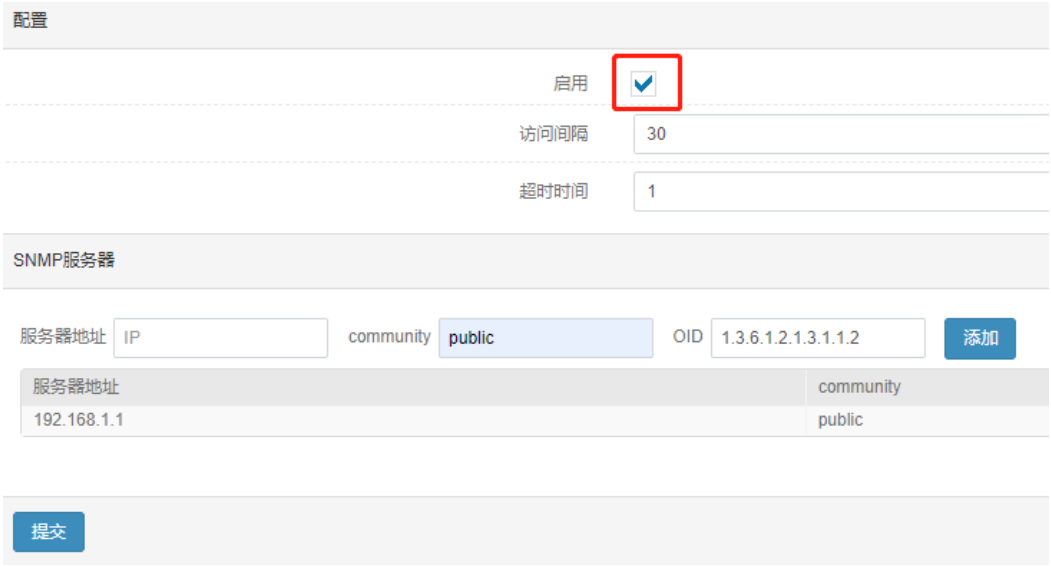
2. 配置完毕后，点击**提交**。

15.5.2 启用交换机联动

配置好的交换机联动必须启用才能使其生效。

配置步骤：

1. 进入**资产防护>资产发现>交换机联动**，在配置页面直接启用，如下图：



2. 勾选**启用**可以启用交换机联动所有已添加的监控范围。

注意

交换机联动缺省为不启用，配置后必须手工启用才能使其生效。

15.5.3 删除SNMP服务器

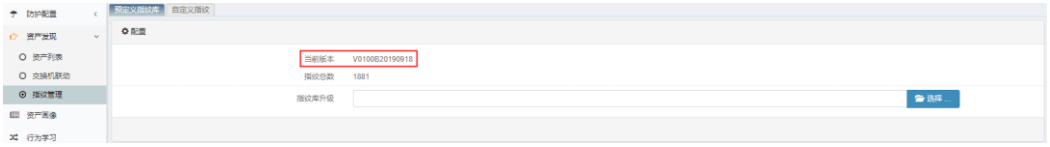
配置步骤：

1. 进入**资产防护>资产发现>交换机联动**，如下图：

2. 点击✖删除 SNMP 服务器，然后点击**提交**。

15.6 配置预定义指纹库

15.6.1 预定义指纹库版本



当前预定义指纹库的版本。

15.6.2 预定义指纹库总数

当前预定义指纹库中的指纹总数。

15.6.3 预定义指纹库升级

配置步骤：

1. 进入**资产防护>资产发现>指纹管理>预自定义指纹库**。
2. 点击**选择**，选择要导入的指纹库。

3. 点击**升级**。

预定义指纹库升级的文件必须是 zip 压缩文件。

预定义指纹库升级会覆盖已有的预定义指纹。

15.7 配置自定义指纹

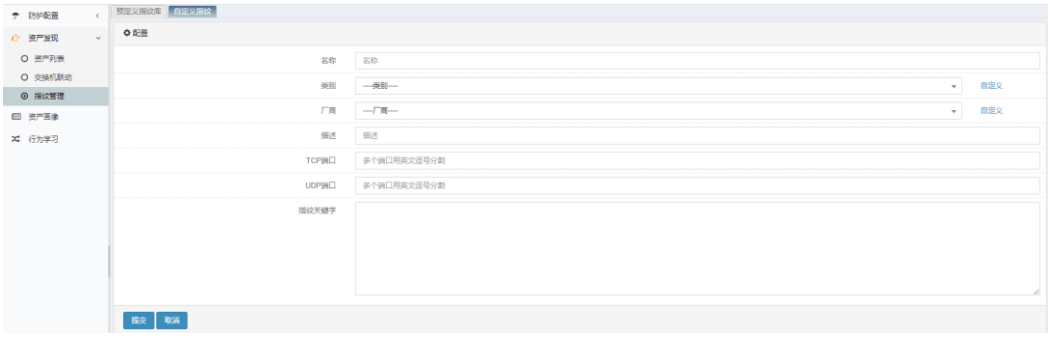
15.7.1 配置的基本要素

自定义指纹的基本要素有名称、类别、厂商、描述、TCP 端口、UDP 端口和指纹。其中，名称、类别、厂商不能为空，且类别和厂商可以选择已有的类别名和厂商名，也可以自定义；TCP 端口、UDP 端口和指纹至少有一个不为空。

配置步骤：

1. 进入**资产防护>资产发现>指纹管理>自定义指纹**，如下图：

2. 点击新建添加自定义指纹，如下图：



参数说明：

名称：显示该项配置的名称；

类别：资产的类型；

厂商：生产此硬件设备的厂商；

描述：关于该自定义指纹的描述，可以是中文，不得超过 63 个字符；

TCP 端口：要扫描的 TCP 端口，端口范围为 1-65535，多个端口用英文逗号分隔；

UDP 端口：要扫描的 UDP 端口，端口范围为 1-65535，多个端口用英文逗号分隔；

指纹关键字：硬件设备回复数据包中的数据特征。

3. 配置完毕后，点击**提交**。

注意 这里的指纹指的是数据包中的数据特征。

15.7.2 编辑自定义指纹

配置步骤：

1. 进入**资产防护>资产发现>指纹管理>自定义指纹**，对某条存在的自定义指纹配置点击名称进入编辑页面。

2. 可以对自定义指纹里面的内容进行编辑修改，修改完毕后点击**提交**。

15.7.3 删除自定义指纹

配置步骤：

1. 进入**资产防护>资产发现>指纹管理>自定义指纹**，如下图：

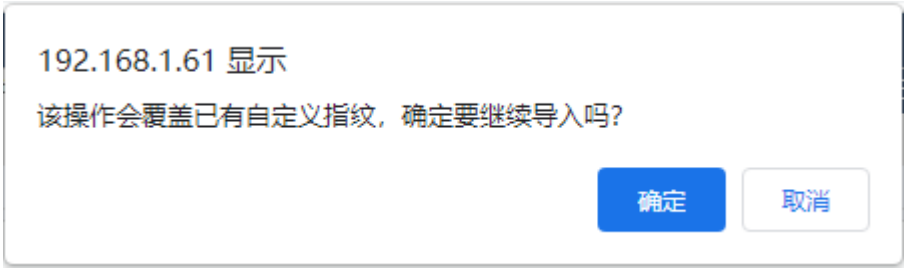
2. 点击✖删除某条自定义指纹，然后点击**确定**删除。

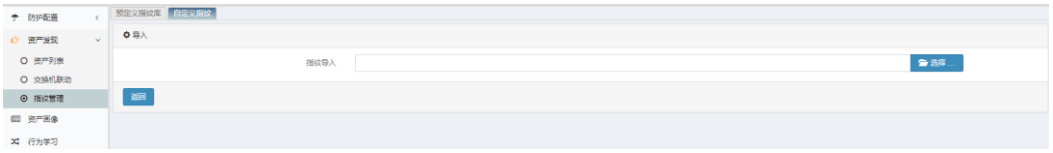
15.7.4 导入自定义指纹

配置步骤：

1. 进入**资产防护>资产发现>指纹管理>自定义指纹**，如下图。

2. 点击**导入**，然后点击确定。





3. 点击**选择**，选择要导入的指纹。

4. 点击**导入**，上传选中文件。

> 注意
>
> 导入自定义指纹的文件必须是加密压缩文件，且解压缩密码是 IOTcustomfinger。
>
> 导入指纹会覆盖已有自定义指纹。

15.7.5 导出自定义指纹

配置步骤：

1. 进入**资产防护>资产发现>指纹管理>自定义指纹**，如下图：

2. 点击**导出**。

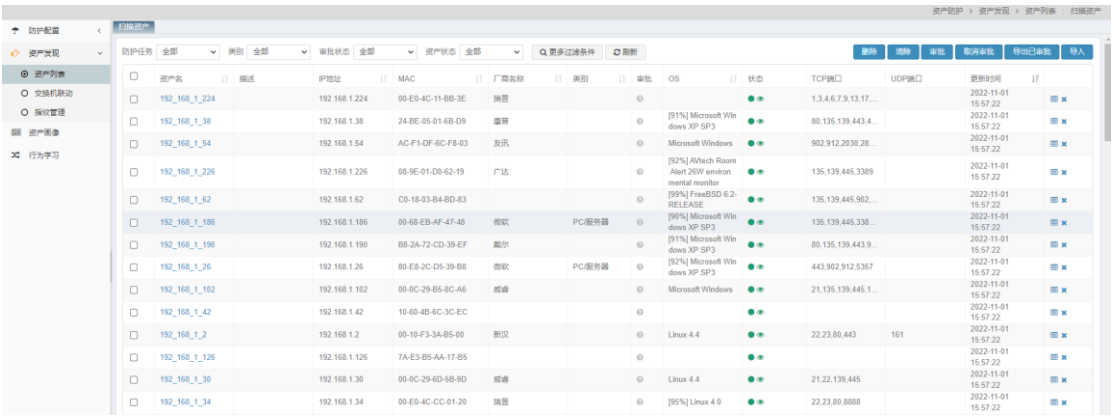
注意

导出的指纹是一个加密压缩文件，解压缩密码是 IOTcustomfinger。

15.8 配置资产列表

15.8.1 资产列表配置

资产列表的主要功能是展示扫描资产的指纹信息，并对资产做一些类似审批、修改、隔离或者放行的管理，如下图所示：



通过资产列表上方的检索框可以快速的搜索想查看的资产，检索项包括防护任务名称，资产类型、资产审批状态、资产状态（是否告警）、资产名称、资产 IP、资产 MAC、资产 OS、资产厂商、资产在线状态等。下面是对资产的指纹解释：

资产名：资产名称；

描述：资产描述；

IP 地址：资产的 IP 地址；

MAC：资产的 MAC 地址；

厂商名称：资产的制造厂商，如惠普、大华等；

类别：资产的类型，如打印机、摄像头等；

审批：当资产的指纹信息得到管理员的认可，可置为审批状态，此时指纹信息若变化就会告警，根据配置，还有可能自动加入黑名单；

OS：资产的操作系统；

状态：代表在线，代表已扫描，代表告警（指纹有变化），代表已隔离（加入 IP 黑名单）

tcp 端口：资产启用的 tcp 端口列表，端口号之间用“,”隔开；

udp 端口：资产启用的 udp 端口列表，端口号之间用“,”隔开；

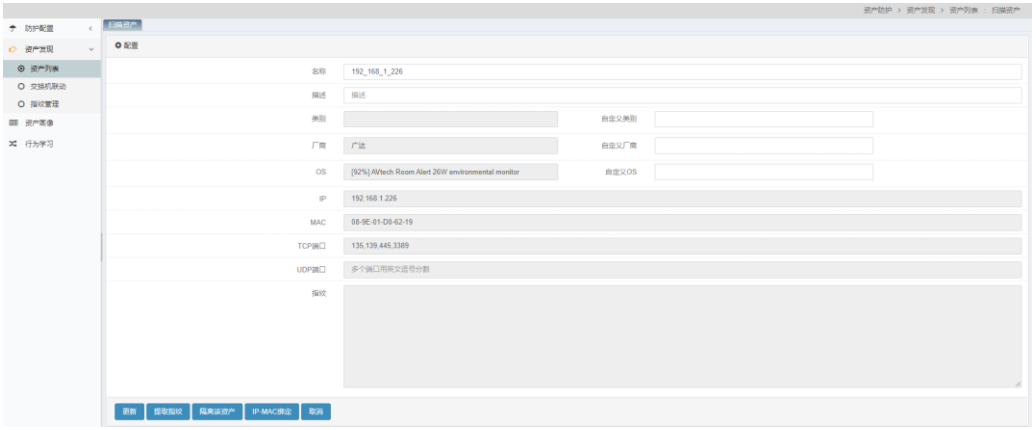
更新时间：资产指纹更新的时间；

资产的操作包括修改、删除、清除（删除所有资产）、审批、取消审批以及导入和导出。其中资产的审批，如下图所示 ：

类似上述操作，也可以批量取消审批资产。

资产导出只能导出已审批资产，导出文件是一个加密的压缩包。导入资产功能只能导入已经导出的审批资产。

点击资产名称，可以进入修改页面，如下所示：



可以自定义资产的类型、厂商和 os，自定义修改后，在上面的资产列表页面将优先显示自定义信息。修改后点击更新即生效。对于有指纹信息（80 或者 443 端口开放的资产 web 首页详情）的资产可以提取指纹，从而建立自定义指纹，自定义指纹的操作见下面指纹管理章节。

另外还有两个快捷按钮：隔离该资产和 IP-MAC 绑定。隔离该资产可以一键将资产加入 IP 黑名单，点击 IP-MAC 绑定按钮，会跳转到 IP-MAC 绑定页面。

15.9 行为学习

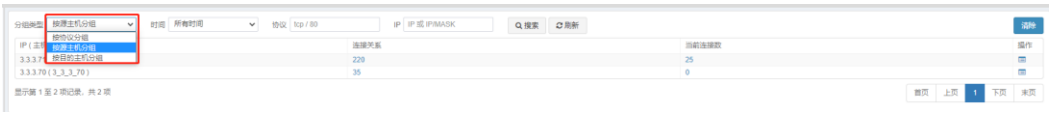
15.9.1 连接和资产统计

查看步骤：

1. 进入**资产防护>行为学习**，默认**按协议分组**查看。

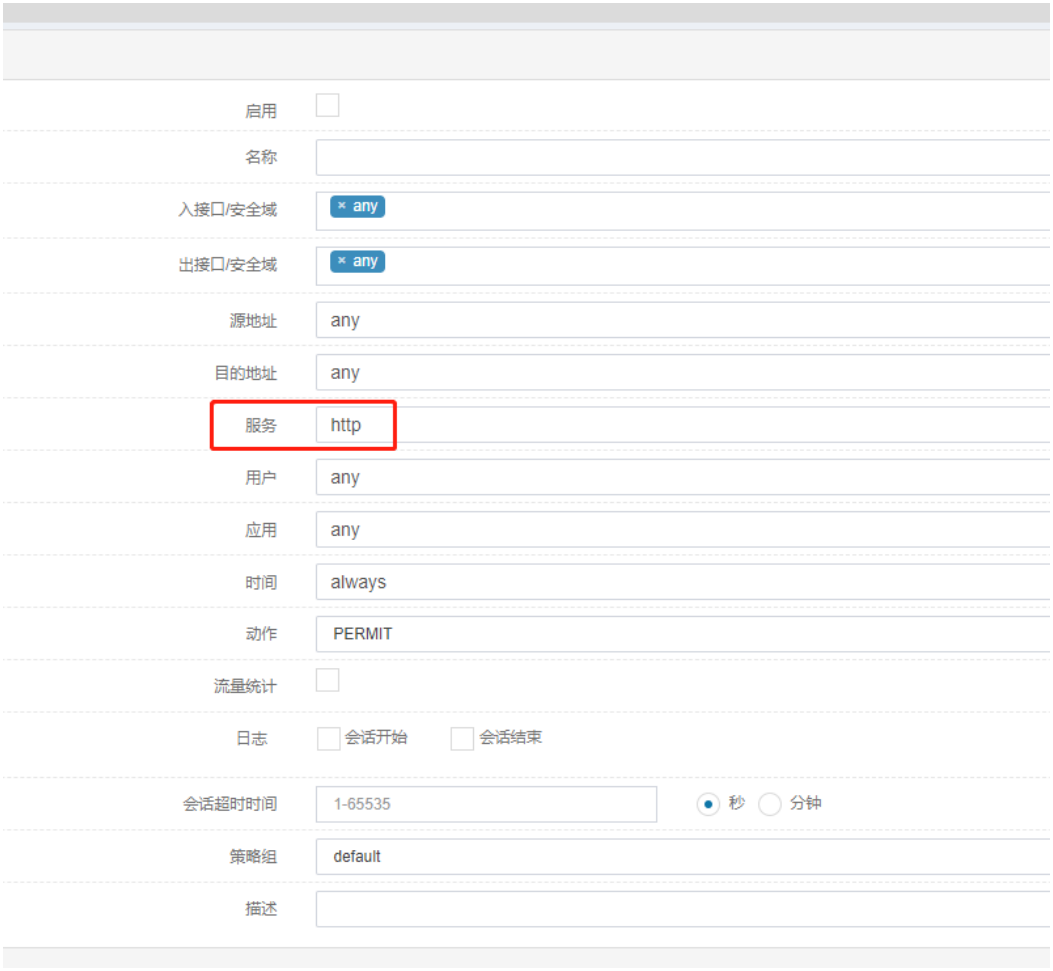
显示每种协议下的连接关系数量、当前连接数和隔离资产数量。

2. 点击**分组类型**，还可以选择按照**源主机分组**或**目的主机分组**查看。



3. 可以输入搜索条件，搜索指定类型的连接。

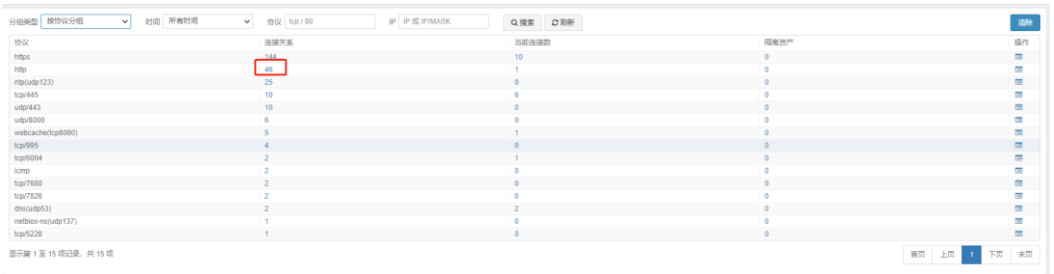
4. 点击某个协议的 可生成对应策略，具体配置步骤请参照对应模块的介绍。

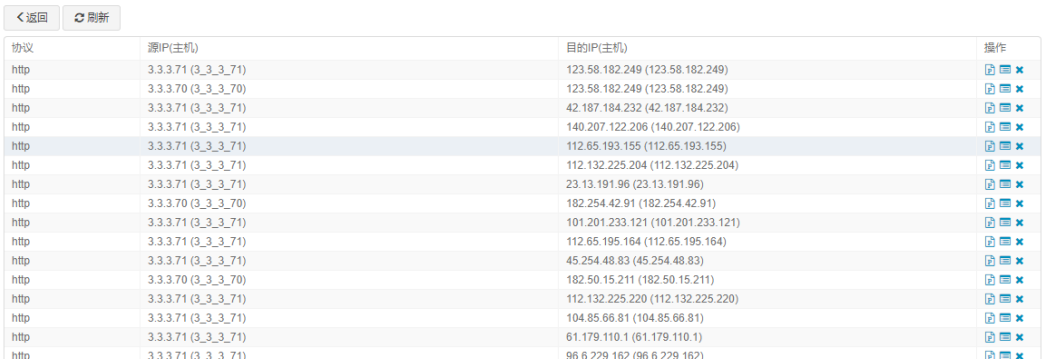


15.9.2 连接关系详情

查看步骤：

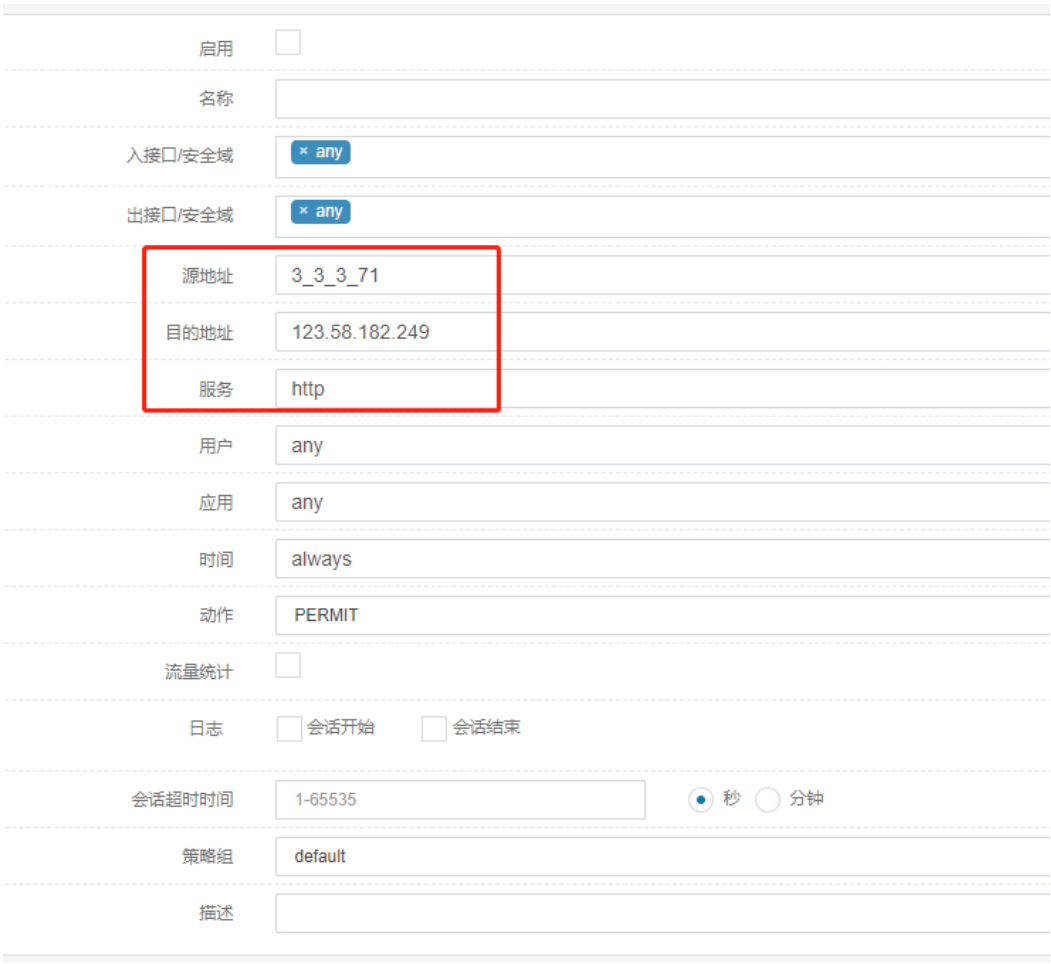
1. 点击相应的**连接关系**统计数值，查看协议对应的连接关系详情。





2. 点击 可对此连接抓包，点击**抓包**开始抓包。

3. 点击可生成对应策略，具体配置步骤请参照对应模块的介绍。

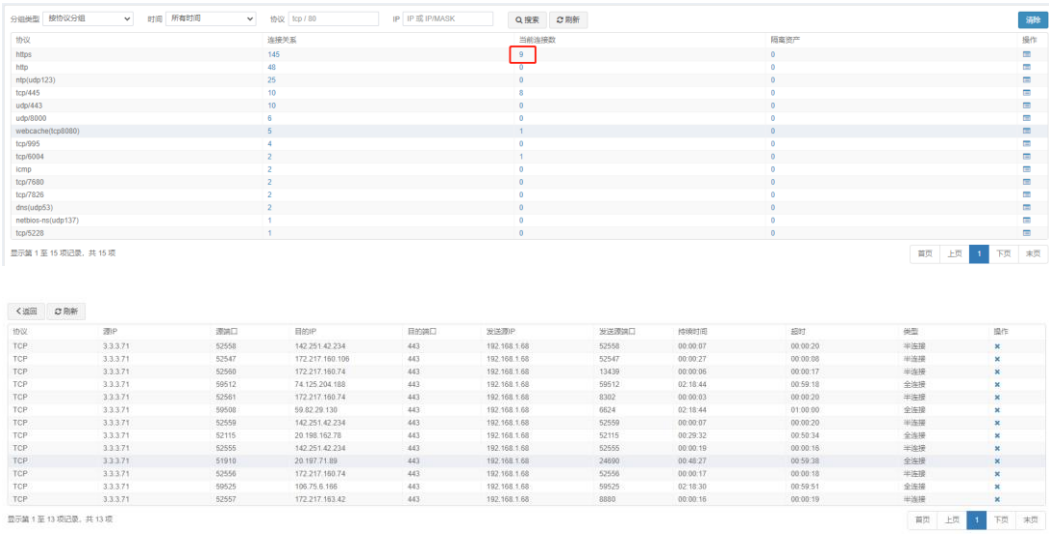


4. 点击删除此条连接关系。

15.9.3 当前连接数详情

查看步骤：

1. 点击相应的**当前连接数**统计数值，查看协议对应的当前连接数详情。

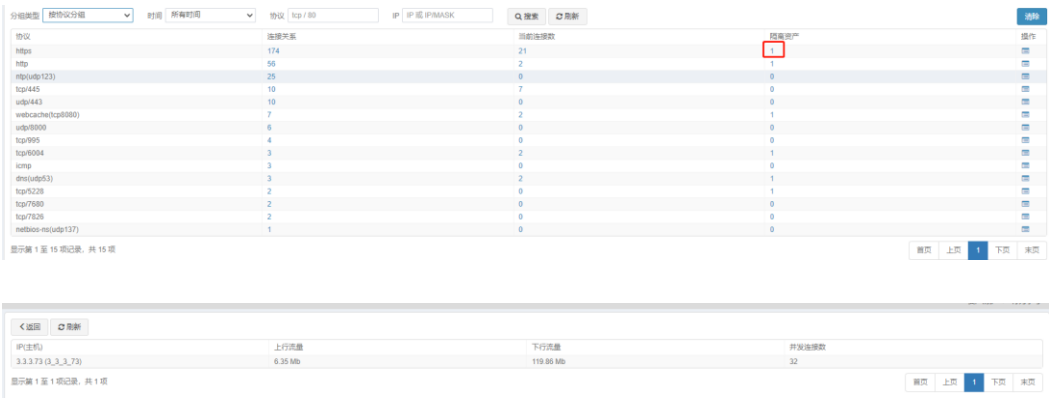


可以查看协议、源 IP、源端口、目的 IP、目的端口、发送源 IP、发送源端口、持续时间、超时、类型。

15.9.4 隔离资产详情

查看步骤：

1．点击相应的**隔离资产**统计数值，查看协议对应的隔离资产详情。



可以查看 IP（主机）、上行流量、下行流量和并发连接数。

15.10 配置案例

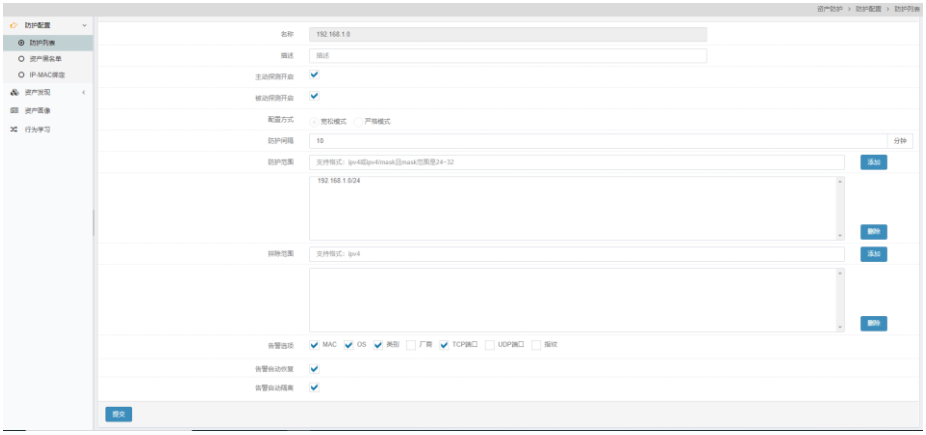
15.10.1 配置案例1：对某个网段开启资产防护功能

案例描述

对网络的某个网段开启资产防护功能。

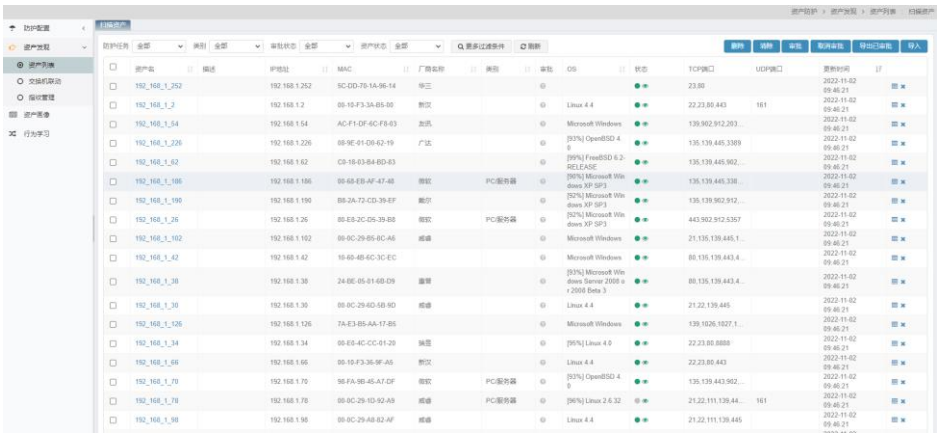
配置步骤：

1. 添加一个防护任务。进入**资产防护>防护配置>防护列表，**点击新建，如下图所示：



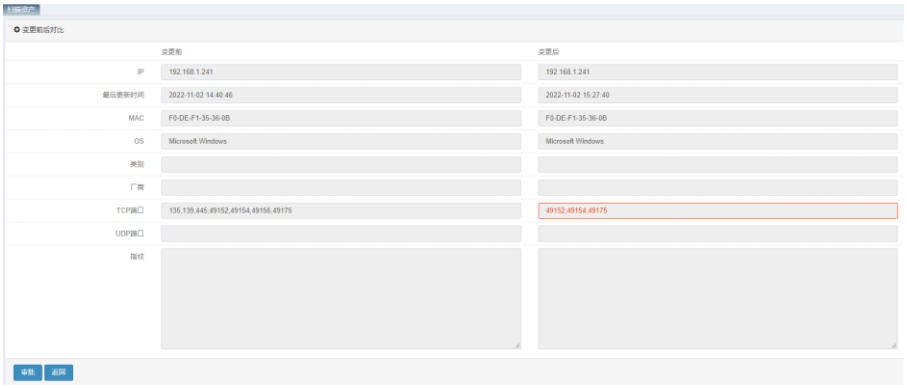
配置名称，描述，添加防护范围 192.168.1.0/24（设备可达网络）,将管理设备的电脑 IP 加入排除范围，以防把管理电脑加入黑名单而不能管理设备，添加一个 TCP 端口作为告警选项，开启告警自动隔离，其他按默认配置，点击提交。刷新一下防护列表，可以看到本条防护列表进入扫描状态。如下图所示：

等待扫描完成，即主动探测状态变为定时等待，进入**资产防护>资产发现>资产列表，**可以查看到本次扫描的资产列表，如下图所示：



2. 模拟资产指纹变化。选取一个可配置的资产，勾选前面的方框选中资产，点击审批，状态转换为已审批。配置这个资产的 TCP 端口，增加一个或者减少一个，等待下次扫描，观察这个资产的状态变化。多出现了两个图标，黄色的异常告警图标和红色的已隔离图标，如下图所示：

点击黄色图标可以看到资产指纹变化前后对比图，如下所示：



进入**资产防护>防护配置>资产黑名单，**可以看到这个资产已经加入 IP 黑名单，如下图所示：

3. 模拟资产指纹恢复。由于防护任务配置了告警自动恢复，将资产的 TCP 端口恢复到之前的配置，等待防护任务再次扫描完成，查看资产，发现状态栏已经没有黄色和红色图标，资产恢复正常。

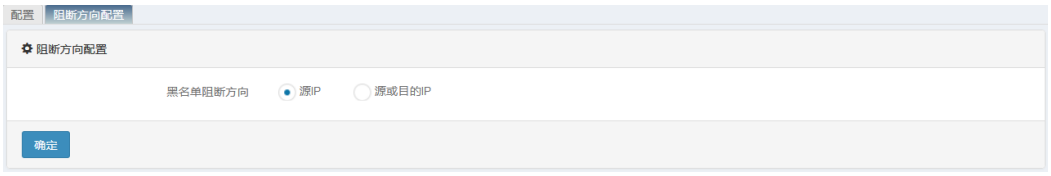
15.10.2 配置案例：创建资产黑名单

案例描述

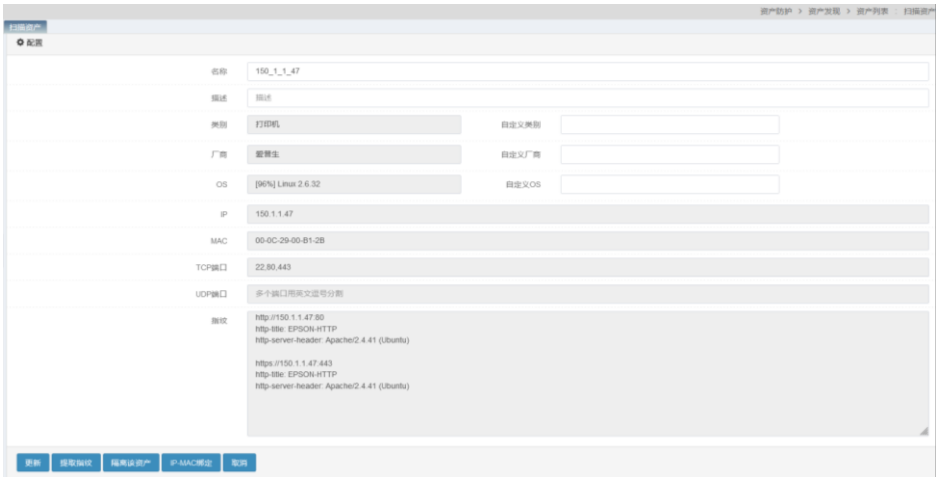
在资产列表中将扫描状态异常的资产通过隔离操作，创建对应资产黑名单，生成后资产黑名单阻断源 IP 为 150.1.1.47 的流量，生效时间为永久。

配置步骤：

1. 进入**资产防护>防护配置>资产黑名单，**选择**阻断方向配置，**配置黑名单阻断方向为源 IP，如下图：



2. 进入**资产防护>资产发现>资产列表**，在**扫描资产**的显示列表下通过点击资产名进入资产修改页面，如下图：



3. 点击 隔离该资产 创建生成一条 IP 为 150.1.1.47 的资产黑名单，完成配置，进入**资产防护>防护配置>资产黑名单**，选择**配置**查看，如下图：

15.10.3 配置案例：交换机联动

案例描述

设备的 ge0/0 连接内网，ge0/1 连接 PC，配置交换机联动

配置步骤：

1. 进入**资产防护>资产发现>交换机联动**，配置访问间隔和超时时间，并勾选**启用**，如下图：

2. 配置 **SNMP 服务器**，如下图：

3. 点击**提交**。

16 第16章 接口

16.1 接口概述

T 系列防火墙网络接口管理分为五种：物理接口配置管理、VLAN 配置管理、透明桥配置管理、链路聚合配置管理、GRE 配置管理。

其中物理接口主要是对以太网接口进行属性配置。

VLAN 配置包括创建 VLAN，并在 VLAN 中加入成员接口。加入到 VLAN 分两种方式：tag 与 untag。tag 的方式启用 802.1Q 协议并能处理协议报文，untag 方式则只能处理不带标签的普通以太网报文。VLAN 支持 STP 协议，根据 STP 协议与其他 VLAN 形成生成树。

透明桥配置包括创建桥接口，并在桥中加入成员接口。透明桥支持 STP 协议，根据 STP 协议与其他设备的透明桥、VLAN 形成生成树。

链路聚合是指将多个物理端口捆绑在一起，成为一个逻辑端口，以实现出/入流量在各成员端口中的负荷分担，提高带宽的作用。链路聚合支持 LACP 协议，可以与对端设备形成动态的链路聚合关系。

GRE 接口能够与远端 GRE 连接形成 GRE VPN 隧道，通过 GRE 接口，可以从 GRE VPN 隧道中接收、发送数据。

16.2 物理接口配置

物理接口的配置管理主要是对设备中的物理接口状态查看与状态、协商、速率、双工等进行配置。

配置步骤：

1. 进入**网络>接口>物理接口**列表，如下图：

共5条

链路状态	名称	IP 地址	MAC 地址	速率	双工模式	管理状态	VLAN 数量	链路聚合
	mgt	192.168.1.132/24	00-e0-4c-08-31-2e	100	FULL	UP	0	
	ge0/0(ge0/0)		00-e0-4c-08-31-30	N/A	N/A	UP	0	
	ge0/1(ge0/1)		00-e0-4c-08-31-31	N/A	N/A	UP	0	
	ge0/2(ge0/2)		00-e0-4c-08-31-2f	N/A	N/A	UP	0	
	ge0/3(ge0/3)	1.1.1.1/24	00-e0-4c-08-31-32	1000	FULL	UP	0	

链路状态：物理接口链路状态，绿色为 UP，红色为 DOWN。

名称：物理接口名称，mgt 是管理口，ge X/X 是千兆口，xge X/X 是万兆口。

IP 地址：物理接口的 IP 地址/掩码。

MAC 地址：物理接口的 MAC 地址。

速率：物理接口实际速率，单位 Mbps。

双工模式：物理接口双工模式，分为全双工/半双工两种（FULL/HALF）。

管理状态：物理接口手工管理状态，分为 UP/DOWN 两种状态。

VLAN 数量：物理接口所属于的 VLAN 数量。

链路聚合：物理接口所属的链路聚合，设备标识是 tvi X。

提示 一个物理接口可以以 tag 方式加入到多个 vlan 中。

2. 点击**接口名称**，进入单个物理接口配置，如下图：

基本属性

接口：物理接口名称，mgt 是管理口，ge X/X 是千兆口，xge X/X 是万兆口。

名称：物理接口的别名。

静态：通过手工配置的方式设置接口的 IP 地址。

IP 地址/掩码：物理接口 IP 地址，可选择 IPv4、IPv6，输入 IP 地址并点击**添加**生效。

浮动 IP：是否是浮动 IP。

UID：HA 单元 ID。

DHCP：通过 DHCP 协议的方式获取接口的 IP 地址。

改变内部 DNS：使用从 DHCP 服务器得到的 DNS 作为本地使用的 DNS。

从服务器重新得到网关：增加 DHCP 的缺省路由，网关为从 DHCP 服务器得到的网关。

管理距离：通过 DHCP 获取的缺省路由的管理距离。

PPPOE：通过 PPPOE 服务器获取接口 IP 地址。

用户：PPPoE 拨号的用户名。

密码：PPPoE 拨号的密码。

指定 IP：如果不使用服务器分配的地址而是使用设备自己指定的 IP 地址，则通过指定 IP 配置设备本身使用的 IP。

管理距离：通过 PPPoE 获取缺省路由的管理距离。

权重：通过 PPPoE 获取缺省路由的权重。

从服务器重新得到网关：增加 PPPoE 类型的缺省路由，网关为从 PPPoE 服务器得到的网关。

改变内部 DNS：使用从 PPPoE 服务器得到的 DNS 做为本地使用的 DNS。

配置

管理状态：物理接口的启用或关闭，可选 UP/DOWN。

协商模式：物理接口协商模式，可选自协商/非自协商。

速率：物理接口协商速率，单位 Mbps。可选 1000/100/10。

双工模式：物理接口双工模式，分为全双工/半双工两种（FULL/HALF）。

MTU：MTU 值，范围为 68-1500。

管理访问：配置该接口地址上允许访问的服务类别。

HTTP：可通过 HTTP 协议访问该接口的地址，来访问管理设备。

HTTPS：可通过 HTTPS 协议访问该接口的地址，来访问管理设备。

PING：该接口地址允许响应 PING。

TELNET：可通过 TELNET 协议访问该接口地址，来访问管理设备。

SSH：可通过 SSH 协议访问该接口地址，来访问管理设备。

BGP：可通过该接口地址访问设备提供的 BGP 服务。

OSPF：可通过该接口地址访问设备提供的 OSPF 服务.。

RIP：可通过该接口地址访问设备提供的 RIP 服务。

DNS：可通过该接口地址访问设备提供的 DNS 服务。

tControl：可通过该接口地址，访问设备提供的可编程服务。

接入控制：此接口是否使用 L2TP、SSLVPN。


提示

只有物理接口协商模式为非自协商时，速率、双工模式才是可配置项，当物理接口为光口时，协商模式变成灰色，即不可改状态。

点击**更新**完成对物理接口的配置。

16.3 VLAN配置

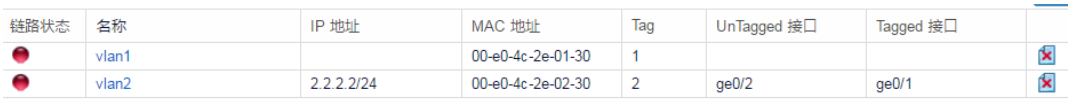
在一个物理局域网内，通过对端口的划分，将局域网内的设备分割为几个各自独立的群组，群组内部的设备之间可以自由地通讯，而当分属不同群组的设备要进行通讯时，必须进行三层的路由转发。通过这种方式，一个物理局域网就如同被划分为几个相互隔离的局域网，这些不同的群组就称为虚拟局域网（VLAN）。加入到 VLAN 中的接口分两种方式：tag 与 untag，tag 的方式启用 802.1Q 协议并能处理协议报文，untag 方式则只能处理不带标签的普通以太网报文。

VLAN 支持 STP 协议，STP（Spanning Tree Protocol）是生成树协议的英文缩写。该协议可应用于环路网络，通过一定的算法实现路径冗余，同时将环路网络修剪成无环路的树型网络，从而避免报文在环路网络中的增生和无限循环。

VLAN 接口可以通过命令开启透明转发模式（透传所有 vlan tag），实现透明桥功能。

16.3.1 添加VLAN

1. 进入**网络>接口>VLAN** 列表，如下图：



链路状态：VLAN 的状态。

名称：VLAN 名称。

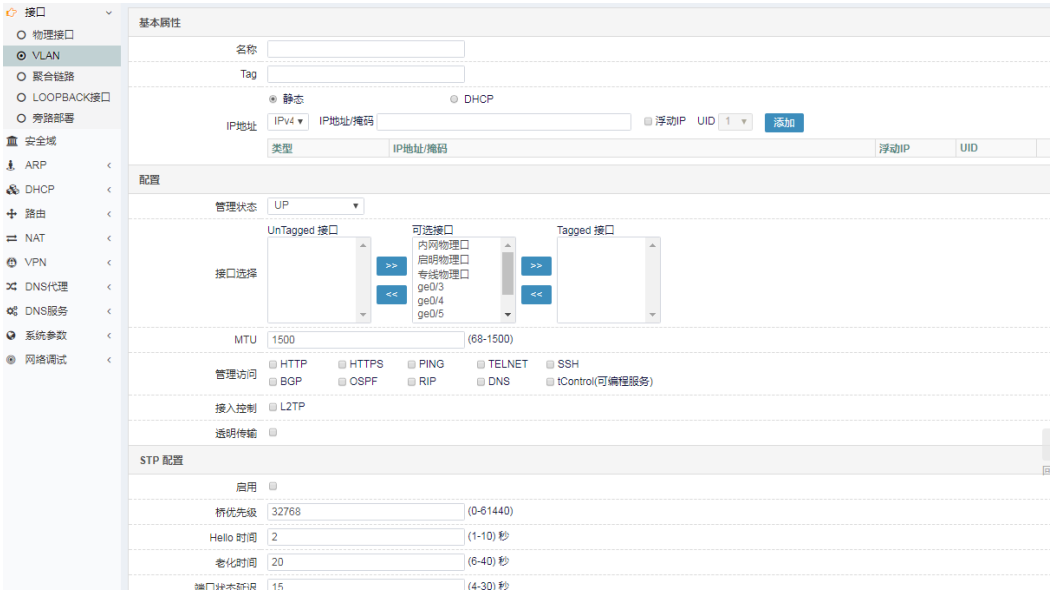
IP 地址：VLAN 的 IP 地址/掩码。

Tag：VLAN 的 ID 号。

UnTagged 接口：VLAN 中不带 Tag 的物理接口。

Tagged 接口：VLAN 中带 Tag 的物理接口，启用 802.1Q 协议。

2. 点击**新建**创建 VLAN，如下图：



基本属性

名称：VLAN 名称。

Tag：VLAN 的 ID 号。

静态：通过手工配置的方式设置接口的 IP 地址。

IP 地址/掩码：物理接口 IP 地址，可选择 IPv4、IPv6，输入 IP 地址并点击**添加**生效。

浮动 IP：是否是浮动 IP。

UID：HA 单元 ID。

DHCP：通过 DHCP 协议的方式获取接口的 IP 地址。

改变内部 DNS：使用从 DHCP 服务器得到的 DNS 作为本地使用的 DNS。

从服务器重新得到网关：增加 DHCP 的缺省路由，网关为从 DHCP 服务器得到的网关。

管理距离：通过 DHCP 获取的缺省路由的管理距离。

配置

管理状态：VLAN 启用或或关闭，可选 UP/DOWN。

可选接口：设备中可以加入的 VLAN 的物理接口。

UnTagged 接口：以 UnTag 方式加入 VLAN 的物理接口。

Tagged 接口：以 Tag 方式加入 VLAN 的物理接口，启用 802.1Q 协议。

MTU：VLAN 的 MTU 值，范围为 68-1500。

管理访问：配置该接口地址上允许访问的服务类别。

HTTP：可通过 HTTP 协议访问该接口的地址，来访问管理设备。

HTTPS：可通过 HTTPS 协议访问该接口的地址，来访问管理设备。

PING：该接口地址允许响应 PING。

TELNET：可通过 TELNET 协议访问该接口地址，来访问管理设备。

SSH：可通过 SSH 协议访问该接口地址，来访问管理设备。

BGP：可通过该接口地址访问设备提供的 BGP 服务。

OSPF：可通过该接口地址访问设备提供的 OSPF 服务.。

RIP：可通过该接口地址访问设备提供的 RIP 服务。

DNS：可通过该接口地址访问设备提供的 DNS 服务。

tControl：可通过该接口地址，访问设备提供的可编程服务。

接入控制：此接口是否使用 L2TP。

透明传输：开启 vlan 透传 tag 功能，需要将 vlan 下的接口以 untag 方式加入 vlan，然后开启这个选项，这样就可以透传所有 vlan tag 了。

3. STP 配置

启用：是否在 VLAN 中启用 STP 协议。

桥优先级：VLAN 在 STP 树中的桥优先级，范围为 0-61440。

Hello 时间：VLAN 发送 STP BPDU 报文间隔，范围 1-10 秒。

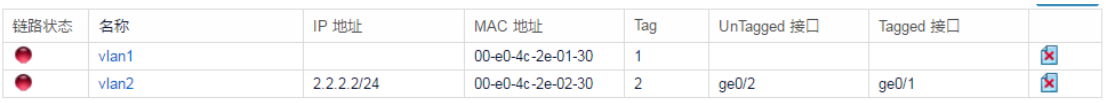
老化时间：STP 状态隔老化时间未更新，认为拓扑改变，范围 6-40 秒。

端口状态延迟：端口状态变换的时延，范围 4-30 秒。

端口状态变换的时延是指：开启 STP 后，端口从 listening 到 learning 到 forwarding 各状态变化的时间间隔。

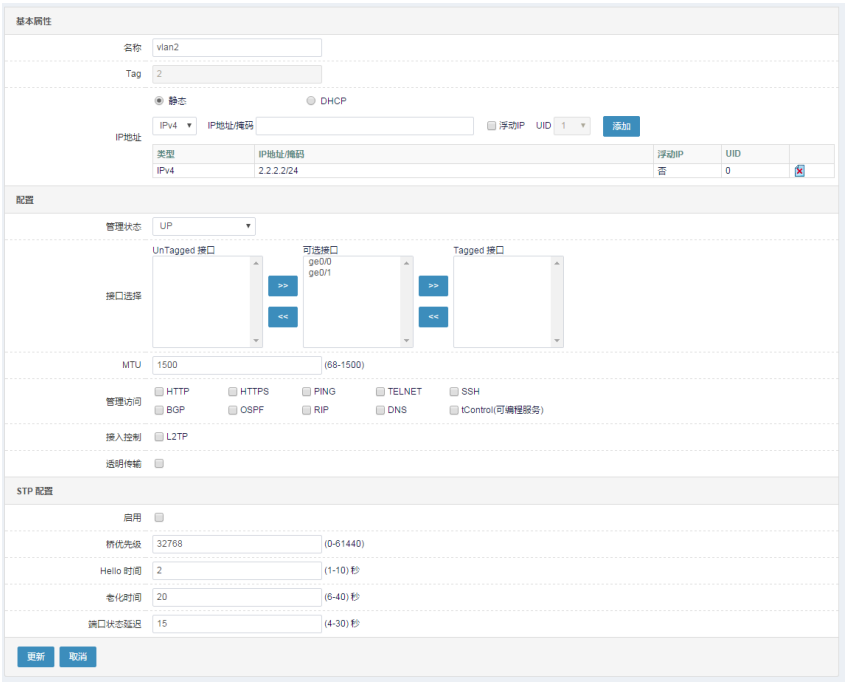
16.3.2 修改VLAN

1. 进入**网络>接口>VLAN** 列表，如下图：



链路状态	名称	IP 地址	MAC 地址	Tag	UnTagged 接口	Tagged 接口	
	vlan1		00-e0-4c-2e-01-30	1			
	vlan2	2.2.2.2/24	00-e0-4c-2e-02-30	2	ge0/2	ge0/1	

2. 点击 VLAN **名称**，修改 VLAN，如下图：



修改 VLAN 的 **IP 地址、管理状态、UnTagged 接口、Tagged 接口、MTU、STP 配置**等信息。

3. 点击**更新**完成修改。

提示 不能修改 vlan 本身的名称、Tag 值。

16.3.3 删除VLAN

1. 进入**网络>接口>VLAN 接口**列表，如下图：

链路状态	名称	IP 地址	MAC 地址	Tag	UnTagged 接口	Tagged 接口	
	vlan1		00-e0-4c-2e-01-30	1			
	vlan2	2.2.2.2/24	00-e0-4c-2e-02-30	2	ge0/2	ge0/1	

2. 点击删除 VLAN。

3. 点击**确定**删除 VLAN。

提示 被其他功能引用的 VLAN 不能被删除。

16.4 VXLAN配置

VXLAN（Virtual eXtensible Local Area Network，虚拟扩展局域网），是由 IETF 定义的 NVO3（Network Virtualization over Layer 3）标准技术之一，是对传统 VLAN 协议的一种扩展。VXLAN 的特点是将 L2 的以太帧封装到 UDP 报文（即 L2 over L4）中，并在 L3 网络中传输。

VXLAN 本质上是一种隧道技术，在源网络设备与目的网络设备之间的 IP 网络上，建立一条逻辑隧道，将用户侧报文经过特定的封装后通过这条隧道转发。从用户的角度来看，接入网络的服务器就像是连接到了一个虚拟的二层交换机的不同端口上，可以方便地通信。

16.4.1 添加VXLAN

4. 进入**网络>接口>VXLAN**，如下图：

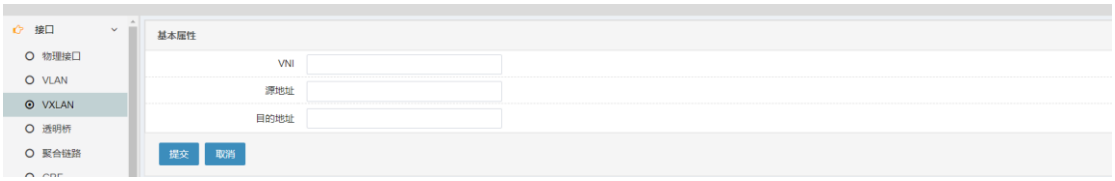
名称：VXLAN 接口名称。

VNI：VXLAN Network Identifier，VXLAN 网络标识符。

源地址：VXLAN 隧道的源地址。

目的地址：VXLAN 隧道的目的地址。

5. 点击**新建**创建 VXLAN，如下图：

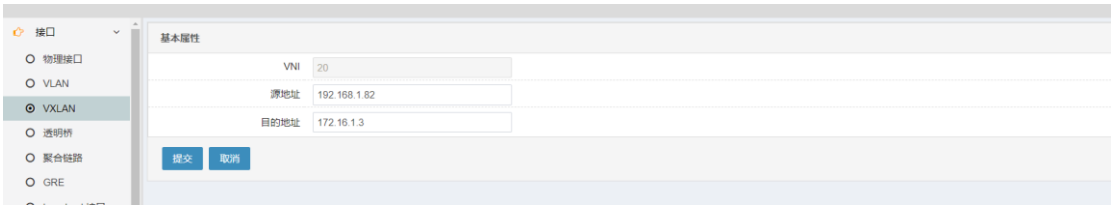


6. 配置 VNI、源地址和目的地址，点击提交，创建一条 vxlan 隧道。

16.4.2 修改VXLAN

4. 进入**网络>接口>VXLAN** 列表，如下图：

5. 点击 VXLAN **名称**，修改 VXLAN，如下图：



修改 VXLAN 的源地址和目的地址。

6. 点击**提交**完成修改。

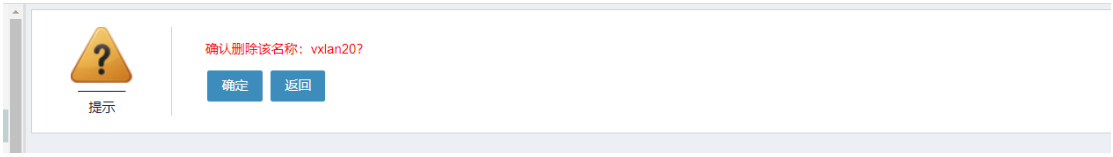
提示

不能修改 VXLAN 的 VNI 参数。

16.4.3 删除VXLAN

4. 进入**网络>接口>VXLAN 接口**列表，如下图：

5. 点击  删除 VXLAN。



6. 点击**确定**删除 VXLAN。

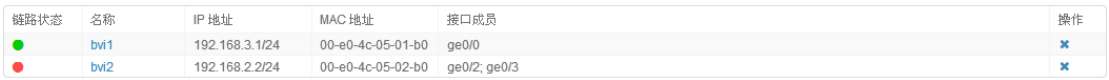
被其他功能引用的 VXLAN 不能被删除。

16.5 透明桥配置

透明网桥功能最初是由 DEC 公司提出，并被 802.1 委员会采纳并标准化。透明网桥实现网络报文链路层转发，使用方便，易于安装。透明桥支持 STP 协议，STP（Spanning Tree Protocol）是生成树协议的英文缩写。该协议可应用于环路网络，通过一定的算法实现路径冗余，同时将环路网络修剪成无环路的树型网络，从而避免报文在环路网络中的增生和无限循环。

16.5.1 添加透明桥

1. 进入**网络>接口>透明桥**列表，如下图：



链路状态：桥接口的状态。

名称：桥接口名称。

IP 地址：桥接口的 IP 地址/掩码。

MAC 地址：桥接口的 MAC 地址。

接口成员：桥接口的物理端口成员。

2. 点击**新建**创建桥接口，如下图：

配置

名称：桥接口名称。

桥组号：桥接口组号。

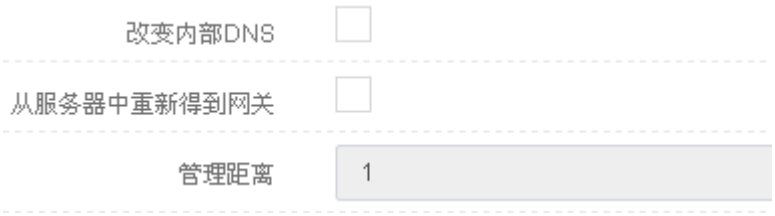
静态 IP：通过手工配置的方式设置桥接口的 IP 地址。

IP 地址/掩码：桥接口 IP 地址，可选择 IPv4、IPv6，输入 IP 地址并点击**添加**生效。

浮动 IP：是否是浮动 IP。

UID：HA 单元 ID。

DHCP（自动获取 IP）：通过 DHCP 协议的方式获取桥接口的 IP 地址。



改变内部 DNS：使用从 DHCP 服务器得到的 DNS 作为本地使用的 DNS。

从服务器重新得到网关：增加 DHCP 的缺省路由，网关为从 DHCP 服务器得到的网关。

管理距离：通过 DHCP 获取的缺省路由的管理距离。

管理状态：桥接口启用或或关闭，可选 UP/DOWN。

接口选择：设备中可以加入的透明桥的物理接口。

MTU：VLAN 的 MTU 值，范围为 68-1500。

管理访问：配置该接口地址上允许访问的服务类别。

HTTP：可通过 HTTP 协议访问该接口的地址，来访问管理设备。

HTTPS：可通过 HTTPS 协议访问该接口的地址，来访问管理设备。

PING：该接口地址允许响应 PING。

TELNET：可通过 TELNET 协议访问该接口地址，来访问管理设备。

SSH：可通过 SSH 协议访问该接口地址，来访问管理设备。

BGP：可通过该接口地址访问设备提供的 BGP 服务。

OSPF：可通过该接口地址访问设备提供的 OSPF 服务.。

RIP：可通过该接口地址访问设备提供的 RIP 服务。

DNS：可通过该接口地址访问设备提供的 DNS 服务。

tControl：可通过该接口地址，访问设备提供的可编程服务。

接入控制：是否允许 L2TP、SSLVPN 接入。

VLAN 透传：透明桥中允许透传的 vlan 报文 vlan id。


提示

Vlan 透传在不配置的时候，默认允许所有 tag 的流量和没有 tag 的流量通过。

透明桥永远允许没有 tag 的流量通过。

3. STP 配置

启用：是否在桥接口中启用 STP 协议。

桥优先级：桥接口在 STP 树中的桥优先级，范围为 0-61440。

Hello 时间：桥接口发送 STP BPDU 报文间隔，范围 1-10 秒。

老化时间：STP 状态隔老化时间未更新，认为拓扑改变，范围 6-40 秒。

端口状态延迟：端口状态变换的时延，范围 4-30 秒。


提示

端口状态变换的时延是指：开启 STP 后，端口从 listening 到 learning 到 forwarding 各状态变化的时间间隔。

16.5.2 修改桥接口

1. 进入**网络>接口>透明桥**列表，如下图：

链路状态	名称	IP 地址	MAC 地址	接口成员	操作
●	bvi1	192.168.3.1/24	00-e0-4c-05-01-b0	ge0/0	✖
●	bvi2	192.168.2.2/24	00-e0-4c-05-02-b0	ge0/2; ge0/3	✖

2. 点击桥接口**名称**，修改桥接口，如下图：

修改桥接口的 **IP 地址、管理状态、成员接口、VLAN 透传、MTU、STP 配置**等信息。

3. 点击**更新**完成修改。

16.5.3 删除桥接口

1. 进入**网络>接口>透明桥**列表，如下图：

2. 点击 ✖ 删除桥接口。

3. 点击**确定**删除桥接口。

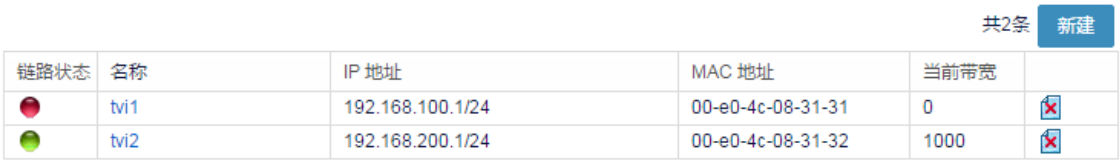
被其他功能引用的桥接口不能被删除。

16.6 链路聚合配置

链路聚合 Trunk 是通过将多个链路组合为一个逻辑的网络链路，以提高设备之间通讯通道的容量和可靠性的技术。链路聚合也提供了负载均衡的方式来处理通讯负荷，使得通讯负荷均分在几个链路中，不会有单独一个链路超负载。通过链路聚合，用户可以在许多应用中得到实际的益处：更高的可靠性、更高的带宽，使用现有的设备，节约成本（不需要更新设备来获取更高的带宽）。

16.6.1 添加链路聚合

1．进入**网络>接口>链路聚合**列表，如下图：



链路状态：链路聚合的状态。

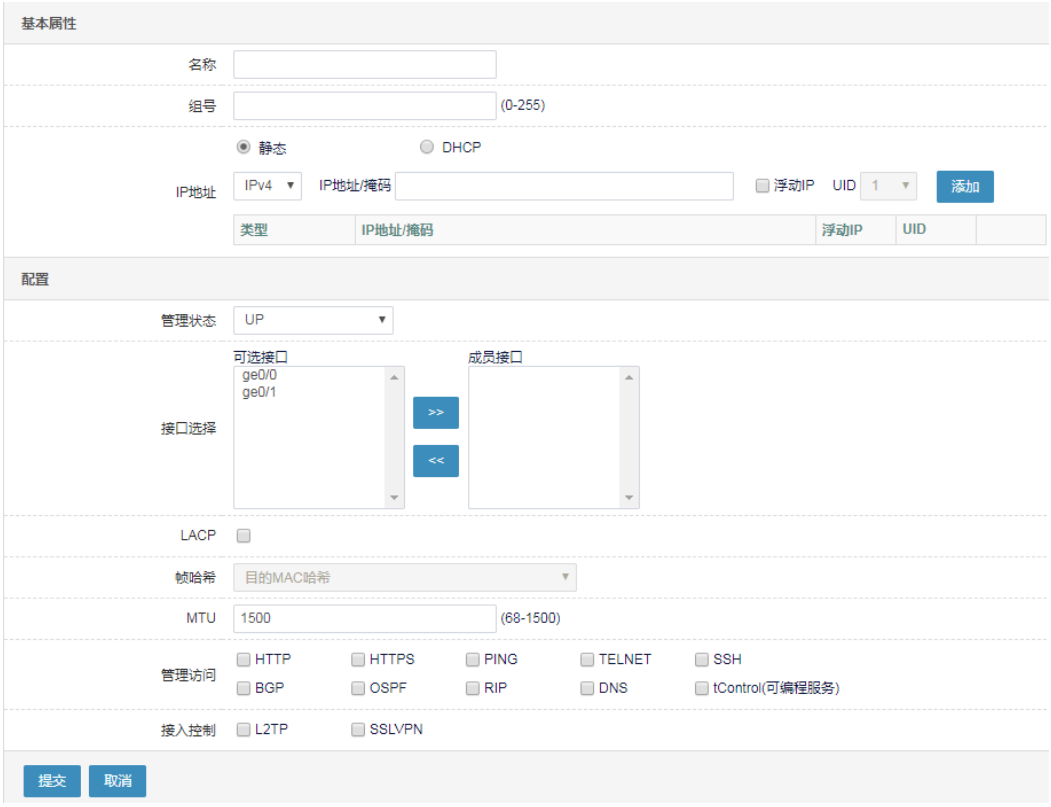
名称：链路聚合名称。

IP 地址：链路聚合的 IP 地址。

MAC 地址：链路聚合的 MAC 地址。

当前带宽：所聚合的链路总带宽，单位 M。

2．点击**新建**创建链路聚合，如下图：



基本属性

名称：链路聚合名称。

组号：链路聚合组号。

手动指定 IP：通过手工配置的方式设置接口的 IP 地址。

IP 地址/掩码：物理接口 IP 地址，可选择 IPv4、IPv6，输入 IP 地址并点击**添加**生效。

浮动 IP：是否是浮动 IP。

UID：HA 单元 ID。

DHCP（自动获取 IP）：通过 DHCP 协议的方式获取接口的 IP 地址。

改变内部 DNS：使用从 DHCP 服务器得到的 DNS 作为本地使用的 DNS。

从服务器重新得到网关：增加 DHCP 的缺省路由，网关为从 DHCP

服务器得到的网关。

管理距离：通过 DHCP 获取的缺省路由的管理距离。

管理状态：链路聚合启用或关闭，可选 UP/DOWN。

可选接口：设备中可以加入的链路聚合组的物理接口。

成员接口：已经加入到链路聚合组中的物理接口。

LACP：是否开启 LACP 协议。

帧哈希：发送数据哈希方法，可选目的 MAC 哈希、源/目的 IP 和端口哈希。

MTU：链路聚合 mtu 值，范围为 68-1500。

管理访问：配置可通过该链路聚合地址，访问设备提供的服务类别。

HTTP：可通过访问该链路聚合的地址，访问设备提供的 HTTP 服务。

HTTPS：可通过访问该链路聚合地址，访问设备提供的 HTTPS 服务。

PING：该链路聚合地址允许响应 PING。

TELNET：可通过该链路聚合地址 TELNET 到设备本地。

SSH：可通过该链路聚合地址 SSH 连到设备本地。

BGP：可通过该链路聚合地址访问设备提供的 BGP 服务。

OSPF：可通过该链路聚合地址访问设备提供的 OSPG 服务。

RIP：可通过该链路聚合地址访问设备提供的 RIP 服务。

DNS：可通过该链路聚合地址访问设备提供的 DNS 服务。

tControl：可通过该链路聚合地址，访问设备提供的可编程服务。

接入控制：此接口是否使用 L2TP、SSLVPN。

不开启 LACP 模式则静态轮询收发报文，开启 LACP 则可以达到动态链路聚合与备份。

16.6.2 修改链路聚合

1. 进入**网络>接口>链路聚合**列表，如下图：

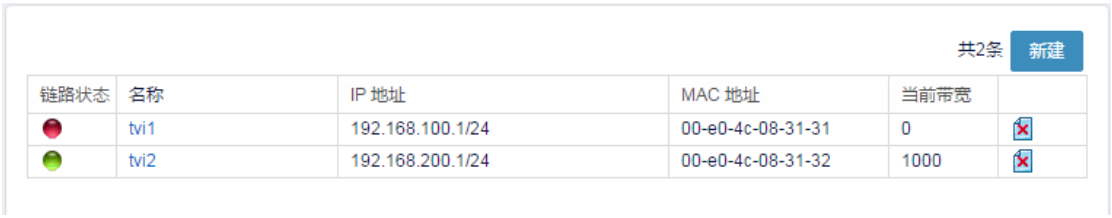
2. 点击链路聚合的名称进入修改页面。

修改链路聚合 **IP 地址、管理状态、成员接口、LACP、帧哈希**等信息。

3. 点击**更新**完成修改。

16.6.3 删除链路聚合

1. 进入**网络>接口>链路聚合**列表，如下图：



2. 点击删除链路聚合。

3. 点击**确定**删除聚合链路。

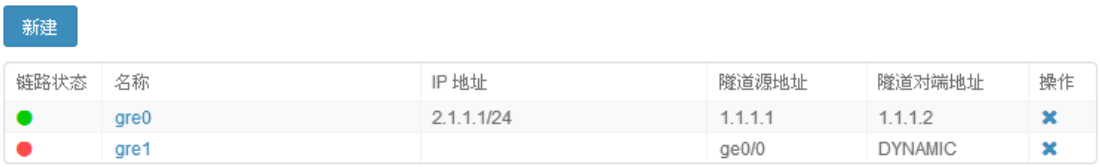
提示 已经被引用的链路聚合不能被删除。

16.7 GRE配置

GRE（Generic Routing Encapsulation，通用路由封装）协议是对网络层协议的数据报文进行封装，使这些被封装的数据报文能够在另一个网络层协议中传输。GRE 采用了 Tunnel（隧道）技术，是 VPN（Virtual Private Network）的第三层隧道协议。通过 GRE 接口配合路由配置，可以将流量引入 GRE 隧道传输。

16.7.1 添加GRE接口

1．进入**网络>接口>GRE** 列表，如下图：



链路状态：GRE 接口的状态。

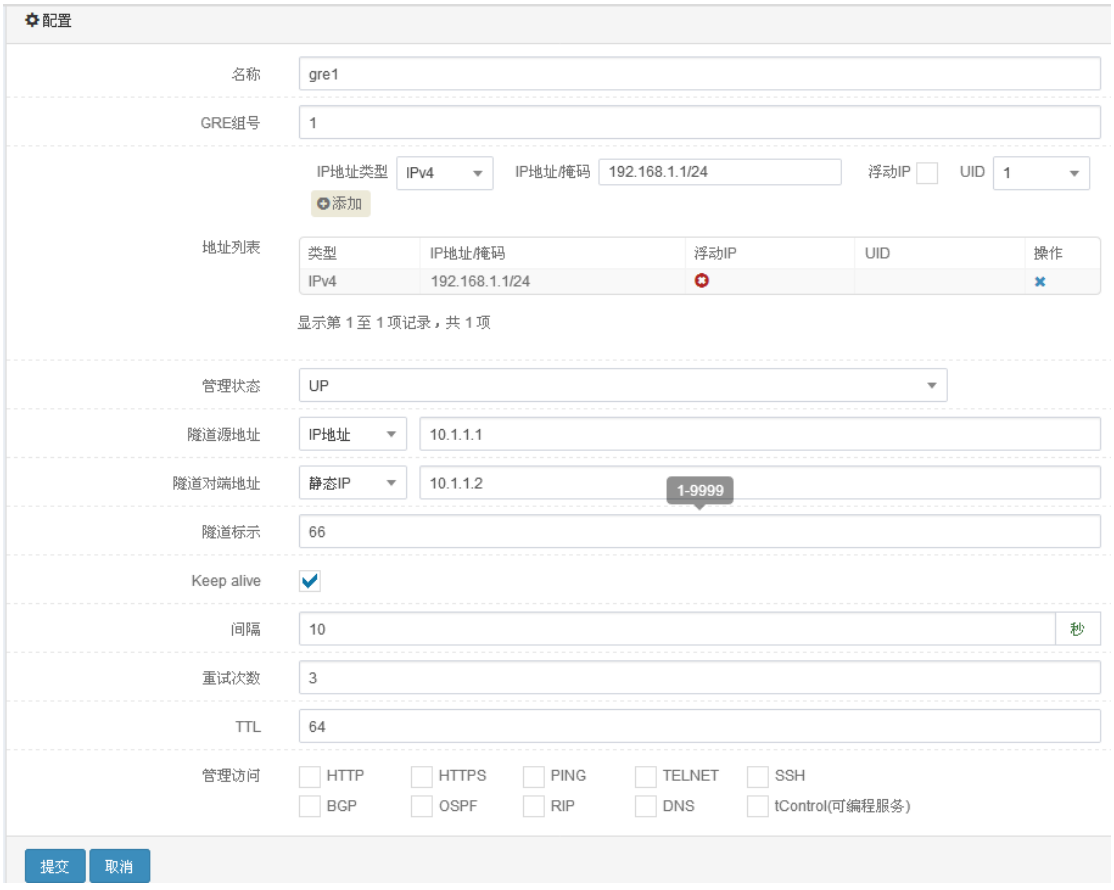
名称：GRE 接口的名称。

IP 地址：GRE 接口的 IP 地址。

隧道源地址：GRE 隧道的源地址。

隧道对端地址：GRE 隧道的对端地址。

2．点击新建创建 GRE 接口，如下图：



基本属性

名称：GRE 接口名称。

组号：GRE 接口组号。

地址列表：GRE 接口 IP 地址

管理状态：GRE 接口启用或关闭，可选 UP/DOWN。

隧道源地址：GRE 隧道的源地址。

隧道对端地址：GRE 隧道的对端地址。

隧道标示：GRE 隧道标示 key，范围 1-9999。

Keep alive：GRE 隧道启用保活机制。

间隔：保活报文发送间隔，范围 1-86400 秒。

重试次数：保活报文重发次数，范围 1-1000 次。

TTL：GRE 隧道 IP 报文的 TTL 值，范围 0-255。

管理访问：配置可通过该 GRE 地址，访问设备提供的服务类别。

HTTP：可通过访问该 GRE 的地址，访问设备提供的 HTTP 服务。

HTTPS：可通过访问该 GRE 地址，访问设备提供的 HTTPS 服务。

PING：该 GRE 地址允许响应 PING。

TELNET：可通过该 GRE 地址 TELNET 到设备本地。

SSH：可通过该 GRE 地址 SSH 连到设备本地。

BGP：可通过该 GRE 地址访问设备提供的 BGP 服务。

OSPF：可通过该 GRE 地址访问设备提供的 OSPG 服务。

RIP：可通过该 GRE 地址访问设备提供的 RIP 服务。

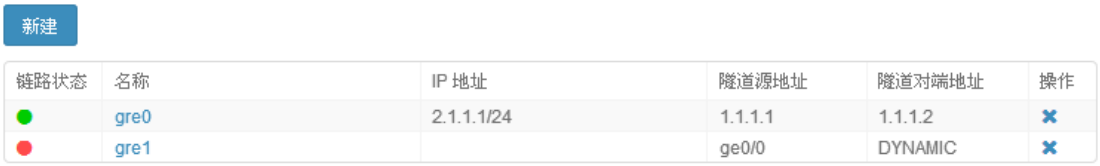
DNS：可通过该 GRE 地址访问设备提供的 DNS 服务。

注意

GRE 隧道两端隧道标示值必须相同才可正常通信。

16.7.2 修改GRE

1. 进入**网络>接口>GRE** 列表，如下图：



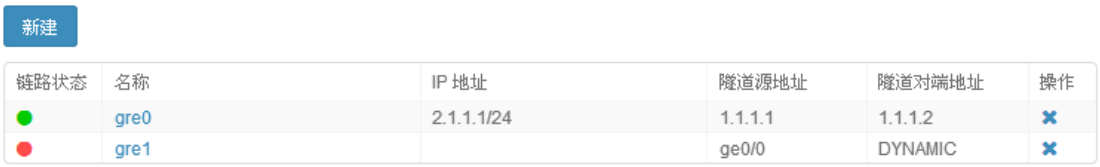
2. 点击 GRE 接口的名称进入修改页面。

修改 GRE 接口 **IP 地址、管理状态、隧道源地址、隧道目的地址**等信息。

3. 点击**更新**完成修改。

16.7.3 删除GRE接口

1. 进入**网络>接口>GRE** 列表，如下图：



2. 点击 删除 GRE 接口。

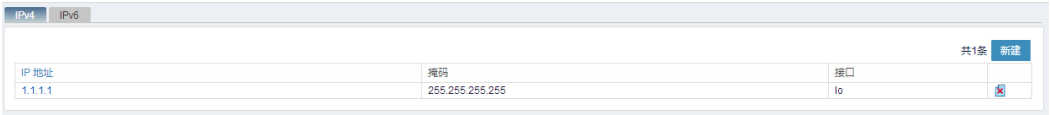
3. 点击**确定**删除 GRE 接口。

提示 已经被引用的 GRE 接口不能被删除。

16.8 LOOPLACK接口配置

16.8.1 添加LOOPBACK接口

1. 进入**网络>接口> LOOPBACK 接口**列表，如下图：



IP 地址：LOOPBACK 接口的 IP 地址。

掩码：LOOPBACK 接口的掩码。

接口：接口说明 lo（loopback）。

2. 点击**新建**创建 LOOPBACK 接口，可创建 IPV4 和 ipv6 地址如下图：

IP 地址：LOOPBACK 接口的 Ipv4 地址。

掩码：LOOPBACK 接口的掩码。

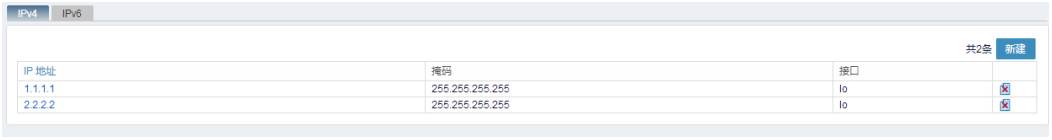
接口：接口说明 lo（loopback）。

IP 地址：LOOPBACK 接口的 Ipv6 地址。

接口：接口说明 lo（loopback）。

16.8.2 修改LOOPBACK接口

1. 进入**网络>接口>LOOPBACK** 接口列表，如下图：



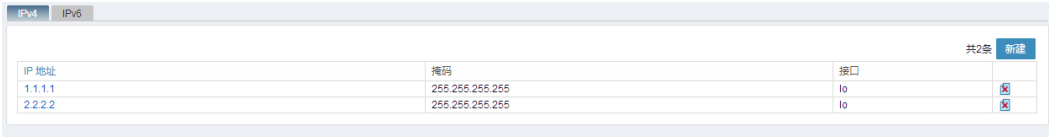
2. 点击 LOOPBACK 接口**名称**，修改 LOOPBACK 接口，如下图：

修改 LOOPBACK 接口的掩码。

3. 点击**更新**完成修改。

16.8.3 删除LOOPBACK接口

1. 进入**网络>接口>LOOPBACK** 接口列表，如下图：



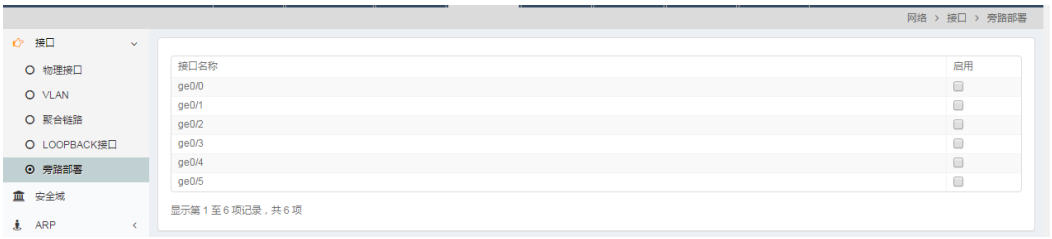
2. 点击删除 LOOPBACK 接口。

3. 点击**确定**删除 LOOPBACK 接口。

16.9 旁路部署

配置步骤：

进入**网络>接口>旁路部署**，如下图：在希望旁路模式的接口后面打钩即可。



16.10 接口联动

16.10.1 接口联动概述

接口联动可以通过配置接口联动组的方式，把多个物理接口绑定在一起，实现联动组内接口之间链路状态一致的功能。

16.10.2 配置接口联动组

接口联动组只能包含物理接口，被加入联动组的物理接口不能再加入其它的联动组，需要先从原有联动组中删除，再加入到新的联动组中。

配置步骤：

1. 进入**网络>接口>接口联动**，如下图：

联动功能：接口联动总开关。

状态：显示联动组中接口的链路状态，● 表示未知，● 表示 down，● 表示 up。

名称：接口联动组名称。

接口成员：接口联动组内包含的接口成员。

2. 点击**新建**创建接口联动组，如下图：

参数说明：

名称：联动组名称。

接口成员：选择联动组内包含的接口成员。

3. 配置完毕后，点击**提交**。

提示 不能引用正在被其它联动组引用的接口

16.10.3 编辑接口联动组

配置步骤：

1. 进入**网络>接口>接口联动**，对于某条存在的接口联动组配置，点击联动组名称进入编辑界面。

2. 可以对接口联动组里面的内容进行编辑修改，修改完毕后点击**更新**。

注意 编辑接口联动组时，联动组名称不能改变。

16.10.4 删除接口联动组

配置步骤：

1. 进入**网络>接口>接口联动**，如下图：

2. 点击 ✖ 删除接口联动组配置。

16.11 配置案例

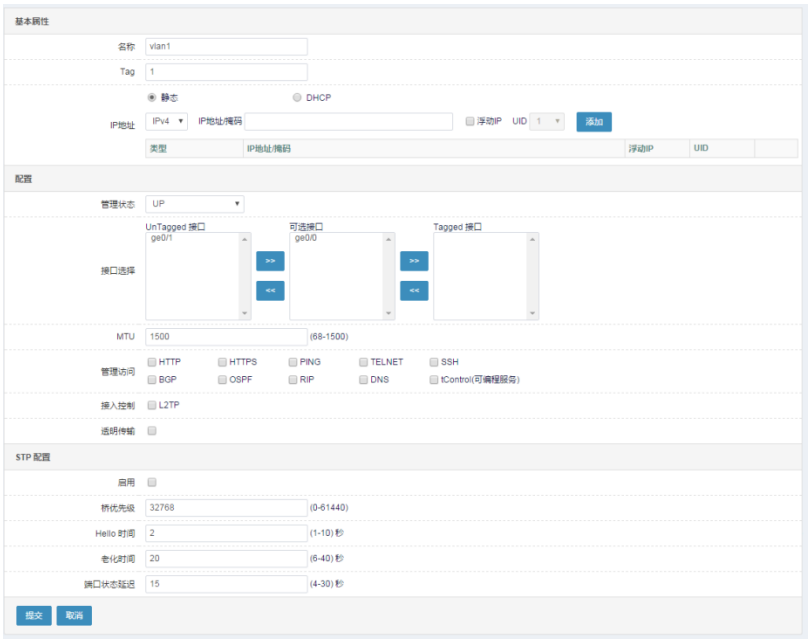
16.11.1 配置案例1：增加一个VLAN

案例描述：

创建一个 VLAN 并在其中加入物理接口成员。

配置步骤：

1. 进入**网络>接口>VLAN** 列表，点击**新建**，如下图：



2. 输入参数：名称 vlan1，Tag 号 1，状态 UP，MTU 1500。

3. 选择**可选接口**中的接口 ge0/1 点击 << 加入到 Untagged 接口中，**可选接口**中的接口 ge0/2 点击 >> 加入到 Tagged 接口中。

4. **启用 STP**，配置 STP **桥优先级** 32768，**Hello 时间** 2 秒，**老化时间** 20 秒，**端口状态延迟** 15 秒。

5. 点击**提交**完成创建 VLAN。

16.11.2 配置案例2：增加一个VXLAN隧道配置

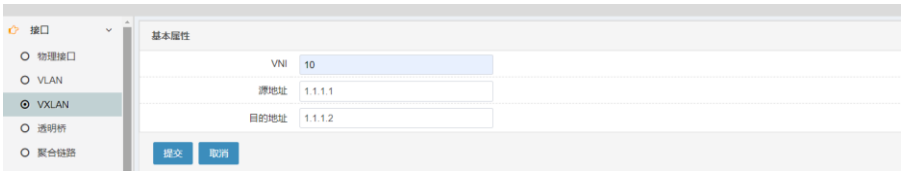
案例描述：

创建 VXLAN 隧道，并让连接的子网设备互通。

配置步骤：

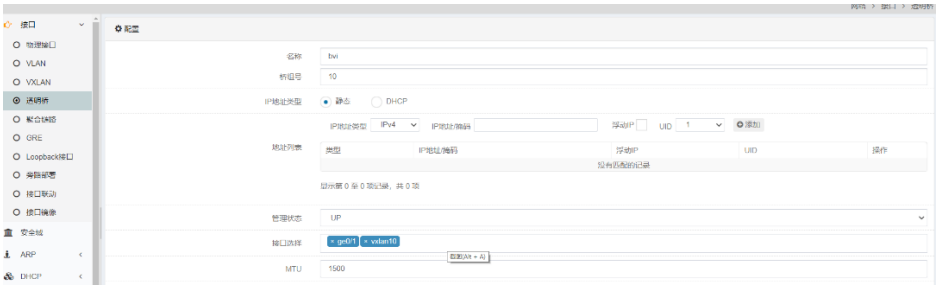
1.两台设备 A、B，其 ge0/0 接口连接在 ip 网络可达的环境里（比如一台交换机）。进入 A 设备管理页面，配置物理接口 ge0/0，配置接口地址为 1.1.1.1/24

2.配置 vxlan，网络>接口>VXLAN，点击**新建**，如下图：



3.输入参数：VNI(0-16777214)，源地址和目的地址分别配置隧道外层地址，这里配置成实际的 1.1.1.1 和 1.1.1.2。

4.创建透明桥口 tvi10，如下图所示，名称为 bvi，桥组号为 10，接口选择上面配置的 vxlan10 和连接子网的 ge0/1，其他的默认选项。



5.同样配置 B 设备，ge0/0 接口地址为 1.1.1.2/24。创建 VXLAN，vni 为 10， 源地址为 1.1.1.2，目的地址为 1.1.1.1。创建透明桥口 bvi10，选择接口 vxlan10 和连接子网的 ge0/1。

6.此时，设备 A 和 B 的 ge0/1 接口所连接的子网（同一个子网）正常通信，A 和 B 设备连接的两个子网就像连在一台交换机下面。

16.11.3 配置案例3：增加一个链路聚合

案例描述：

创建一个链路聚合组，并在其中加入物理接口成员。

配置步骤：

1. 进入**网络>接口>链路聚合**列表，点击**新建**，如下图：

输入参数：名称 tvi1，组号 1，管理状态 UP。

2. **可选接口**中的接口 ge0/3、ge0/4 点击 >> 加入到链路聚合中。
3. **开启 LACP**，**帧哈希**源/目的 IP 和端口哈希。
4. 点击**提交**完成创建链路聚合。

16.11.4 配置案例4：配置桥模式

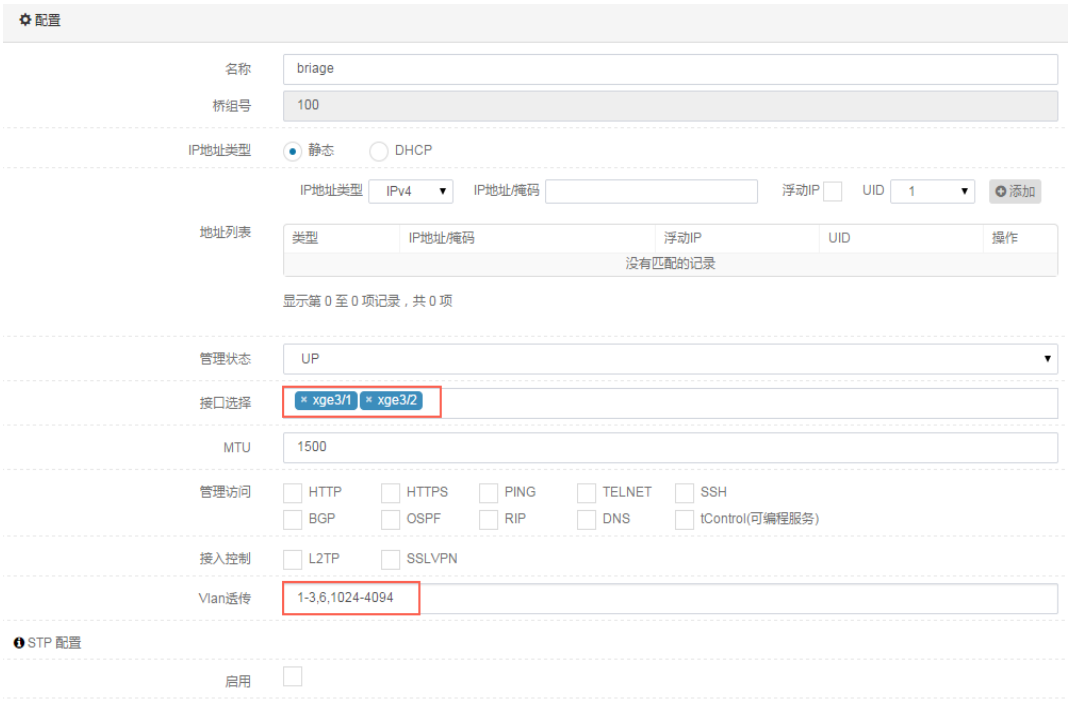
案例描述：

配置透明桥模式。

配置步骤：

1. 进入**网络>接口>透明桥**列表，点击**新建**，新建一个桥接口。

2. 将两个准备桥接的物理口加入桥接口。并配置允许透传的 vlan 标签 ID。



3. 此时将需要桥接的流量接到桥内的物理接口，就可以实现桥接了。

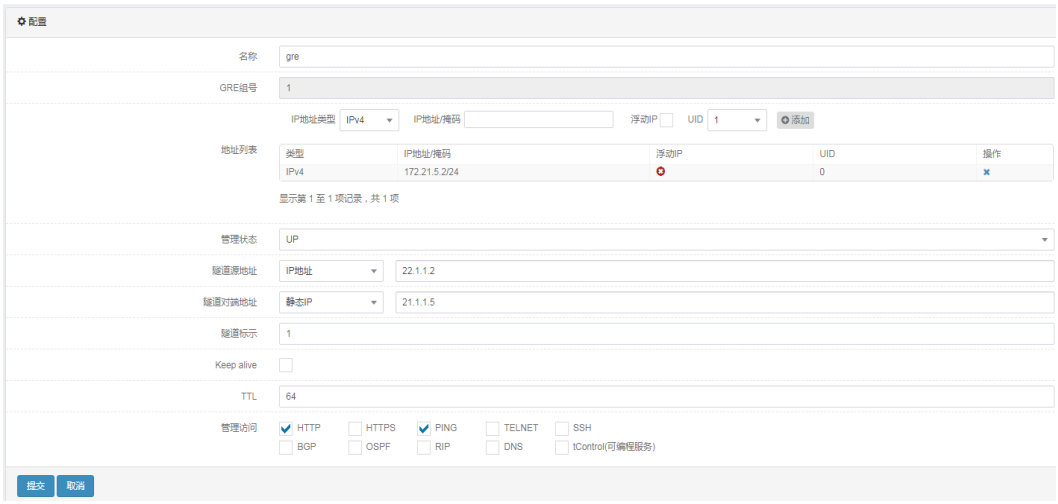
16.11.5 配置案例5：增加一个GRE接口

案例描述：

创建一个 GRE 接口

配置步骤：

1. 进入**网络>接口>GRE** 列表，点击**新建**，如下图：



2. 输入参数：名称 gre，组号 1。

3. 配置 GRE 地址，隧道源地址、隧道对端地址，隧道标识（两端必须保

持一致）

4. 管理访问勾选 HTTP、PING，可通过 GRE 接口进行 HTTP、PING 访问。

5. 点击**提交**完成创建 GRE。

16.12 常见故障分析

16.12.1 故障现象：链路聚合接口无效

现象	链路聚合接口不能接收报文也不能发送报文
分析	可能是链路聚合LACP协商不成功，导致其下接口没有激活
解决	检查对端设备 LACP 配置，使两端聚合 LACP 协商成功

16.12.2 故障现象：VLAN下tagged接口无效

现象	VLAN 下 tagged 接口不能收发报文
分析	可能是对端发送的非802.1Q协议的报文或报文VLAN ID与tag不同
解决	检查对端发送与 tag 相同的 802.1Q 协议报文

16.12.3 故障现象：桥接环境，部分流量不通

现象	桥接环境下，部分流量可以通，部分流量不通
分析	可能是该流量通过设备转发时带有vlan TAG，“vlan透传”没有配置该TAG。
解决	检查该流量是否带有 TAG 通过设备，并在“vlan 透传”配置允许该 TAG ID 通过

16.12.4 故障现象：GRE隧道环境，流量不通

现象	GRE 隧道环境，流量不通
分析	可能GRE借用的物理口状态为down，或者隧道对端地址不可达，或者隧道标示配置不一致
解决	1、 检查物理接口状态是否正常，若为 down 状态，修改成 up 状态 2、 检查是否有到达隧道对端地址的路由，若没有路由，添加到达隧道对端地址的路由 3、 检查隧道标示配置是否正常，若不同，则修改相同的标示

17 第17章 安全域

17.1 安全域概述

传统防火墙的策略配置通常都是围绕报文入接口、出接口展开的，这在早期的双穴防火墙中还比较普遍。随着防火墙的不断发展，已经逐渐摆脱了只连接外网和内网的角色，并且向着提供高端口密度的方向发展。一台高端防火墙通常能够提供十几个以上的物理接口，同时连接多个逻辑网段。在这种组网环境中，传统基于接口的策略配置方式需要为每一个接口配置安全策略，给网络管理员带来了极大的负担，安全策略的维护工作量成倍增加，从而也增加了因为配置引入安全风险的概率。

和传统防火墙基于接口的策略配置方式不同，业界主流防火墙通过围绕安全域（Security Zone）来配置安全策略的方式解决上述问题。所谓安全域，是一个抽象的概念，它可以包含普通物理接口和逻辑接口，也可以包括二层物理 Trunk 接口和 VLAN，划分到同一个安全区域中的接口通常在安全策略控制中具有一致的安全需求。引入安全区域的概念之后，安全管理员将安全需求相同的接口进行分类（划分到不同的区域），能够实现策略的分层管理。同时如果后续网络变化，只需要调整相关域内的接口，而安全策略不需要修改。

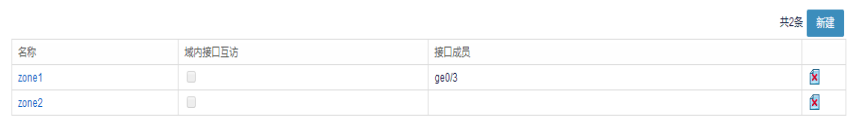
17.2 配置安全域

17.2.1 配置安全域

安全域可以包含普通物理接口和逻辑接口，也可以包括二层物理 Trunk 接口和 VLAN，可在策略出接口\入接口配置处引用安全域，进行接口条件过滤。开启防火墙策略的策略匹配开关后，如果没有命中的安全策略，同一安全域内的接口之间也可通过配置实现域内互访。

配置步骤：

1. 进入**网络>安全域**，如下图：



名称：安全域名称。

域内接口互访：显示该安全域是否开启域内接口互访功能。

接口成员：安全域内包含的接口成员。

2.点击**新建**创建安全域，如下图：

参数说明：

名称：安全域名称。

允许接口间互相访问：勾选后，如果防火墙策略的‘策略匹配’开关为开启状态，且没有匹配的防火墙策略，那么此域中的所有接口也均可互相访问。

接口选择：选择安全域内包含的接口成员。

3. 配置完毕后，点击**提交**。

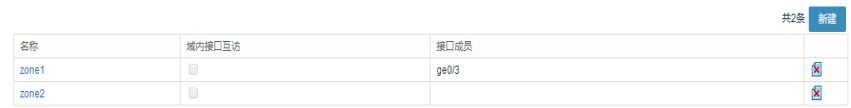
提示 安全域名称不能与其它接口名称、其它安全域名称重复。

提示 不能引用正在被其它安全域、vlan、trunk 引用的接口，也不能引用正在被防火墙策略引用的接口。

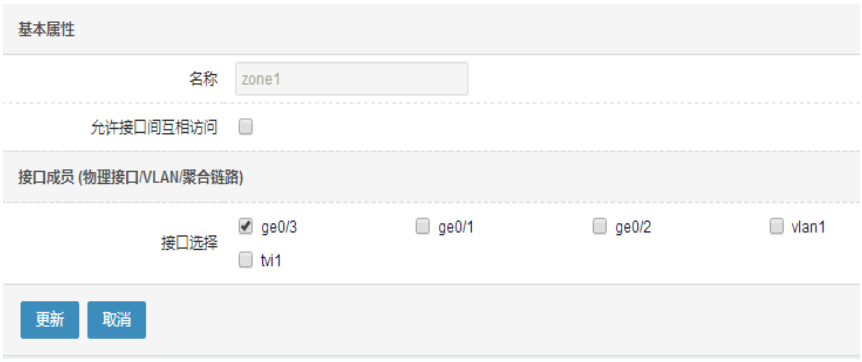
17.2.2 编辑安全域

配置步骤：

1. 进入**网络>安全域**，对于某条存在的安全域，点击安全域名称进入编辑界面。



2. 可以对安全域里面的内容进行编辑修改，修改完毕后点击**更新**。



注意

编辑安全域时，安全域名称不能改变。

17.2.3 删除安全域

配置步骤：

1. 进入**网络>安全域**，如下图：

2. 点击删除安全域。

17.3 配置案例

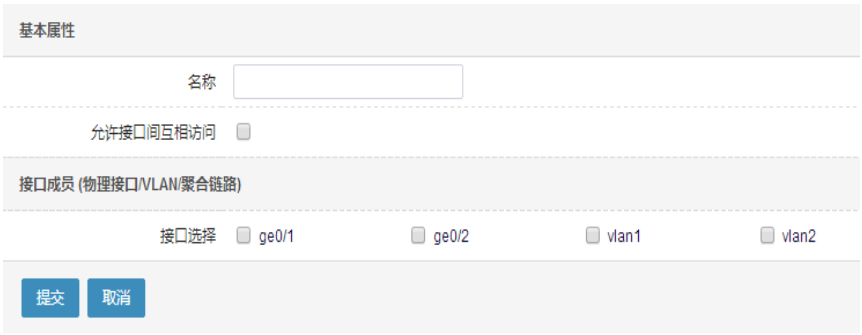
17.3.1 配置案例1：增加一个安全域并在防火墙策略中进行引用

案例描述

在防火墙策略上配置一个包括 ge0/1 和 ge0/2 的安全域作为防火墙策略的入接口。

配置步骤：

1. 进入**网络>安全域**，点击**新建**，如下图所示：



配置名称为 zone_fw_policy，接口成员选择 ge0/1 和 ge0/2。

2. 点击**提交**添加安全域成功，如下图：

3. 进入**策略>防火墙>策略**，点击**新建**，如下图所示：

4. 选择入接口为 zone_fw_policy 这个安全域，点击提交完成配置，如下图所示：

17.4 常见故障分析

17.4.1 故障现象：安全域无法选择某接口

现象	安全域接口选择时没有显示想要选择的某个接口。
分析	有可能是以下情况导致该接口无法加入安全域中： ➢ 接口已被vlan、trunk或其它安全域引用； ➢ 接口已被防火墙策略引用。
解决	重新选择可用接口或释放掉该接口在其它位置的引用。

18 第18章 静态 ARP

18.1 静态ARP概述

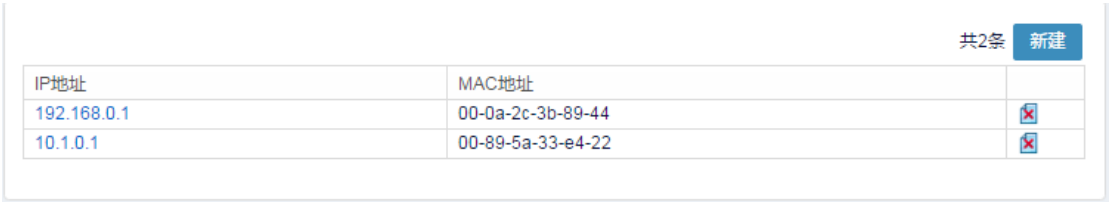
IP 数据包常通过以太网发送。以太网设备并不识别 32 位 IP 地址：它们是以 48 位以太网地址(MAC 地址)传输以太网数据包的。因此，IP 驱动器必须把 IP 地址转换成 MAC 地址。在这两种地址之间存在着某种静态的或算法的映射，常常需要查看一张表。地址解析协议(Address Resolution Protocol，ARP)就是用来确定这些映象的协议。

通常设备的 arp 表是动态从网络中获得，但有很多场景需要在无法获得外界 arp 的情况下向外发生数据，这就需要静态 ARP 功能来完成。静态 ARP 是强制绑定某 IP 地址与某 MAC 地址的功能，通过该功能可以完成黑洞路由、直接发送 IP 数据等功能。

18.2 静态ARP配置

18.2.1 添加静态ARP

1. 进入**网络>ARP>静态 ARP**，如下如所示：



IP 地址：静态 ARP 绑定的 IP 地址

MAC 地址：静态 ARP 绑定的 MAC 地址

2. 点击**新建**添加静态 ARP，如下图所示：

IP 地址：静态 ARP 绑定的 IP 地址

MAC 地址：静态 ARP 绑定的 MAC 地址

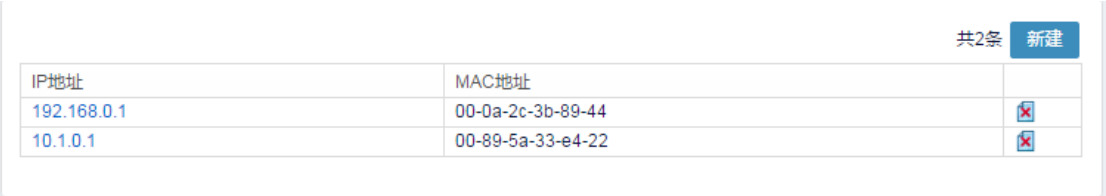
3. 点击**提交**完成静态 ARP 的添加。

注意

配置静态 ARP 时，MAC 地址可以重复添加，但 IP 地址必须唯一。

18.2.2 修改静态ARP

1. 进入**网络配置>ARP>静态 ARP**，如下如所示：



2. 点击静态 ARP 的 **IP 地址进行**修改，如下图所示：

修改静态 ARP 的 MAC 地址信息。

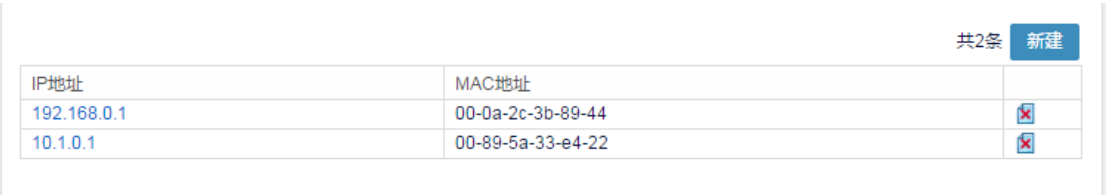
3. 点击**更新**完成修改。

注意

修改一条静态 ARP 不能修改其 IP 地址本身，只能修改其 MAC 地址。

18.2.3 删除静态ARP

1. 进入**网络配置>ARP>静态 ARP**，如下如所示：



2. 点击删除静态 ARP，如下图所示：

3. 点击**确定**删除。

18.3 常见故障分析

18.3.1 故障现象：添加静态ARP后网络不通

现象	添加静态 ARP 对端网络不通
分析	可能是静态ARP 中IP地址与对端网络IP相同导致冲突
解决	删除静态 ARP，直接使用对端网络中 IP 地址

19 第19章 DHCP 服务器

19.1 DHCP服务概述

本设备提供两种 DHCP 服务功能：DHCP 服务器和 DHCP Relay。

19.1.1 DHCP服务器概述

DHCP 的全称是动态主机配置协议（Dynamic Host Configuration Protocol）。设备可以作为 DHCP Server，用于实现对网络中 IP 地址的动态分配和集中管理。动态分配是指当 DHCP 客户端第一次从 DHCP Server 租用到 IP 地址后，并非永久的使用该地址，只要租约到期，客户端就要释放(Release)这个 IP 地址以给其它工作站使用。为了实现 IP 地址的动态分配，必须设置 DHCP Server 拥有一个 IP 地址范围，用来分配给用户，这个用来分配给客户端的地址范围也叫 IP 地址池（IP Pool）。

下图反映了 DHCP 客户端从 DHCP 服务器申请 IP 地址的过程。主机 A（客户端）先广播 DHCPDISCOVER 包寻找网络上的 DHCP 服务器，DHCP 服务器向客户端单播包含配置参数的 DHCPOFFER 消息。

图 13-1DHCP 客户端从 DHCP 服务器申请 IP 地址

- 当客户端第一次登录到网络时，它会向网络广播一个 DHCPDISCOVER 消息，此时由于客户端还不知道自己属于哪一个网路，所以封包的来源地址为 0.0.0.0，目的地址则为 255.255.255.255。
- 由于网络上可能不止一个 DHCP 服务器，凡是具有有效 IP 地址信息的 DHCP 服务器均从各自还没有租出的地址中选择一个空闲 IP，然后将该提议回应给客户端。
- 客户端从接收到的第一个提议中选定 IP 地址信息，并广播一条租用地址的消息请求。由发出该提议的 DHCP 服务器响应该消息，确认已接受请求并开始租用。
- 客户端收到确认后开始使用此地址

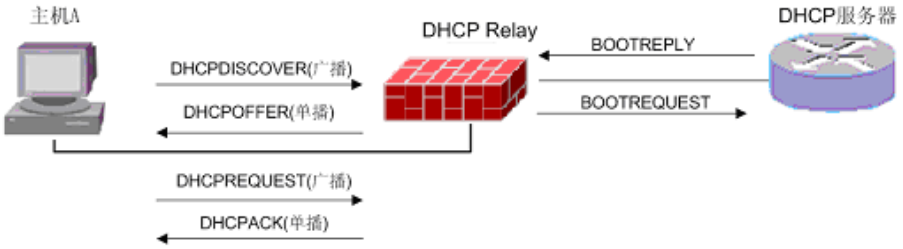
注意

DHCP 客户端可以接收多个 DHCP 服务器的消息，自己从中选一个 DHCP 服务器，同时也暗示它拒绝了其它 DHCP 服务器应答的配置参数。

19.1.2 DHCP Relay概述

DHCP Relay 是用来将一个网段的 DHCP 请求转发给其它网段的 DHCP Server，由其它网段的 DHCP Server 分配 IP 地址。DHCP Relay 存在的原因是因为 DHCP 客户端还没有 IP 环境设定，这时由 DHCP Relay 来接管客户的 DHCP 请求然后将 DHCP 消息传递给 DHCP Server，再将 DHCP 服务器的应答消息传给客户端，客户端获得 IP 地址。当然也可以在每一个网段之中安装 DHCP Server 但这样的话设备成本会增加而且管理上面也比较分散。DHCP Relay 的工作原理如下图所示：

图 13-2DHCP 客户端通过 Relay 从 DHCP 服务器申请 IP 地址



19.2 配置说明

19.2.1 在接口上指定DHCP服务

进入**网络>DHCP>服务**

接口	服务
mgt	空
ge0/0	空
ge0/1	空
ge0/2	空
ge0/3	空

接口：包括物理接口、vlan 口和 trunk 接口。

服务：该接口上启用的 DHCP 服务类型（空、 DHCP 服务器、 DHCP Relay）。

配置接口 DHCP 服务：

点击接口。

接口：接口名称。

服务:

空：表示该接口不启用 DHCP 服务。

DHCP 服务器：表示该接口启用 DHCP 服务器。

DHCP 中继代理：即 DHCP Relay，表示该接口启用 DHCP 中继服务。

编辑框“**DHCP 服务器**”：指该接口上的 DHCP 中继对应的对端 DHCP 服务器地址。

19.2.2 配置DHCP服务器地址池

进入**网络>DHCP>服务器。**

名称：DHCP Server 地址池名称。

子网/掩码：地址池的子网和掩码。

缺省网关：地址池配置的缺省网关。

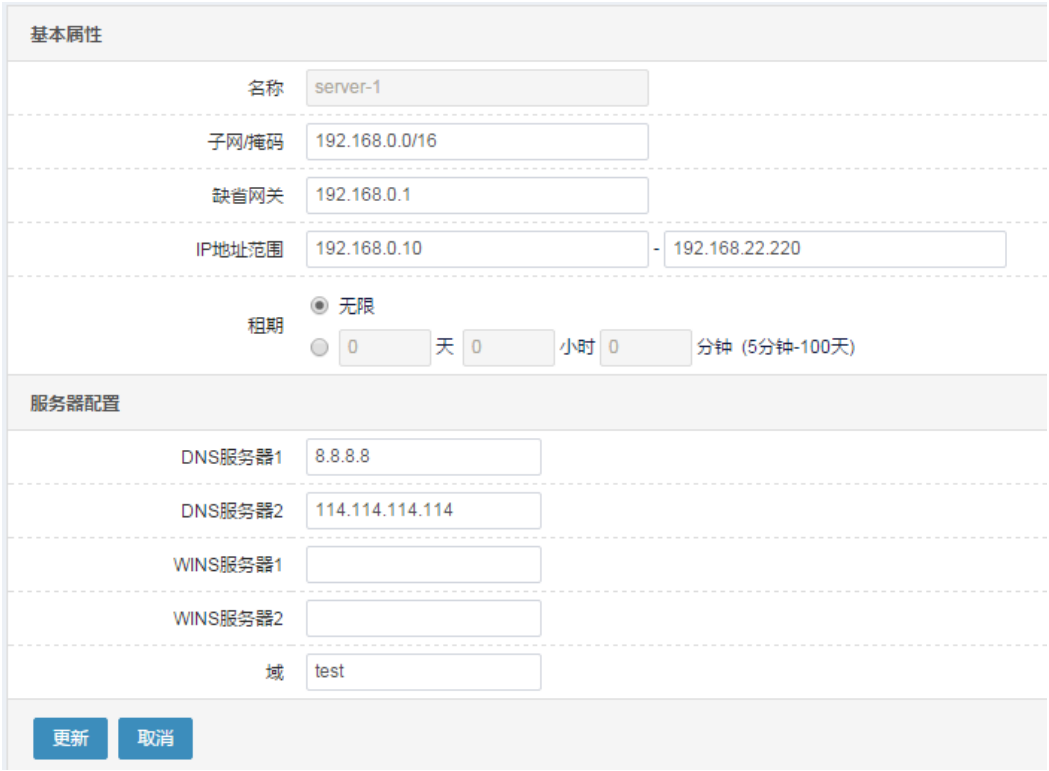
IP 地址范围：地址池范围。

新建：新建一个 DHCP Server 地址池。

：删除该地址池。

配置 DHCP 服务器地址池：

点击**新建**按钮。



名称：DHCP Server 地址池名称。

子网/掩码：地址池的子网和掩码。

缺省网关：地址池配置的缺省网关。

IP 地址范围：地址池范围。

租期：地址租约，可选“无限”或具体租约。

DNS 服务器 1：主 DNS 服务器选项。

DNS 服务器 2：备份 DNS 服务器选项。

WINS 服务器 1：主 WINS 服务器选项。

WINS 服务器 2：备份 WINS 服务器选项。

域：域名选项。

更新：新建该 DHCP Server 地址池。

取消：取消本次配置。

注意

每个子网只可以有 1 个地址池。若租约不为无限，则其取值范围为 5 分钟至 100 天。

19.2.3 配置DHCP服务器地址排除

进入**网络>DHCP>排除范围。**

起始 IP：排除范围的起始地址。

结束 IP：排除范围的结束地址。

新建：新建一个地址排除范围。

：删除该地址排除范围。

配置 DHCP 地址排除：

点击**新建**按钮。

起始 IP：排除范围的起始地址。

结束 IP：排除范围的结束地址。

更新：新建该地址排除范围。

取消：取消本次配置。

19.2.4 配置DHCP服务器地址绑定

进入**网络>DHCP>IP-MAC 绑定。**

名称：DHCP 地址绑定名称。

服务器：该 ip-mac 绑定相关联的 DHCP 服务器

IP 地址：地址绑定对应 IP。

MAC 地址：地址绑定对应 MAC。

新建：新建一个 DHCP 地址绑定。

：删除该地址绑定。

配置 DHCP 地址绑定：

点击**新建**按钮。

名称：DHCP 地址绑定名称。

服务器：关联的 DHCP 服务器

IP 地址：地址绑定对应 IP。

MAC 地址：地址绑定对应 MAC。

更新： 新建该地址绑定。

取消： 取消本次配置。

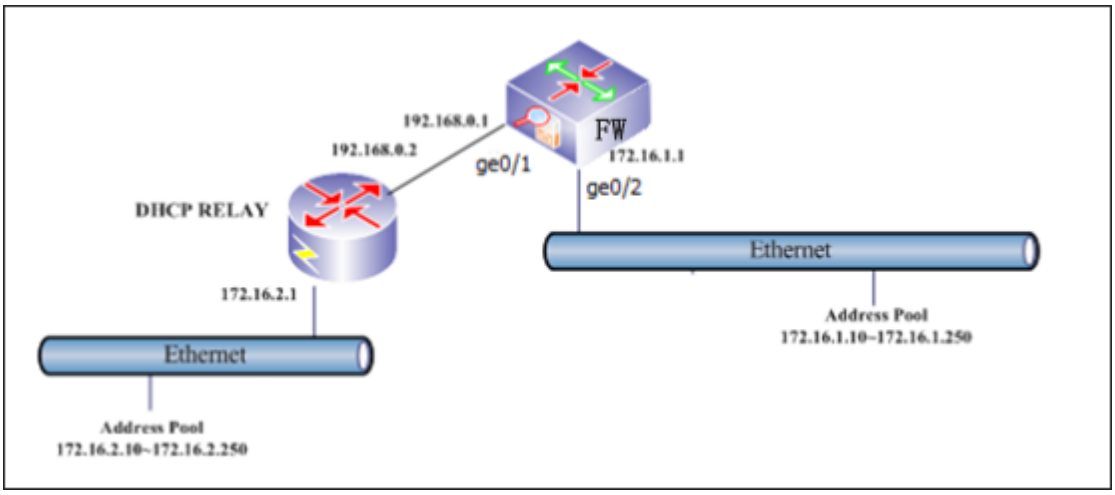
19.3 配置案例

19.3.1 案例1：接口ge0/2配置DHCP Server

案例描述：

配置设备（DHCP Server）给两个子网分配 IP 地址，如下图所示：172.16.1.0/16 为直接相连的子网，172.16.2.0/16 为通过另一台设备（DHCP Relay）后的子网。

图19-1 DHCP 服务配置案例组网图



配置步骤：

1. 进入**网络>DHCP>服务**，点击（接口 ge0/2）**编辑**，如下图：

选中 **DHCP 服务器** 服务选项。

2. 点击提交完成设置。

3. 进入网络>DHCP>服务器，点击新建，如下图：

填写服务器参数；

名称：DHCP Server 地址池名称为“server1(172.16.1.0)”。

子网/掩码：地址池的子网和掩码为“172.16.1.0/24”。

缺省网关：地址池配置的缺省网关为“172.16.1.1”。

IP 地址范围：地址池范围为“172.16.1.10-172.16.1.250”。

租期：地址租约，为“1 天”。

DNS 服务器 1：主 DNS 服务器选项为“202.106.0.20”。

DNS 服务器 2：备份 DNS 服务器选项为“202.99.1.140”。

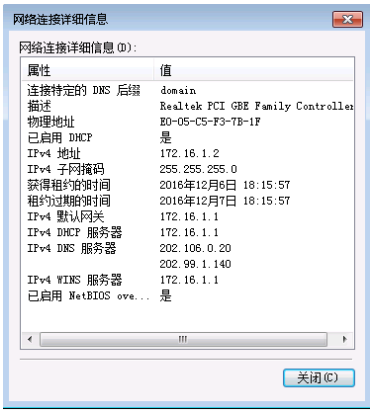
WINS 服务器 1：主 WINS 服务器选项为“172.16.1.1”。

WINS 服务器 2：备份 WINS 服务器选项为空。

域：域名选项为“domain”。

4. 点击提交完成设置。

5. 客户端 pc 配置好自动获取 IP 地址，最终获取的 IP 地址信息如下：



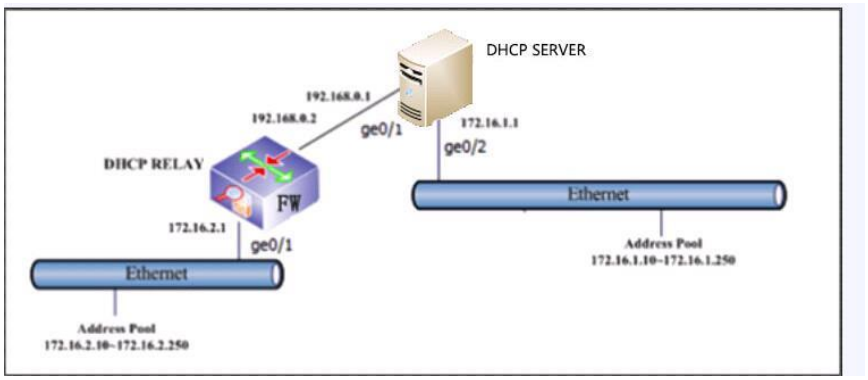
6. 防火墙设备上 DHCP 监视器显示信息如下：

19.3.2 案例2：接口ge0/1配置DHCP Relay

案例描述

配置设备（DHCP RELAY）从 DHCP Server（192.168.0.1）给客户端分配 IP 地址，如下图所示：

图19-2 DHCP Relay 配置案例组网图



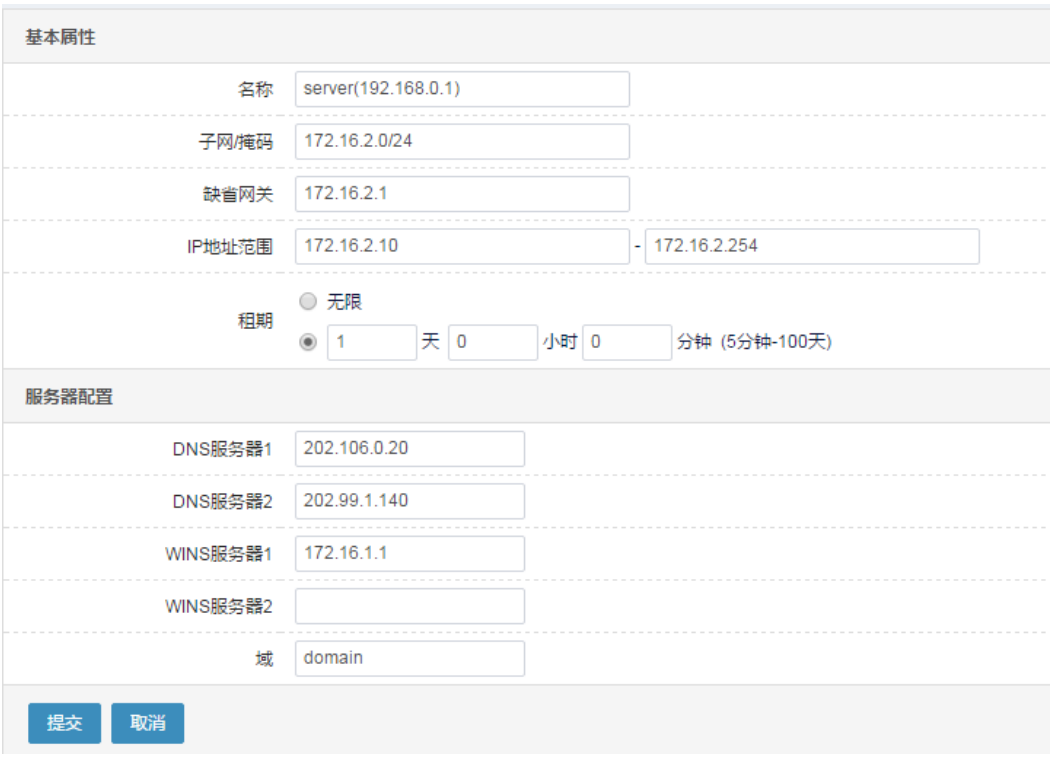
配置步骤：

1. 进入**网络>DHCP>服务**，点击(接口 ge0/1)**编辑**，如下图：

选中 **DHCP 中继代理**， **DHCP 服务器**编辑框上填入 DHCP Server 地址“192.168.0.1”。

2. 点击提交完成设置。

3. 配置 DHCP 服务器：（首先保证 DHCP 服务器到客户端网段 172.16.2.0/24 网络可达）



4. 点击提交完成设置。

19.4 监控与维护

19.4.1 查看DHCP服务器的地址分配

进入**网络>DHCP>监视器**如下图：

IP：该地址租约对应客户端获得的 IP。

MAC：该地址租约对应客户端 MAC。

起始时间：该地址租约申请时间。

结束时间：该地址租约结束时间。

接口选项：显示通过接口分配的地址信息，**所有**为显示所有地址分配信息。

19.5 常见故障分析

19.5.1 故障现象：启用DHCP Server的接口对应的DHCP Client不能获得地址

现象		接口对应的DHCP Client不能获得地址。
分析		1) 该接口是否配置IP地址。 2) 该接口是否启用DHCP Server。 3) DHCP Server是否配置该接口IP对应的地址池。
解决		1) 正确配置接口地址。 2) 该接口启用DHCP Server。 3) DHCP Server正确配置该接口IP对应的地址池。

19.5.2 故障现象：启用DHCP Relay的接口对应的DHCP Client不能获得地址

现象		接口对应的DHCP Client不能获得地址。
分析		1) 该接口地址是否与对端DHCP Server地址互通。 2) 该接口是否启用DHCP Relay，并配置对端DHCP Server地址。 3) 对端DHCP Server是否启用并有对应的地址池。
解决		1) 正确配置接口地址和路由。 2) 该接口启用DHCP Relay并正确配置对端DHCP Server地址。 3) 正确配置对端DHCP Server的地址池，并启用服务。

20 第20章 静态路由

20.1 静态路由概述

静态路由是在路由器中人工配置的固定路由条目。除非网络管理员干预，否则静态路由不会发生变化。由于静态路由不能对网络的改变作出反映，一般用于网络规模不大、拓扑结构固定的网络中。静态路由的优点是简单、高效、可靠。在所有的路由中，静态路由优先级最高。当动态路由与静态路由发生冲突时，以静态路由为准。

设备静态路由支持对路由的健康检查，通过配置健康检查策略，支持对静态路由状态进行监测。当健康检查失败后，会将路由状态置为失效，从而避免数据转发到不可用的下一跳上。

20.2 配置静态路由

20.2.1 配置IPv4静态路由

配置步骤：

进入**网络>路由>静态路由：IPv4**，配置界面如下：

IP 地址/掩码：静态路由的目的网段。

下一跳地址：静态路由网关地址。

出接口：静态路由的出接口。

权重：路由权重，范围 1-100，等价路由情况下按照权重比例轮询转发。

距离：路由优先级，范围<1-255>。

健康检查：引用健康检查模板，支持 TCP 和 ICMP 两种健康检查方式。

点击**提交**，完成设置。

注意

静态路由健康检查的对象只能是路由的下一跳地址。

20.2.2 查看IPv4路由表

配置步骤：

进入**网络>路由>路由表：IPv4**

此界面可以查看系统的路由信息，并且可以根据类型，目的地址及下一跳进行检索。

20.2.3 配置IPv6静态路由

配置步骤：

进入**网络>路由>静态路由：IPv6**

IP 地址/掩码：目的 IPv6 地址及掩码。

下一跳类型：下一跳地址、出接口、下一跳地址和出接口

下一跳地址：路由网关地址。

出接口：数据转发的出接口。

下一跳地址和出接口：路由网关地址和数据转发的出接口。

权重：路由权重，范围 1-100。

距离：路由优先级，范围<1-255>。

点击**提交**，完成设置。

20.2.4 查看IPv6路由表

配置步骤：

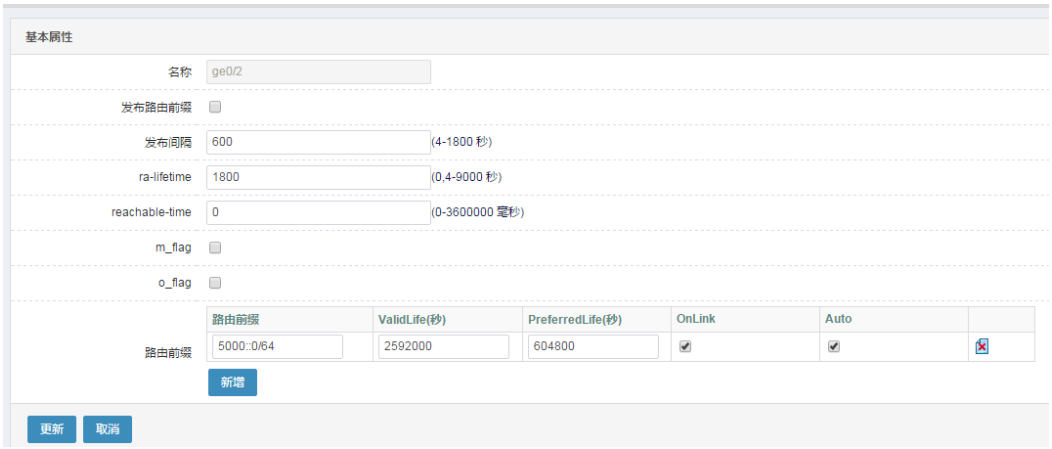
进入**网络>路由>路由表>IPv6**

此界面可以查看系统的路由信息，并且可以根据类型，目的地址及下一跳进行检索。

20.2.5 IPv6前缀公告

配置步骤：

进入**网络>路由> IPv6 前缀公告**



名称：发生路由前缀的 vlan 接口名称

发布路由前缀：启用/关闭前缀公告

发布时间间隔：每发布一次路由前缀的时间间隔

ra-lifetime：路由前缀生存时间

reachable-time：路由器可到达时间

m_flag：管理地址配置标示

o_flag：其他状态配置标示

路由前缀：所要发布的路由前缀

ValidLife：路由前缀有效生存时间

PreferredLife：路由前缀首选生存时间

点击**更新**完成设置。

20.3 配置案例

20.3.1 配置案例1：对多条路由配置路由监控

案例描述：

某企业有多个出口，下一跳地址分别为 30.1.1.1、31.1.1.1 和 32.1.1.1。

用户需求如下：

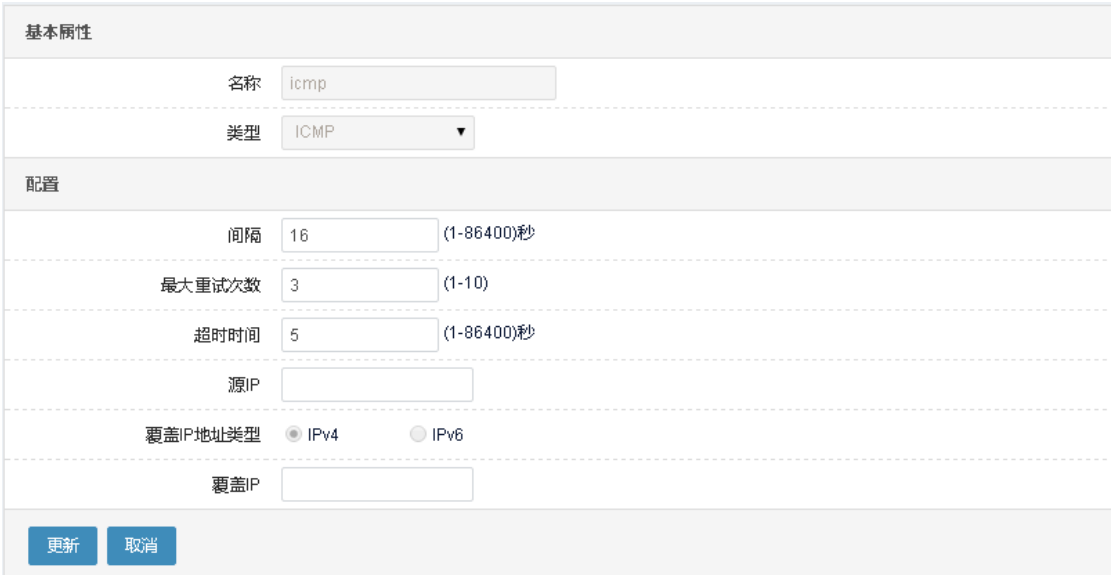
1. 配置两条默认路由，同时需要对下一跳的可用性进行健康检查。当健康检查失败，则将路由状态置为失效，以保证业务可以转发到其他可用下一跳上。

2. 对 30.1.1.1 和 31.1.1.1 下一跳需要使用 icmp 方式进行健康检查，32.1.1.1 下一跳需要使用 tcp 方式进行健康检查。

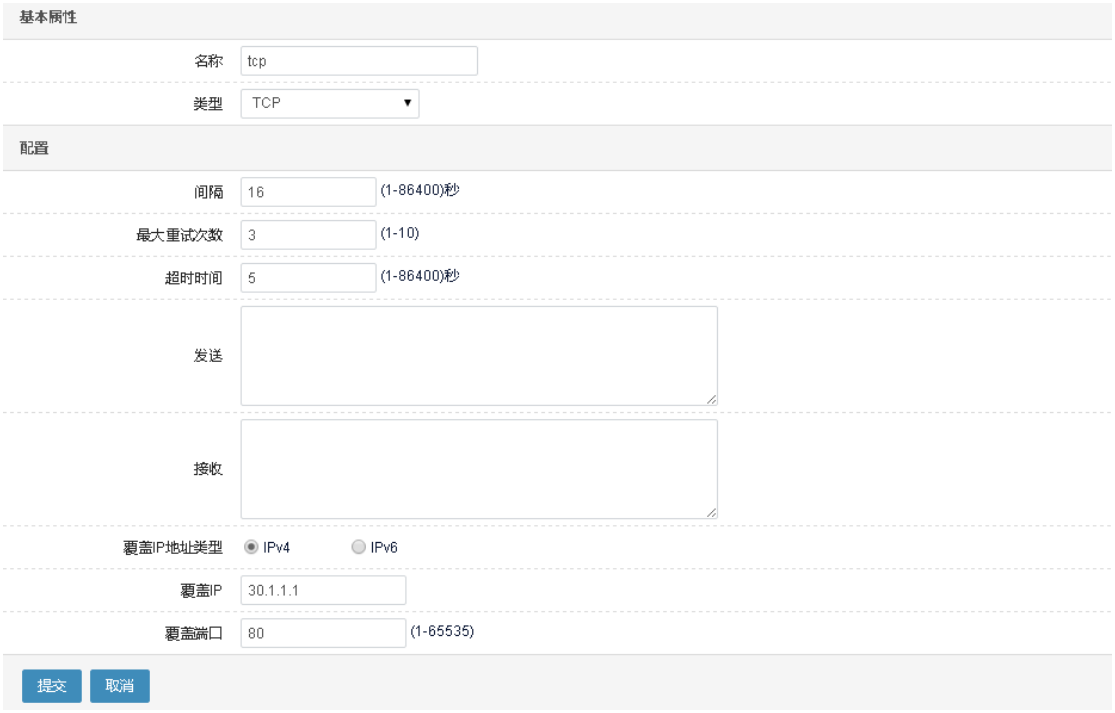
配置步骤：

1. 进入**对象>健康检查**，创建 ICMP 类型的健康检查。覆盖 IP 不填写则自

动选择路由的下一跳作为健康检查的对象。



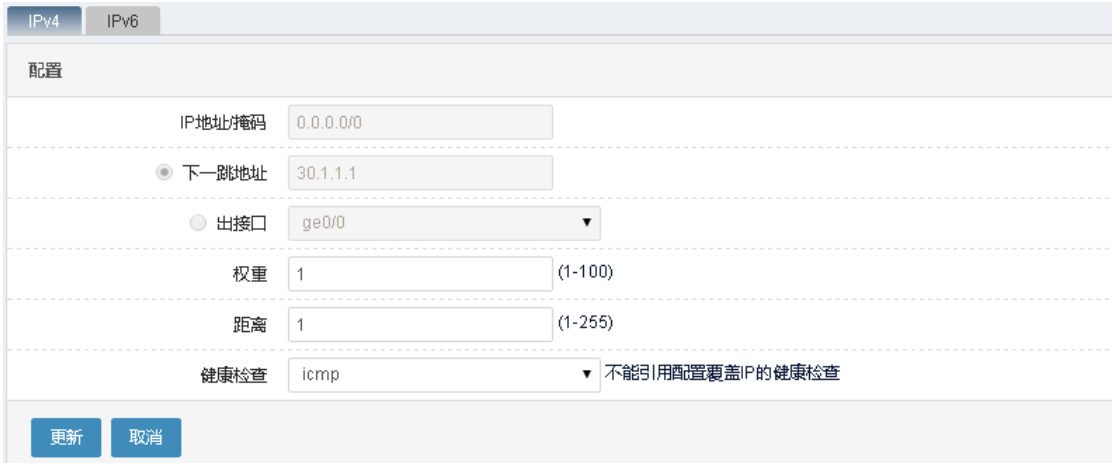
2. 进入对象>健康检查，创建 TCP 类型的健康检查。覆盖 IP 填写路由下一跳地址，覆盖端口填写下一跳开放的端口。



3. 进入**网络>路由>静态路由**，配置添加三条默认路由，30.1.1.1 和 31.1.1.1

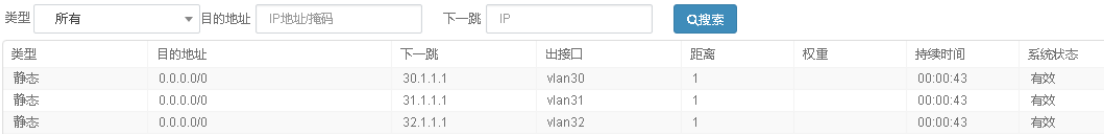
下一跳引用 icmp 健康检查模板，32.1.1.1 下一跳引用 tcp 健康检查模

板。



4. 进入**网络>路由>路由表**，查看路由状态，健康检查成功，路由状态显示

为有效。若健康检查失败，则路由会显示为失效状态。



20.4 常见故障分析

20.4.1 路由状态为失效状态

故障现象	配置了静态路由后，路由状态显示为失效状态
分析	若静态路由没有配置健康检查，从以下几点分析： 1. 路由配置的下一跳地址对应出接口down。 2. 依据路由配置的下一跳地址查找不到出接口。 3. 相同路由情况下，有管理距离更优的路由。 若静态路由配置了健康检查，除了上述内容外，还需要从以下几点分析： 1. 检查健康检查日志，是否由于路由健康检查失败导致的静态路由失效。 2. 检查是否健康检查模板覆盖IP地址配置了非下一跳的IP地址。 3. 检查是否健康检查的配置的超时时间和重试次数过短，健康检查报文在超时时间内没有返回则认为健康检查失败。
解决	检查上面分析中的配置是否正确。

21 第21章 静态路由 BFD

21.1 BFD概述

BFD(Bidirectional Forwarding Detection，双向转发检测)协议提供一种轻负载、快速检测两台邻接路由器之间转发路径连通状态的方法。协议邻居通过该方式可以快速检测到转发路径的连通故障，加快启用备份转发路径，提升现有网络性能。

21.2 配置说明

21.2.1 配置静态路由BFD

进入**网络>路由>静态路由 BFD**

源地址：静态路由 BFD 的源地址。

下一跳地址：静态路由 BFD 的目的地址，即静态路由的下一跳地址。

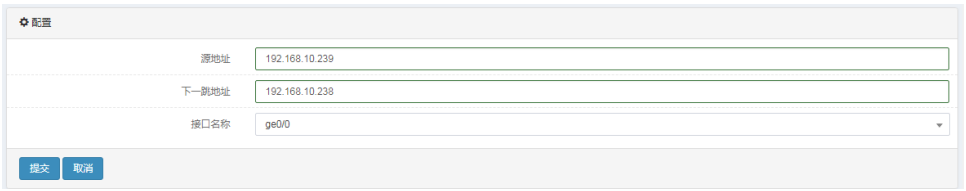
接口名称：与下一跳连接的接口名称。

新建：新建一条静态路由 BFD。

：删除该条静态路由 BFD。

配置静态路由 BFD：

点击**新建**按钮。



源地址：静态路由 BFD 的源地址。

下一跳地址：静态路由 BFD 的目的地址，即静态路由的下一跳地址。

接口名称：与下一跳连接的接口名称。

提交：新建该条静态路由 BFD。

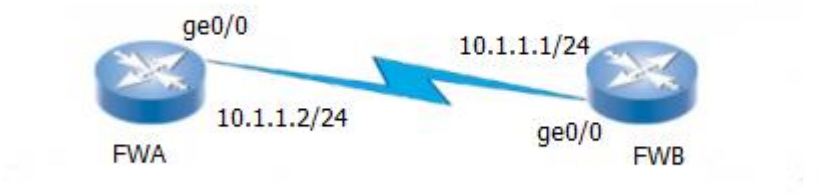
取消：取消本次配置。

21.3 配置案例

21.3.1 配置BFD与静态路由联动

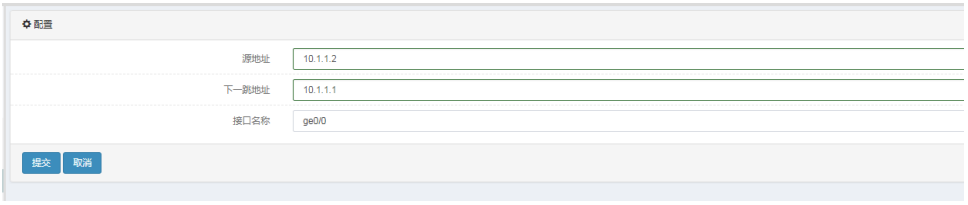
案例描述：

设备配置一条静态路由，下一跳指向另一台设备，为了能快速发现下一跳是否出现故障，在静态路由上启用 BFD 检测功能，当链路出现故障的时候，能够快速检测。



FWA 的配置步骤：

1、进入**网络>路由>静态路由 BFD**，点击新建，如下图：



源地址：静态路由 BFD 的源地址为 10.1.1.2。

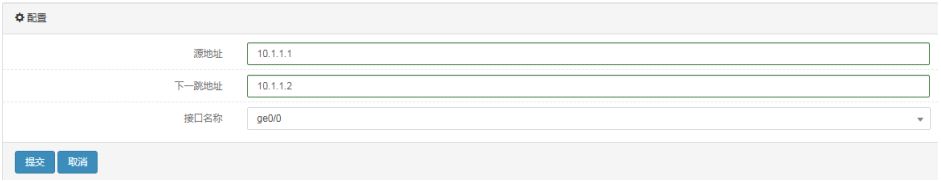
下一跳地址：静态路由 BFD 的目的地址，即静态路由的下一跳地址为 10.1.1.1。

接口名称：与下一跳连接的接口名称是 ge0/0。

2、点击**提交**完成设置。

FWB 的配置步骤：

1、进入**网络>路由>静态路由 BFD**，点击新建，如下图：



源地址：静态路由 BFD 的源地址为 10.1.1.1。

下一跳地址：静态路由 BFD 的目的地址，即静态路由的下一跳地址为 10.1.1.2。

接口名称：与下一跳连接的接口名称是 ge0/0。

2、点击**提交**完成设置。

21.4 故障分析

21.4.1 BFD邻居建立失败

现象	两端配置静态路由bfd，但是bfd邻居建立失败
分析	● bfd邻居地址是否配置错误 ● 接口地址是否配置错误 ● 两端接口IP是否互通

22 第22章 RIP 路由

22.1 RIP协议概述

RIP 协议是一种基于 D-V 算法（又称为 Bellmen-Ford 算法）的内部动态路由协议（即 IGP, Interior Gateway Protocol）,它通过 UDP 数据报交换路由信息。D-V 算法又称为距离向量算法,这种算法在 ARPARNET 早期就用于计算机网络的路由的计算。RIP 协议在目前已成为路由器、主机路由信息传递的标准之一，是使用最广泛的 IGP 之一，被大多数 IP 路由器商业卖主广泛使用。 RIP 协议被设计用于使用同种技术的中小型网络，因此适应于大多数的校园网和使用速率变化不是很大的连续的地区性网络。对于更复杂的环境，一般不使用 RIP 协议。

RIP 协议使用路由权(即跳数)来衡量到达目标主机的距离，RIP 协议使用两种形式的报文：路径信息请求报文和路径信息响应报文。在路由器端口第一次启动时，将会发送请求报文。路径信息响应报文包含了实际的路由信息，以 30 秒的间隔发送给相邻端口。在 RIP 协议中，还使用了水平分割、毒性逆转机制来消除路由环路，并且使用触发更新和路由超时机制确保路由的正确性。

22.2 配置RIP协议

22.2.1 缺省配置信息

T 系列防火墙设备关于 RIP 的缺省设置信息如以下表所示：

RIP 缺省配置信息

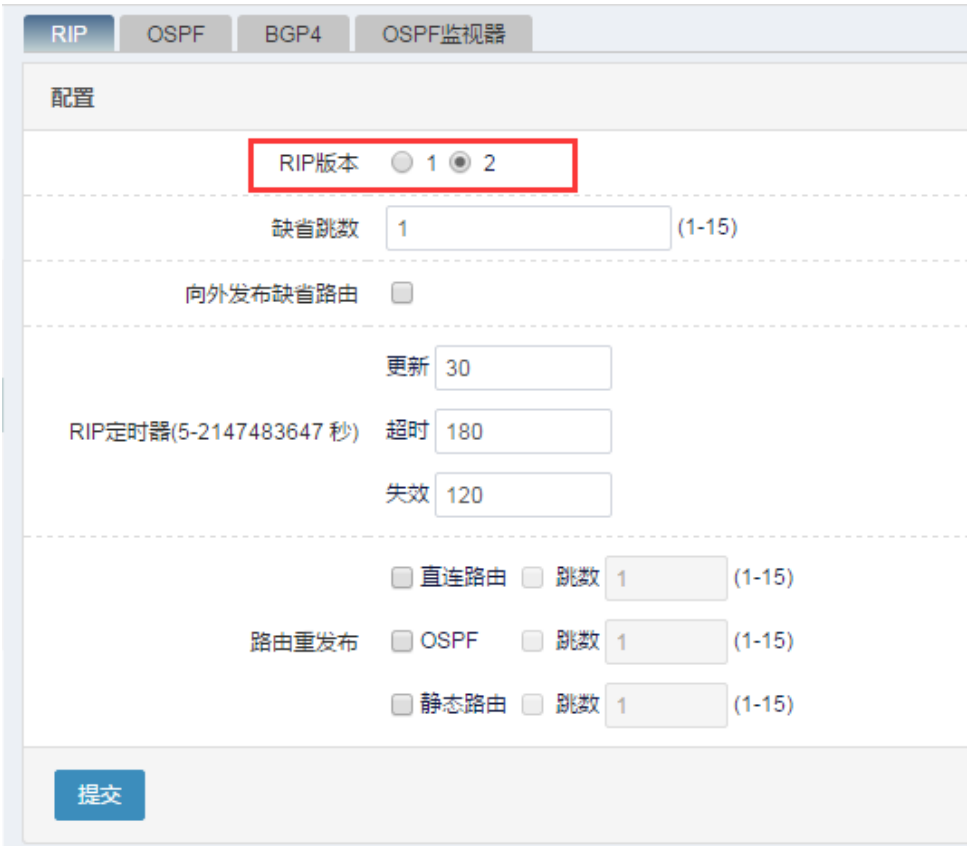
内容	缺省设置	备注
使能/禁止状态（enable/disable）	disable	可更改设置
接口认证类型（none/text/md5）	none	可更改设置
版本	2	可更改设置
定时更新时间	30秒	建议采用缺省设置
超时时间	180秒	建议采用缺省设置
垃圾收集时间	120秒	建议采用缺省设置

22.2.2 配置RIP版本

RIP 的版本配置，在接口没有做出版本配置的情况下控制 RIP 协议收发报文的版本信息。高级选项如果没有设置，则按默认信息提交。

配置步骤：

1. 进入**网络>路由>动态路由>RIP**：



参数说明：

RIP 版本：RIP 的版本 1 或者 2

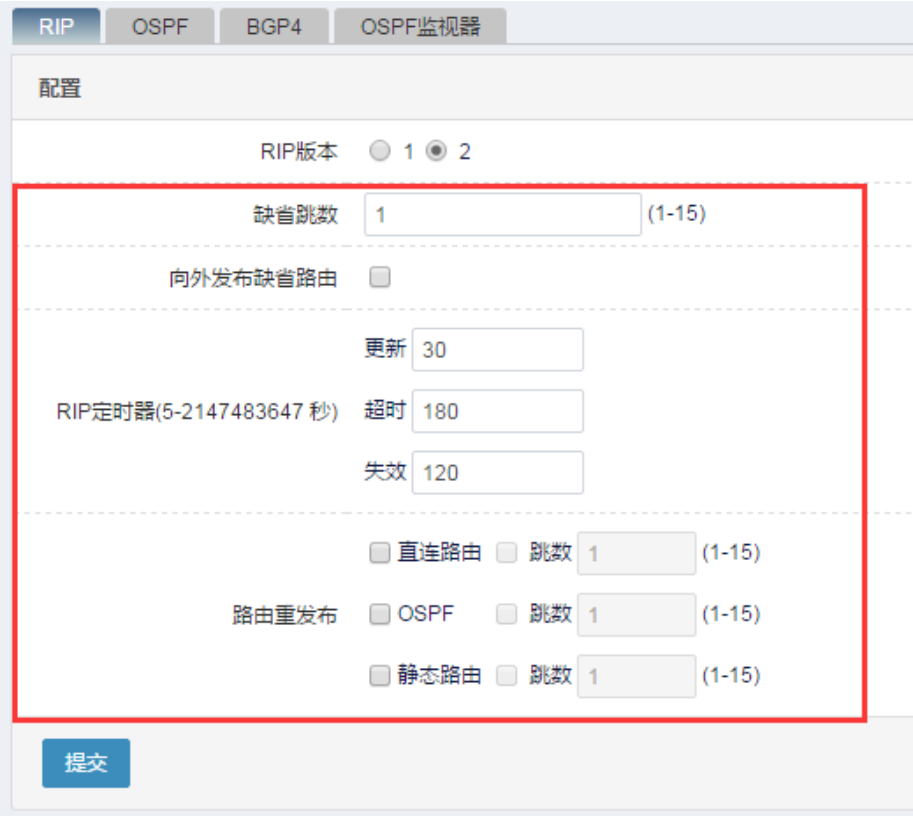
2. 点击**提交：**完成对版本的设置，并按默认值提交高级选项。

22.2.3 配置RIP高级选项

高级选项中涉及到缺省重发布度量，缺省路由重发布的设置，定时更新、超时、垃圾收集三个定时器的触发时间，还有重发布的路由类型。

配置步骤：

1. 进入**网络>路由>动态路由>RIP**：



参数说明：

缺省跳数：设置重发布路由的缺省跳数

向外发布缺省路由：设置是否产生缺省路由并发布出去

RIP 定时器-更新：设置定时更新的触发时间

RIP 定时器-超时：设置超时定时器的触发时间

RIP 定时器-失效：设置垃圾收集定时器的触发时间

路由重发布-直连路由：设置是否重发布直连路由

路由重发布-OSPF：设置是否重发布 OSPF 路由

路由重发布-静态路由：设置是否重发布静态路由

跳数：三种重发布类型进行重发布时的度量

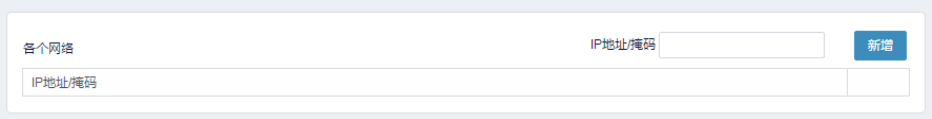
2. 点击**提交**：完成对 RIP 的设置。

22.2.4 配置RIP发布的网络

把系统所在的直连网络发布出去，使其他路由器能够学到到达本地网络的路由。

配置步骤：

1. 进入**网络>路由>动态路由>RIP**：



IP 地址/掩码：本机直连网络地址，按 A.B.C.D/M 格式输入。

2. 点击**新增**：完成对网络的添加

3. 点击  ：删除对应配置的网络。

22.2.5 配置RIP接口

配置接口收发报文的版本和认证类型。

配置步骤：

1. 进入**网络>路由>动态路由>RIP**：

2. 点击**新增**：进入接口配置页面。

接口：需要进行配置的接口名

发送版本：接口的发送报文版本

接收版本：接口的接收报文版本

认证算法：接口的认证类型

点击**提交**：完成对接口的配置

点击**取消**：取消对接口的配置

3. 按上图配置，点击**提交**

点击**接口名称**：对已有的接口配置进行编辑。

点击  ：删除对应接口的配置。

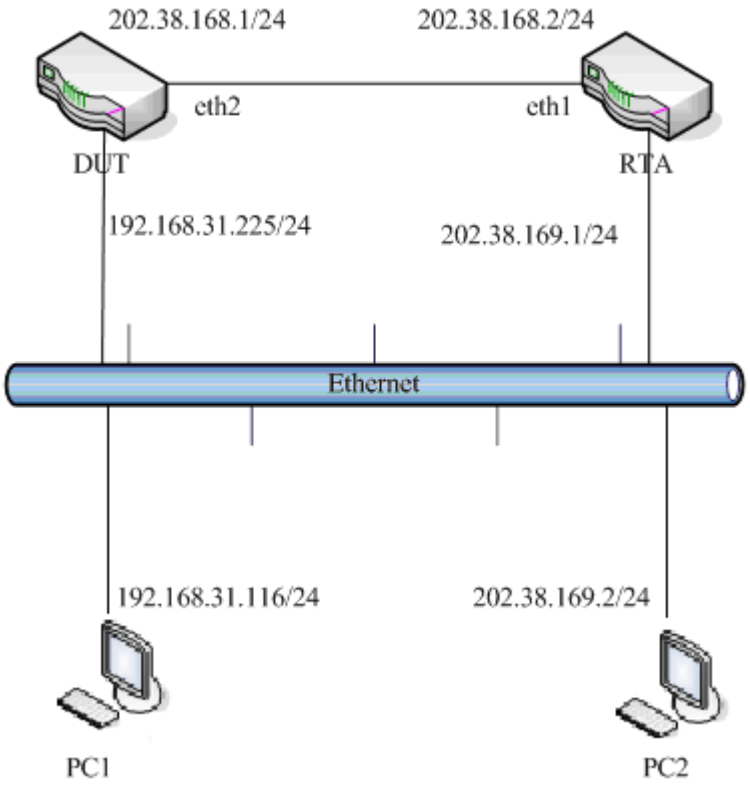
22.3 配置案例

22.3.1 配置案例：配置两台T系列防火墙设备互连

案例描述

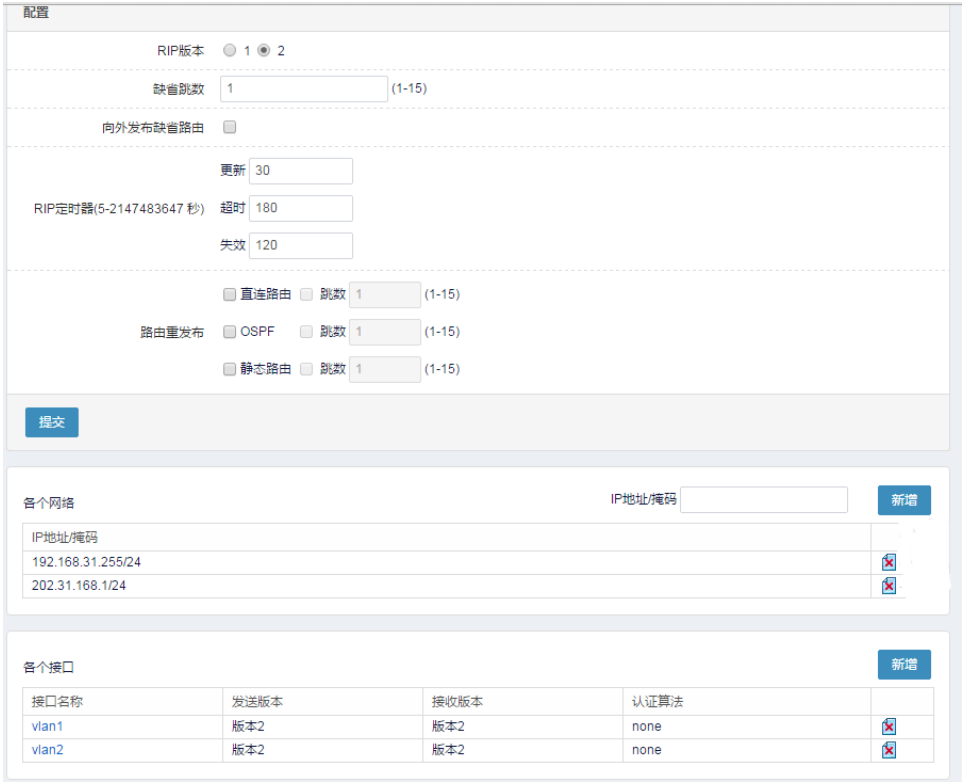
DUT 和 RTA 都为 T 系列防火墙设备，IP 地址配置如图，DUT 在 vlan1 和 vlan2 接口上启用了 RIP，RTA 在接口 vlan1 和 vlan2 上启用了 RIP，两个设备互连的接口收发报文的版本都设置为 2）。

案例组网图：



配置步骤：

1. 配置 DUT 的基本信息。



2. RTA 的基本配置。

3. 配置 PC1 的网关为 192.168.31.225，配置 PC2 的网关为 202.38.169.1。从 PC1PING 向 PC2，可以 PING 通。

22.4 查看RIP配置信息

22.4.1 查看RIP配置信息

进入**网络>路由>动态路由>RIP**，可以查看 **RIP 的配置。**

22.5 常见故障分析

22.5.1 故障现象1：两台设备不能正常通信

现象	两台设备不能正常通信
分析	互连接口收发版本不匹配，认证类型不匹配，接口配置是否正确
解决	检查接口配置，修改接口配置

23 第23章 OSPF 路由

23.1 OSPF协议概述

OSPF(Open Shortest Path First)是动态路由协议,其功能是实现网际间的路由。

OSPF(Open Shortest Path First)是一个内部网关协议(Interior Gateway Protocol, IGP），用于在单一自治系统（autonomous system,AS）内决策路由。与 RIP 等距离向量路由协议不同的是，OSPF 是基于链路状态的路由协议。它能够在网络链路变化时快速产生新路由，并能够管理比 RIP 范围更大的网络自治系统。

OSPF 是自治系统内部使用的链路状态路由协议，OSPF 通过路由器之间通告链路状态信息（LSA）来建立链路状态数据库，然后就可以根据 SPF 算法计算出到每个结点的最短路径树了，进而可计算出路由。它的工作方式与我们熟悉的 RIP 和 IGRP 协议不同，OSPF 只须发送当前结点到相邻结点的路由结构信息，而 RIP 和 IGRP 需要结点把自己保留的路由表或路由表的一部分全部发送到相邻结点，相邻结点根据这些信息更新自己的路由表，显然 OSPF 协议发送的信息量少，而 RIP 发送的信息量较多。在通告的链路状态结构中，OSPF 协议支持 IP 子网结构。

OSPF 向相邻的路由器定期发送一个 hello 报文，并接收邻居路由器发来的 hello 报文。这个 hello 报文不但可以帮助路由器在初始工作时了解相邻结构，而且可以在运行中了解相邻路由器的工作情况，如果相邻的路由器关机了，或链路不通了，就不会从相应邻居那里收到 hello 报文了，从而能够很快知道哪些路由器不能工作了，能够对网络拓扑结构的变化做到快速反应。

如果网络支持多个路由器，可以实现在一个网段的诸多 OSPF 路由器中选择一个指定路由器 DR 和一个备份指定路由器 BDR，在进行链路数据库同步时，由指定路由器向整个网络发送 LSA，以减少流量开销。

23.2 配置OSPF协议

23.2.1 缺省配置信息

T 系列防火墙设备关于 OSPF 的缺省设置信息如以下表所示：

OSPF 缺省配置信息

1. 内容	2. 缺省设置	3. 备注
使能/禁止状态（enable/disable）	disable	可更改设置

OSPF 区域认证类型（none/text/md5）	不认证	可更改设置
接口认证类型（none/text/md5）	不认证	可更改设置
发布缺省路由	不发布	可更改设置
LSA重传时间	5秒	建议采用缺省设置
LSA发送延迟	1秒	建议采用缺省设置
Hello-interval值	10秒	可更改设置
Dead-interval值	4* Hello-interval	可更改设置
接口选举DR的优先级	1	可更改设置

23.2.2 配置OSPF

OSPF 协议需要路由器的 ID，作为本路由器在自治系统中的唯一标识。一般在协议任务启动后，会自动选出一个路由器 ID。路由器 ID 的选择机制是先看是否有环回口，有则选取最大的环回地址。无环回口则挑选最大的接口 IP 地址。除此之外可以手工指定一个路由器 ID，建议手工指定路由器 ID。

路由重发布是将其他类型的路由发布到 OSPF 自制系统内。

1．进入**网络>路由>动态路由>OSPF**

路由器 ID：在路由器 ID 后输入路由器 ID。如果不输入，如后面的提示，系统会自动选取路由器 ID。

缺省路由：设置是否发布默认路由。当路由表中没有缺省路由信息，要发布默认路由，须选择强制发布选项。

直连路由：设置是否重发布直连路由。

静态路由：设置是否重发布静态路由。

RIP 路由：设置是否重发布 RIP 路由。

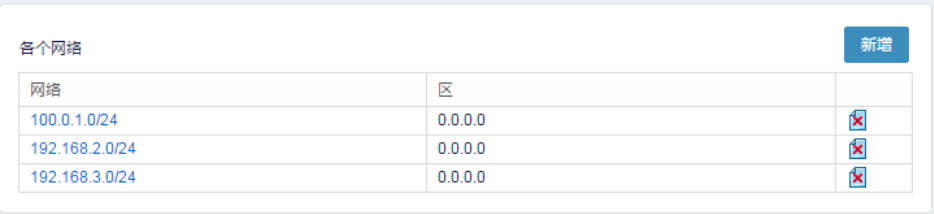
权重：三种重发布类型重发布的权重。

2. 点击**提交：**完成对 OSPF 的设置。

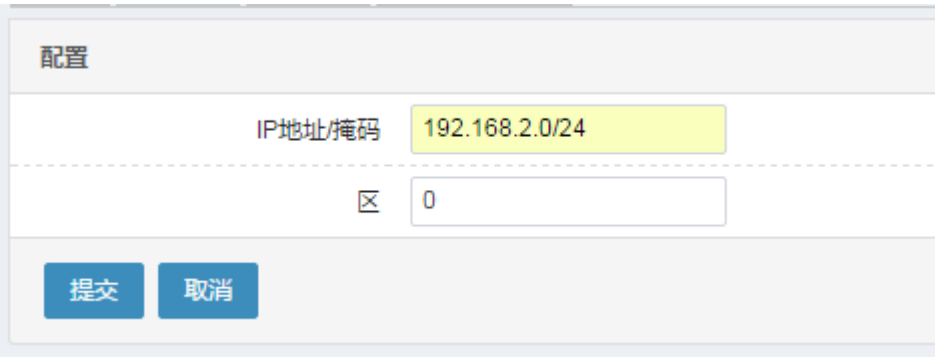
23.2.3 配置OSPF的网络

配置运行 OSPF 的接口以及其所属的区域。

1. 进入**网络>路由>动态路由>OSPF**



2. 点击**新增**：



IP 地址/掩码：网络地址和网络地址掩码

区域：区域 ID

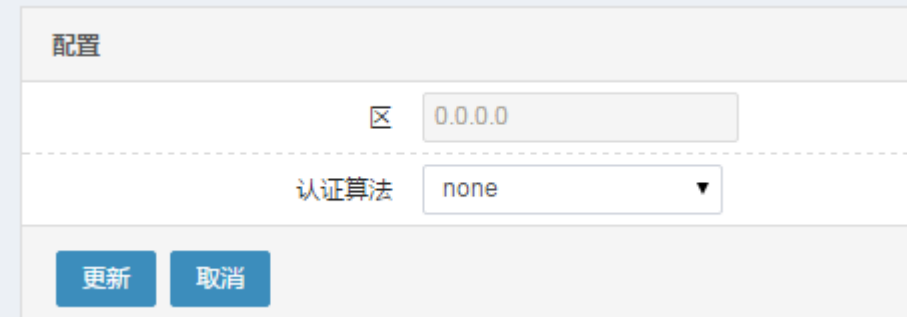
3.点击**提交**。

23.2.4 编辑区域属性

编辑区域的认证方式：

1. 进入**网络>路由>动态路由>OSPF。**

2. 点击**区域** ID 编辑区域属性。



区：区域 ID

认证：认证方式，可以选择 none（不认证）、text（明文认证）、md5（密文认证）

3. 点击**更新**。

23.2.5 配置OSPF接口

配置接口收发报文的版本和认证类型。

配置步骤：

1. 进入**网络>路由>动态路由>OSPF。**

2. 点击**新增：**进入接口配置对话框。

接口：需要进行配置的接口名。

优先级：接口进行 DR/BDR 选举时的优先级。

发送开销：发送报文的开销值（cost）。0 表示根据接口类型和速率自动计算。

网络类型：接口的 OSPF 网络类型

认证类型：认证类型。none（不认证）、text（明文认证）、md5（密文认证）

密码：明文认证类型时的密钥。（认证算法为 text 时）

ID：Key-ID。（认证密码为 MD5 时）

密钥：密文认证时候的密钥。（认证密码为 MD5 时）

Hello 间隔：Hello 报文发送间隔时间。

Dead 间隔：邻居路由器失效间隔时间。

重传间隔：LSA 重传间隔时间。

发送延迟：LSA 发送延迟。

点击**提交**：完成对接口的配置。

点击**取消**：取消对接口的配置。


注意

1. 如果 OSPF 接口采用默认参数配置时，点击提交后 web 不显示相应的配置接口信息。只有参数配置不全是默认参数配置时才会显示在 OSPF 接口信息。

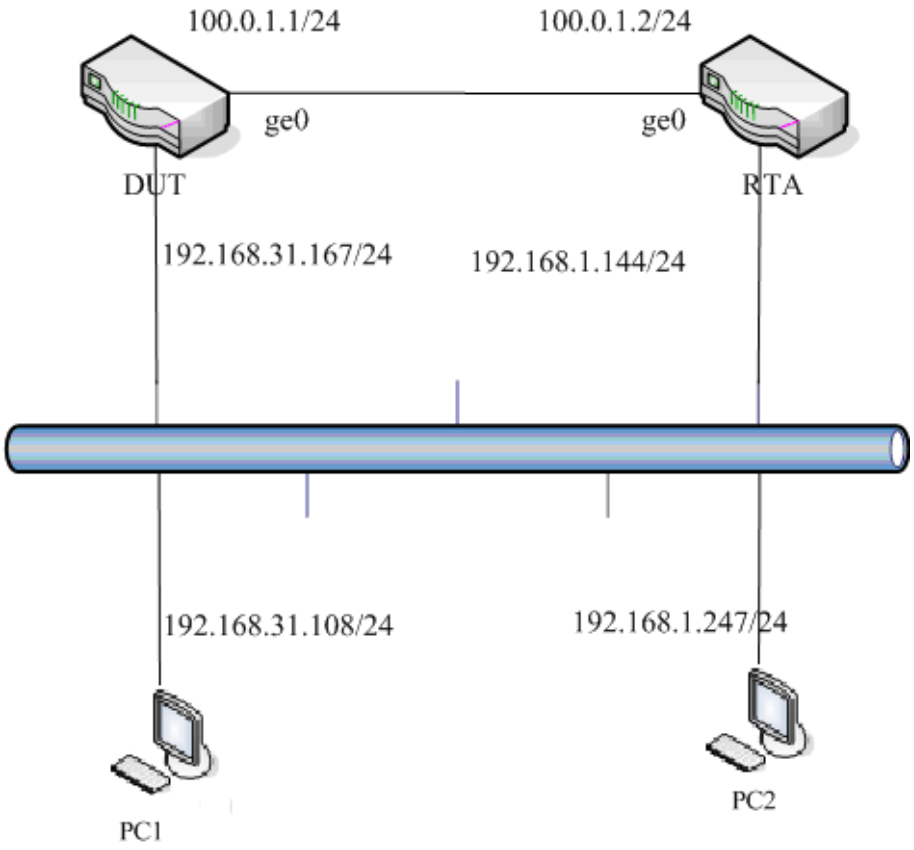
23.3 配置案例

23.3.1 配置案例：配置两台T系列防火墙设备互连

案例描述

DUT 和 RTA 都为 T 系列防火墙设备，IP 地址配置如图，通过在两台设备上使用 OSPF，DUT 设备能学到 192.168.1.0/24 网段的路由，RTA 能学到 192.168.31.0/24 网段的路由。

案例组网图：

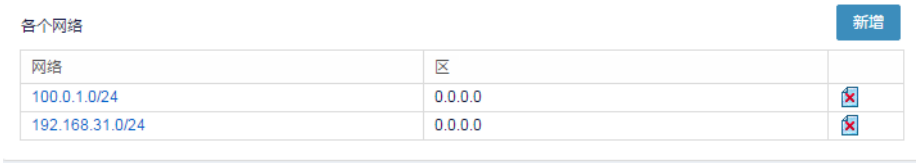


配置步骤：

1. 配置 DUT 的基本信息。

路由器 ID 自动选举产生，所以可以不输入路由器 ID，直接**提交**。

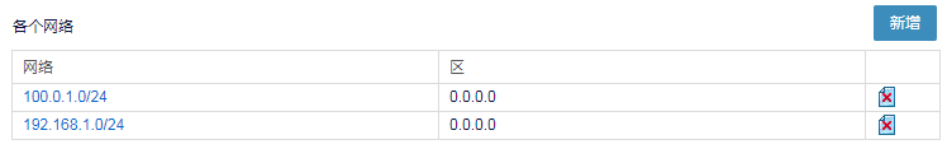
2. 配置 DUT 发布的网络。



3. 配置 RTA 的基本信息：

路由器 ID 自动选举产生，所以可以不输入路由器 ID，直接**提交**。

4. 配置 RTA 发布的网络：



23.4 OSPF监控与维护

23.4.1 查看邻居路由器状态信息

进入**路由>动态路由>OSPF>监视器**，可以查看**邻居路由**状态信息：

23.5 常见故障分析

23.5.1 故障现象：两台设备不能建立邻接关系

现象	两台设备不能建立邻接关系
分析	1. 区域ID不匹配 2. 认证类型不匹配 3. 密钥不匹配 4. 网段（网络掩码不匹配） 5. Hello-interval不匹配 6. Dead-interval不匹配 7. 两台设备间是否需要建立邻接关系？
解决	1. 检查接口上OSPF参数的配置 2. 是否应该和邻居路由器建立一个邻接关系，满足下列条件中的一个或者多

	个，那么将建立邻接关系： A、 网络类型是点对点的 B、 网络类型是点到多点的 C、 网络类型是虚链路 D、 本地路由器是邻接路由器所在网络的 DR E、 本地路由器是邻接路由器所在网络的 BDR F、 邻居路由器是 DR G、邻居路由器是 BDR

24 第24章 BGP 路由

24.1 BGP协议概述

BGP（Border Gateway Protocol）是一种不同自治系统的路由器之间进行通信的外部网关协议(Exterior Gateway Protocol，EGP)，其主要功能是在不同的自治系统(Autonomous Systems，AS)之间交换网络可达信息，并通过协议自身机制来消除路由环路。

BGP 使用 TCP 协议作为传输协议，通过 TCP 协议的可靠传输机制保证 BGP 的传输可靠性。

运行 BGP 协议的 Router 称为 BGP Speaker，建立了 BGP 会话连接(BGP Session)的 BGP Speakers 之间被称作对等体(BGP Peers)。BGP speaker 之间建立对等体的模式有两种： IBGP(Internal BGP)和 EBGP(External BGP)。IBGP 是指在相同 AS 内建立的 BGP 连接，EBGP 是指在不同 AS 之间建立的 BGP 连接。二者的作用简而言之就是：EBGP 是完成不同 AS 之间路由信息的交换，IBGP 是完成路由信息在本 AS 内的过渡。

本产品支持的是版本是 BGP-4，具有如下特点：

支持配置 router-id

支持手动指定 BGP 对等体

支持 BGP 对等体组

支持使用 Loopback 接口

支持多跳跃 EBGP 连接

支持接收路由数量限制

支持过滤私有 AS 号

支持定时器设置

支持 BGP 和 IGP 交互

支持 BGP 路由聚合

支持 BGP 路由衰减

支持 BGP 路由反射器

支持 AS 联盟

支持管理距离配置

支持 BGP 软复位

支持 BGP 的监控和维护

支持的路由属性主要有以下十种：

ORIGN

AS_PATH

NEXT_HOP

MULTI_EXIT_DISC

LOCAL-PREFERENCE

ATOMIC_AGGREGATE

AGGREGATOR

COMMUNITY

ORIGINATOR_ID

CLUSTER_LIST

除此而外，还支持对接收和发布的路由实施策略，支持 AS 路径列表过滤，访问列表(access list)、前缀列表(prefix list)、分发控制列表(distribute-list)和路由映射(Route map)过滤器。

24.2 配置BGP协议

24.2.1 缺省配置信息

BGP 缺省配置信息

内容	缺省设置	备注
1. 路由器ID	如果配置了loopback接口，就从loopback接口中选择IP地址最大的，否则就从物理接口中选择IP地址最大的。	可更改设置
2. 缺省路由生成	不生成	可更改设置
3. EBGP多跳	关闭/255	可更改设置
4. 发布缺省路由	不发布	可更改设置
5. TCP MD5认证	不认证	不可更改设置
6. Keepalive Time值	60秒	建议采用缺省设置

7.	Holdtime 值	180秒	可更改设置
8.	ConnectRetry time	120秒	不可更改设置
9.	AdvIntelval（IBGP）	15秒	建议采用缺省设置
10.	Advintelval(EBGP)	30秒	建议采用缺省设置
11.	Bgp scan time	60秒	可更改设置
12.	MED值	0	可更改设置
13.	Local_pref值	100	可更改设置
14.	路由聚合	关闭	可更改设置
15.	路由衰减	关闭	可更改设置
16.	Suppress limit	2000	可更改设置
17.	Half-life-time	15minutes	可更改设置
18.	Reuse limit	750	可更改设置
19.	Max-suppress time	4*half-life-time	可更改设置
20.	管理距离	EBGP 20 IBGP 200 Local 200	
21.	IGP 路由检查	不检查	可更改设置

24.2.2 配置BGP Router-ID

BGP 协议需要路由器的 Router-ID，作为本路由器在自治系统中的唯一标识。一般在协议任务启动后，会自动选出一个 Router-ID。通常路由器先挑选 IP 地址最大的环回地址。若无环回地址，则选择状态 up 的接口地址大的作为本路由器的 Router-ID.也可以指定一个 Router-ID。高级选项如果没有设置，则按默认信息提交。

配置步骤：

1. 进入**网络>路由>动态路由>BGP4**

参数说明：

路由器 ID：在路由器 ID 后输入路由器 ID。如果不输入，系统会自动选取路由器 ID。

2. 点击**提交：**完成对路由器 ID 设置，并且按照高级选项的默认值进

行配置。

24.2.3 配置运行BGP

配置启动 BGP

配置步骤：

1. 进入**网络>路由>动态路由>BGP4**

参数说明：

本地自治系统号：1 到 4294967295

2. 点击**提交：**运行 BGP。

24.2.4 配置指定BGP的对等体

配置指定 BGP 的对等体

配置步骤：

1. 进入**网络>路由>动态路由>BGP4：**

2. 点击**新增：**

IP 地址：远端对等体的地址

远端 AS：远端的自治系统号

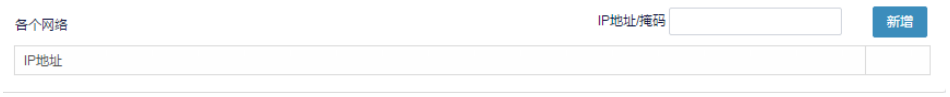
3. 点击**提交**：提交对应的配置。点击**取消**：取消本次配置。

24.2.5 配置宣告网络

配置宣告网络：

配置步骤：

1. 进入**网络>路由>动态路由>BGP4：**



IP 地址/掩码：对应要宣告的地址和子网掩码

2. 点击**新增**：完成添加。

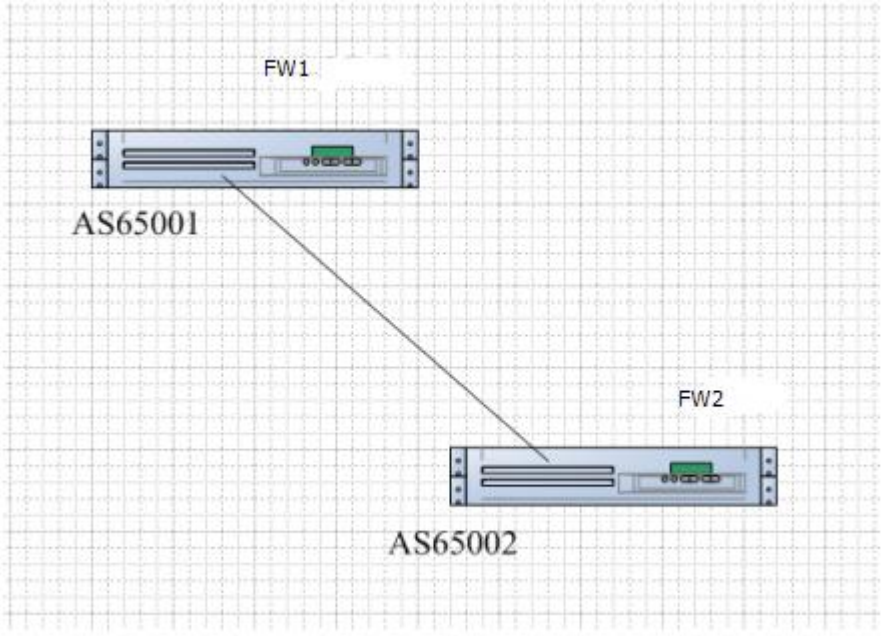
24.3 配置案例

24.3.1 配置案例1：配置两台FW设备互连

案例描述：

FW1 和 FW2 同为 T 系列防火墙设备，FW1 属于 AS65001，router-id 是 192.168.31.106，FW2 属于 AS65002，router-id 是 192.168.31.107，他们之间建立 EBGP 对等体。

案例组网图：



配置步骤：

1. FW1 配置运行 BGP。

2. 配置 FW1 发布的网络。

3. 配置 FW1 的对等体。

4、对应以上步骤配置 FW2 设备 BGP 相关配置。

24.4 BGP监控与维护

查看BGP路由信息

进入**网络>路由>路由表**，选择**类型**为 BGP，点击**搜索**，即可查看 BGP 的路由信息。

24.5 常见故障分析

24.5.1 故障现象1：两台设备不能建立邻接关系

现象	两台设备不能建立邻接关系
分析	1. 两边peer地址路由不可达 2. 对等体IP地址或者AS号配置错误 3. Open报文协商不成功 4. 配置loopback接口路由不可达 5. Igp之间网络不通 6. Router-id冲突
解决	1. 检查接口配置 2. 打开debug开关 3. 通过抓包分析

25 第25章 策略路由

25.1 策略路由概述

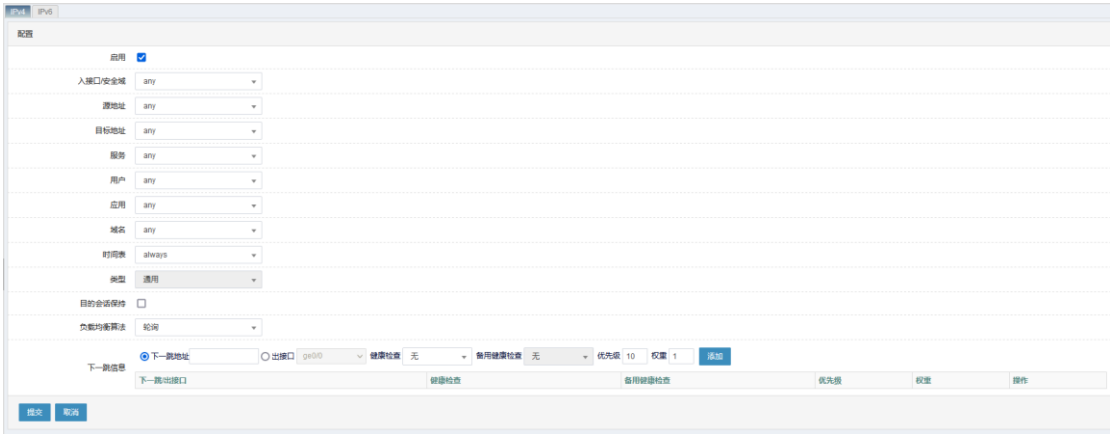
策略路由，也叫做基于策略的路由，是指一个 IPv4 或 IPv6 类型的 IP 包在决定下一跳转发地址时，不是简单的根据目的或源 IP 地址来决定，而是综合考虑多种因素决定。这些因素可以是源地址、目的地址、入接口、服务、用户、应用、域名、时间表等的组合。策略路由支持轮询、加权轮询、源 IP 哈希、源 IP 和端口哈希等选择下一跳的算法，并支持根据健康检查的结果决定下一跳的可用状态。策略路由是一种更加灵活的路由机制，其优先级高于路由选路。

25.2 配置策略路由

25.2.1 创建策略路由

1．配置策略路由之前，需要配置相应的地址对象、服务对象、应用对象、时间对象和健康检查模板。

2．进入**网络>路由>策略路由**，选择 **IPV4** 或 **IPV6**，点击**新建**。



参数说明：

启用：是否启用本条策略路由，只有启用的情况下，该策略路由才会参与匹配。

入接口：指定策略路由匹配入接口，只有从该接口进入的报文才会进入到策略路由流程中，any 表示所有接口。

源地址：指定策略路由匹配 IPv4 或 IPv6 类型的源地址或网段，any 表示所有源地址。

目的地址：指定策略路由匹配 IPv4 或 IPv6 类型的目的地址或网段，any 表

示所有目的地址。

服务：指定策略路由匹配的服务对象, any 表示所有目的服务。

用户：指定策略路由匹配的用户对象，any 表示所有用户。

应用：指定策略路由匹配的应用对象，any 表示所有应用。

域名：指定策略路由匹配的域名对象，any 表示所有域名。

时间表：指定策略路由匹配的时间对象，always 表示全部时间。

目的会话保持：是否启用基于目的地址的会话保持功能。

负载均衡算法：选择下一跳的算法，支持轮询、加权轮询、源 IP 哈希、源 IP 和端口哈希等。

下一跳地址：路由下一跳地址。

出接口：路由下一跳出接口。

健康检查：引用健康检查模板，用于探测下一跳的健康状态。

备用健康检查：引用健康检查模板，用于探测下一跳的健康状态。主备健康检查都失败后则认为该网关地址失效。

优先级：下一跳的优先级，范围 1 到 100。

权重：下一跳的权重，范围 1 到 255。

3．点击**提交**。

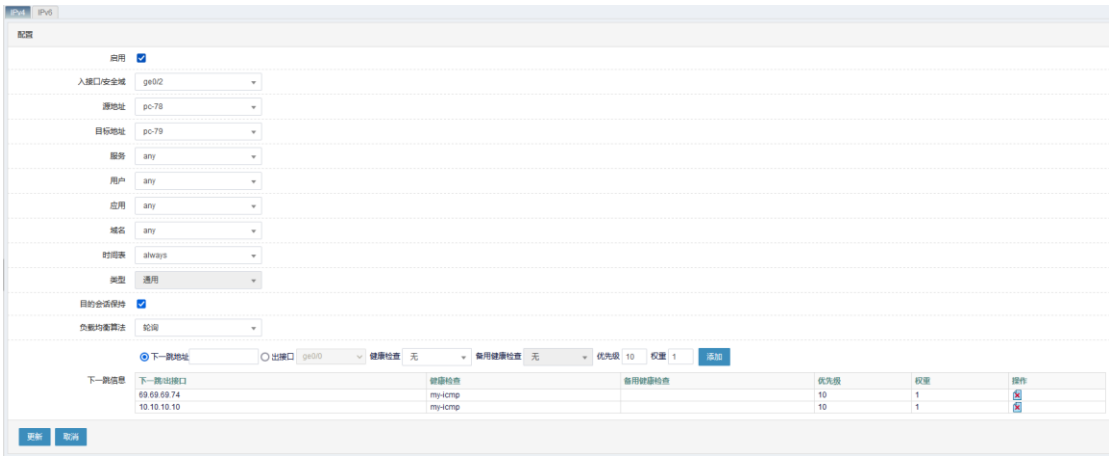
注意

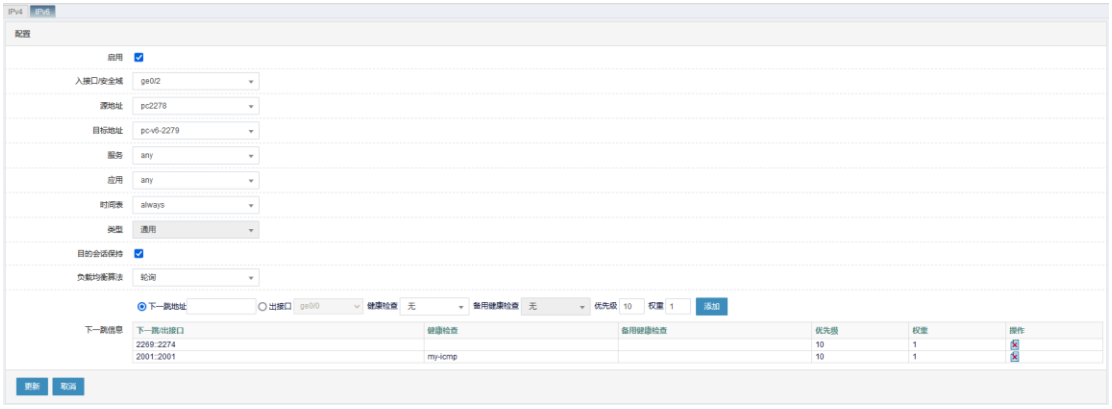
1. 策略路由优先级高于普通路由选路。
2. 策略路由依据接口、源地址、目标地址等作为冲突检查。如果配置重叠或者出现冲突，则会提示配置错误。
3. IPv6 类型策略路由配置参数不包含用户及域名。
4. 优先级越高下一跳越优，高优先级链路健康检查失败后，会自动切换到低优先级下一跳转发。当高优先级故障恢复后，则再次切换到高优先级下一跳转发。
5. 健康检查对象若为非下一跳地址，注意设备要有到该地址的路由，且下一跳为策略路由配置的下一跳地址。
6. 对于设备直连的路由网段不匹配策略路由转发而是查直连路由转发。

25.2.2 编辑策略路由

1．进入**网络>路由>策略路由**，选择 **IPV4** 或 **IPV6**，点击 **ID** 字段可编辑对应策略路由。

2．进入策略路由编辑界面，如下图

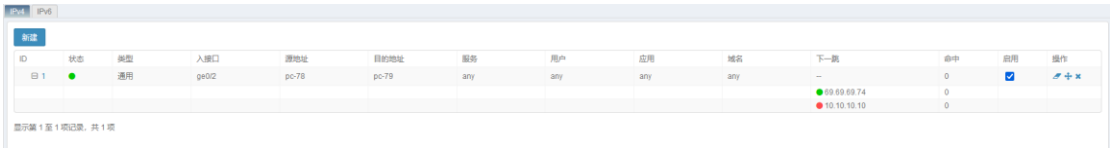


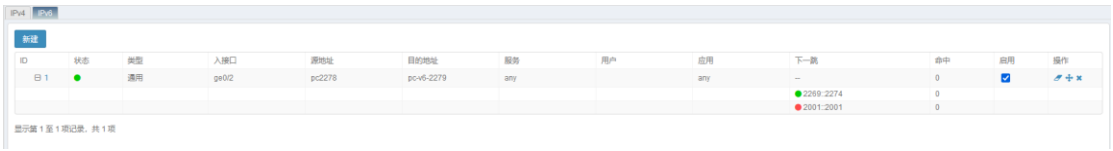


3．编辑完成后点击**更新**按钮。

25.2.3 删除策略路由

1．进入**网络>路由>策略路由**，选择 **IPV4** 或 **IPV6**，如下图：



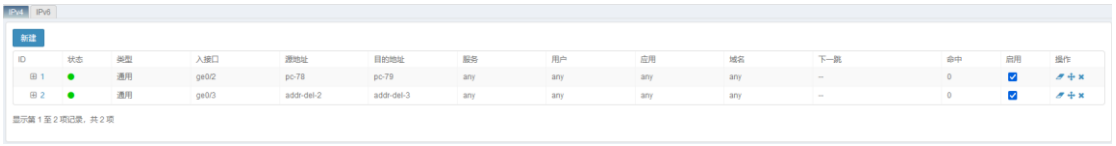


2．点击 删除对应策略路由

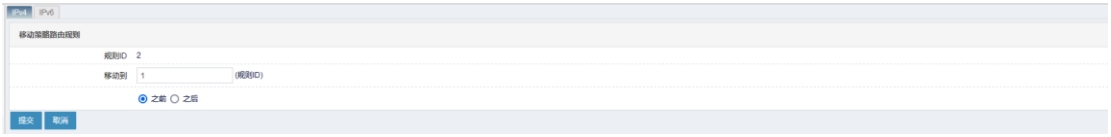
3．点击**确定**删除策略路由。

25.2.4 策略路由顺序调整

1. 进入**网络>路由>策略路由**，选择 **IPV4** 或 **IPV6**，如下图：



2. 点击  调整对应策略路由的匹配优先级。



规则 ID：需要被移动的策略 ID 号。

移动到：参考策略 ID 号。

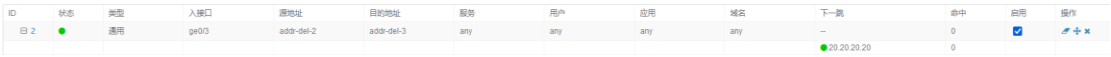
之前：移动到参考策略 ID 之前。

之后：移动到参考策略 ID 之后。

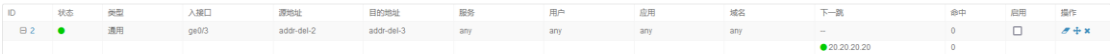
流量匹配策略路由时，按照页面顺序向下匹配，命中后不再进行后续策略匹配。当所有的策略路由都无法匹配时，则匹配路由转发。

25.2.5 策略路由启用禁用

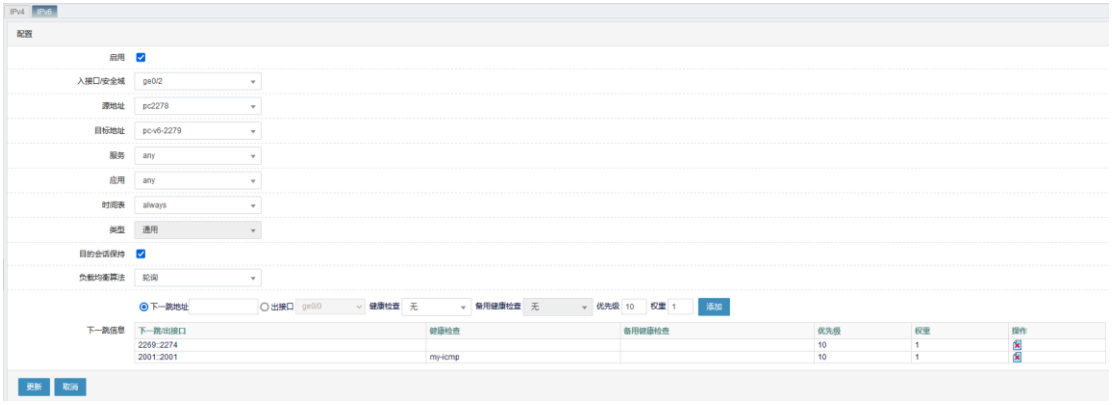
1．进入**网络>路由>策略路由**，选择 **IPV4** 或 **IPV6**，勾选启用按钮，如下图，策略启用。



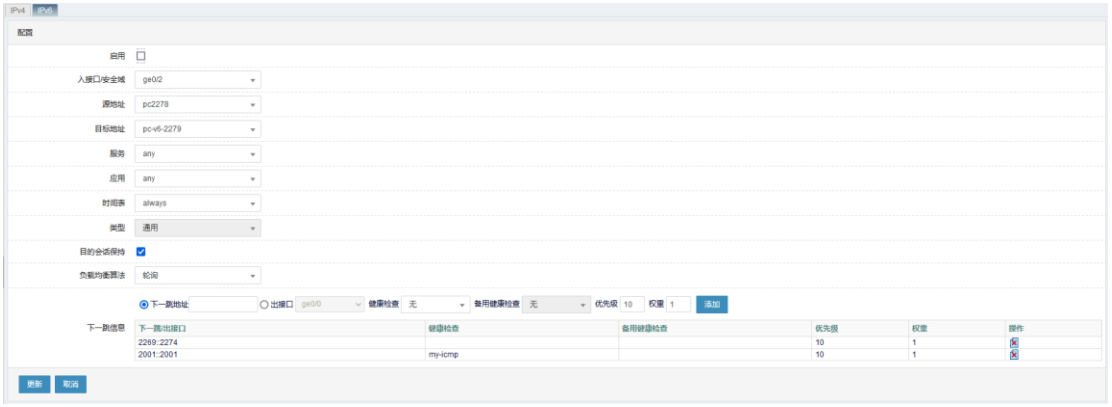
2．进入**网络>路由>策略路由**，选择 **IPV4** 或 **IPV6**，不勾选启用按钮，如下图，策略禁用。



3．进入**网络>路由>策略路由**，选择 **IPV4** 或 **IPV6**，点击 **ID** 字段编辑对应策略路由，勾选启用按钮，点击更新提交。如下图，策略启用。

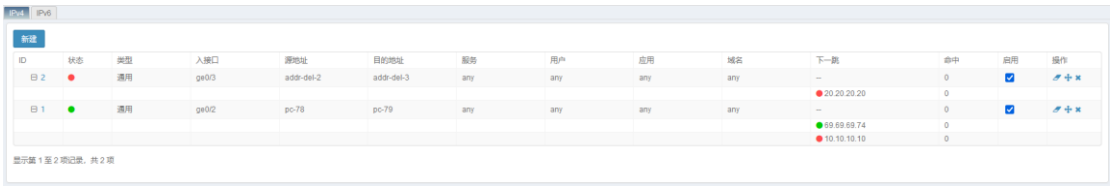


4．进入**网络>路由>策略路由**，选择 **IPV4** 或 **IPV6**，点击 **ID** 字段编辑对应策略路由，不勾选启用按钮，点击更新提交。如下图，策略禁用。



25.2.6 查看策略路由列表

1．进入**网络>路由>策略路由**，选择 **IPV4** 或 **IPV6**，如下图：



2．策略状态：  -策略可用，  -没有可用下一跳，策略不可用。

3. 下一跳状态：  -健康检查成功，下一跳可用  -健康检查失败，下一跳不可用。

4. 点击  即可对下一跳进行展开和收缩操作。

5. 点击 即可重置对应策略路由的命中统计。

25.3 配置案例

25.3.1 策略路由案例 1

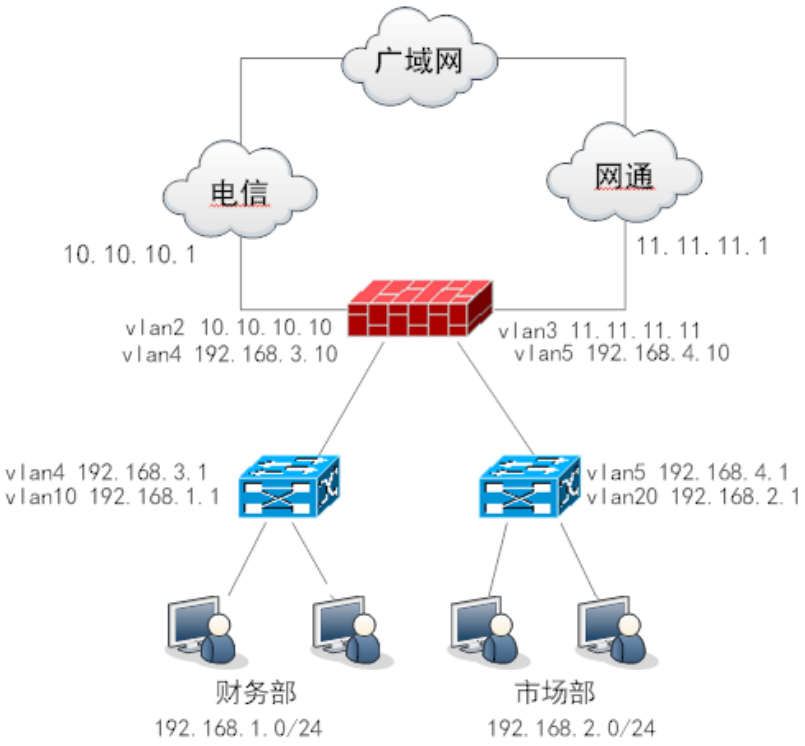
案例描述：

企业需要通过 FW 进行互联网访问，内网地址段为 192.168.1.0/24 和 192.168.2.0/24。现在有两条出口链路分别属于电信、网通，电信的公网地址为 10.10.10.10，网关为 10.10.10.1；网通的公网地址为 11.11.11.11，网关为 11.11.11.1。

用户需求如下：

1. 目的地址为电信 IP 地址，选择电信的链路作为出链路。电信链路故障以后，选择网通的链路作为出链路。
2. 目的地址为网通 IP 地址，选择网通的链路作为出链路。网通链路故障以后，选择电信的链路作为出链路。
3. 目的地址不属于电信、网通，可以均匀选择出链路，但是内网互访不受策略路由控制。

配置案例组网图：

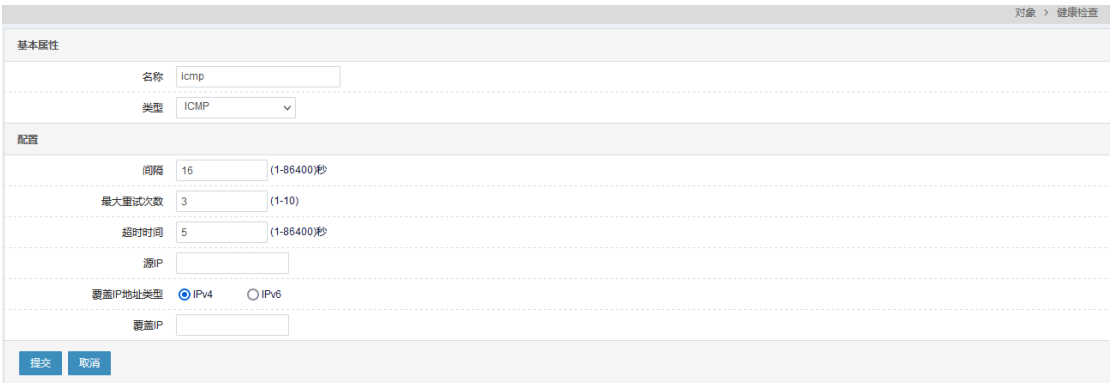


配置步骤：

1. 进入**对象>地址对象>地址节点**，分别创建包含**电信 ISP 地址库**、**网通 ISP 地址库**的地址对象和**外网地址**对象，成员为 0.0.0.0/0，同时将内网用户 192.168.1.0/24 和 192.168.2.0/24 添加到**排除**地址中。

2. 进入**对象>健康检查**，创建 **icmp** 健康检查模板。

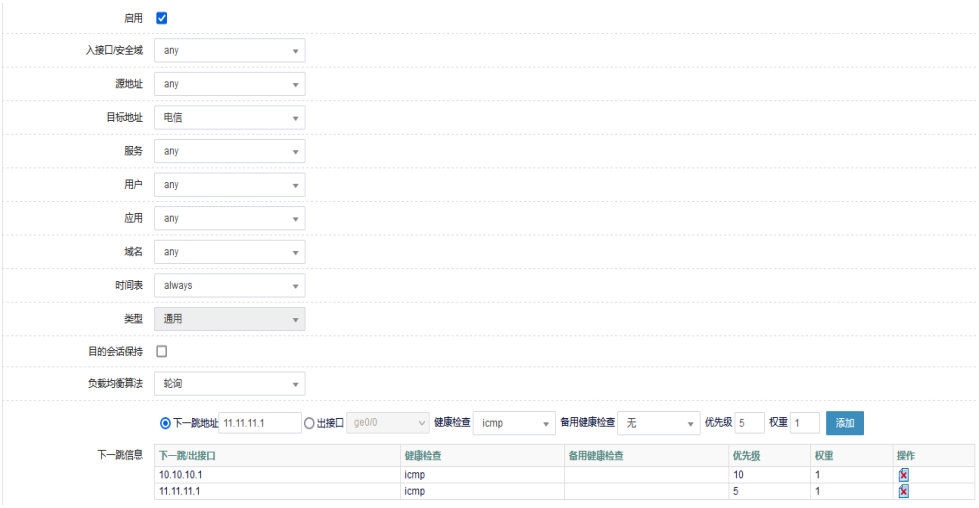
   源 IP 和覆盖 IP 若不填写，健康检查会使用策略路由的下一跳作为目的 IP 进行检查，源 IP 会自动选择出接口的 IP。



3. 进入**网络>路由>策略路由**，选择 IPv4 类型，分别创建**电信策略路由**、**网通策略路由**和**默认策略路由**。

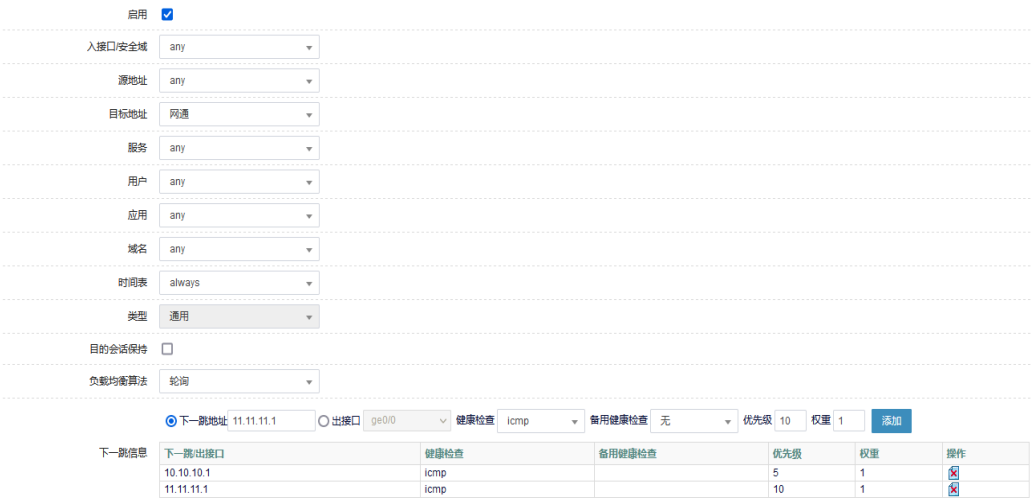
   电信策略路由：

   目标地址选择电信地址对象，网关添加电信链路和网通链路，电信链路优先级高于网通链路，并引用 icmp 健康检查模板。



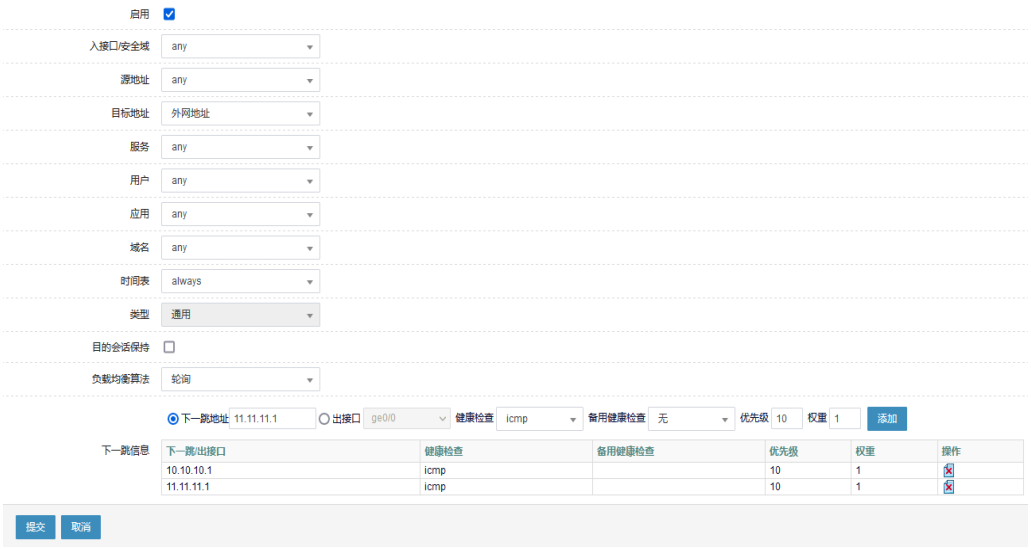
网通策略路由：

目标地址选择网通地址对象，网关添加电信链路和网通链路，网通链路优先级高于电信链路，并引用 icmp 健康检查模板。

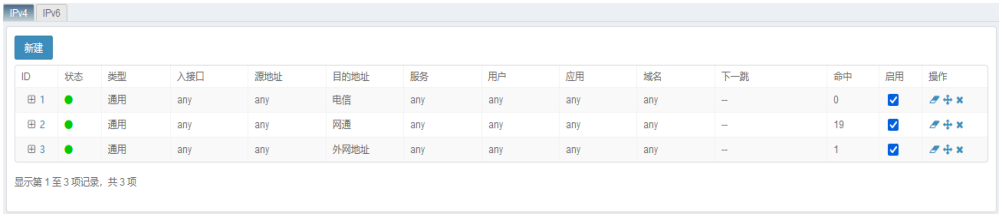


默认策略路由

目标地址选择外网地址对象，外网地址添加了内网网段 192.168.1.0/24 和 192.168.2.0/24 的排除地址，故内网之间的互访不会匹配策略路由。网关添加电信链路和网通链路，网通链路优先级和电信链路优先级相同，使其轮询转发，并引用 icmp 健康检查模板。



4. 配置完成后查看策略，依据命中数可以查看到匹配策略路由调度的情况。



25.3.2 策略路由案例2

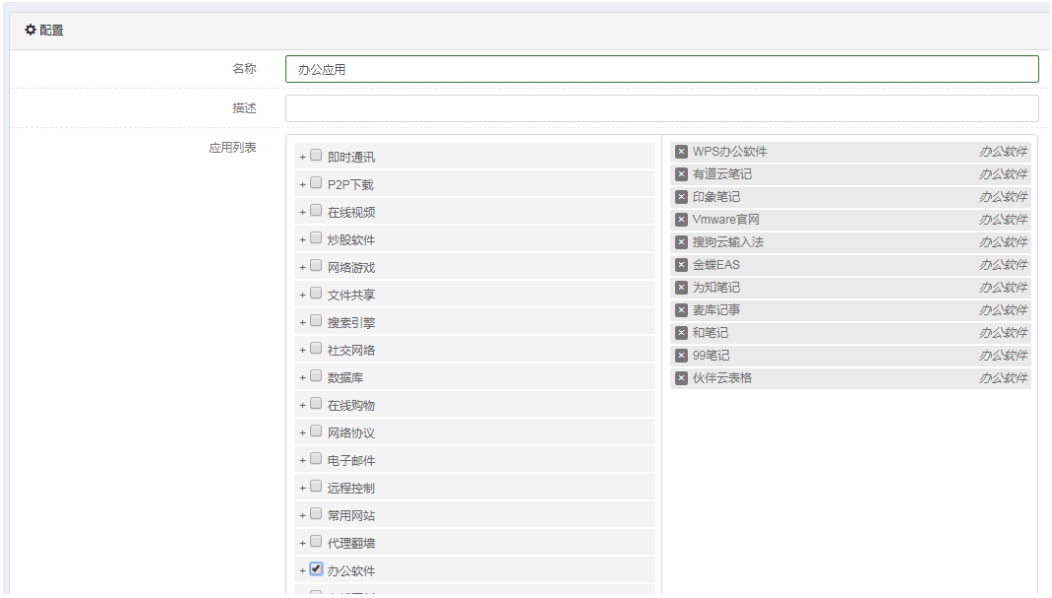
案例描述：

某企业财务部门在工作时间需要将电子邮件和办公软件等办公类应用通过电信专线访问外网，财务部门 IP 地址范围 192.168.0.10 – 192.168.0.20。

配置步骤：

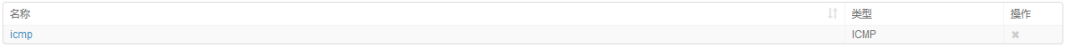
1. 进入**对象>地址对象>地址节点**，创建**财务部地址对象**。

2. 进入**对象>应用对象>应用组**，创建**应用对象**。



3. 进入**对象>时间对象>周期时间**，创建**工作时间对象**。

4. 进入**对象>健康检查**，创建 **ICMP** 健康检查模板。



5. 进入**网络>路由>策略路由**，选择 **IPv4** 类型，创建**财务部策略路由**。

源地址选择**财务部**，**应用**选择**办公应用**，**时间表**选择**工作时间**，网关填写电信专线的下一跳网关，健康检查选择 icmp，点击**添加**，再点击**提交**即可实现财务部在工作时间办公应用通过电信专线访问外网。

25.3.3 策略路由案例3

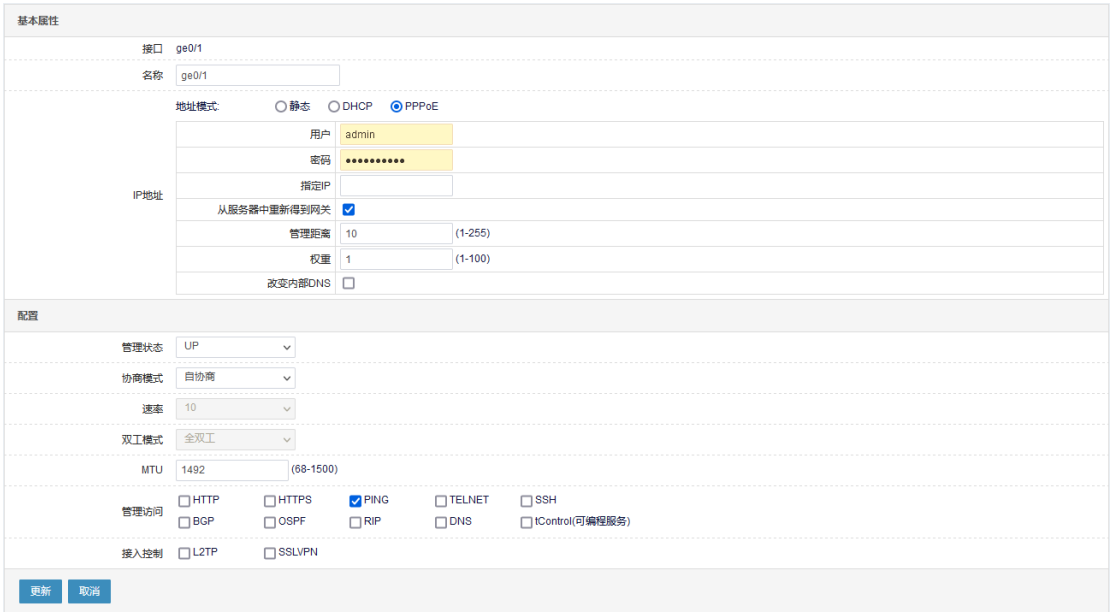
案例描述：

某企业所有客户端需要通过 pppoe 服务器访问外网，策略路由可以直

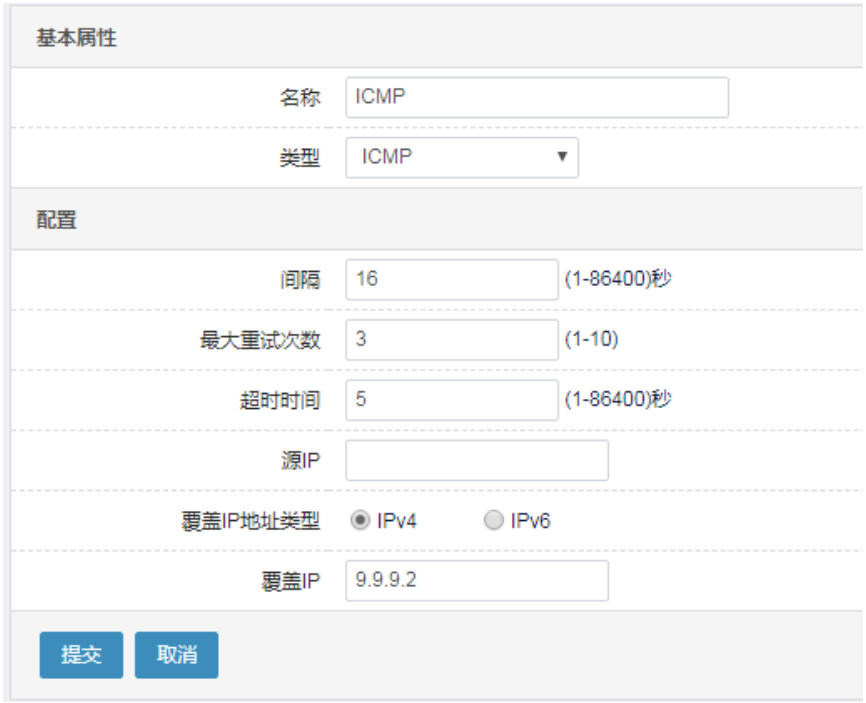
接选择下一跳为出接口。

配置步骤：

1、进入接口>物理接口配置 pppoe 获取地址



2、进入**对象>健康检查**，创建 **ICMP** 健康检查模板。需要配置覆盖 IP



3、进入**网络>路由>策略路由**，选择 **IPv4** 类型，创建**策略路由**

25.4 常见故障分析

25.4.1 策略路由不生效

现象	配置策略路由后没有按照策略路由配置转发到对应下一跳
分析	分析可能为以下几种情况： 1. 策略路由没有启用。 2. 匹配上了比本条策略路由优先级更高的策略路由。 3. 检查策略路由下一跳是否配置正确，该下一跳是否有直连路由。 4. 检查策略路由下一跳健康检查是否成功。 5. 检查源IP或者目的IP地址是否在地址对象中添加了排除。 6. 检查访问的目的网段是否在设备上有直连路由。 7. 检查匹配策略路由的报文是否为反向报文。 8. 依据会话信息，检查连接是否为配置开启策略路由之前的连接。 9. 查看命中策略路由的报文是否通过设备进行二层转发。
解决	1. 将策略路由启用。 2. 可以根据需求修改策略路由或者改变策略路由的顺序。 3. 若依据下一跳地址查不到直连路由，则不会从该下一跳出，顺序向下匹配其他策略路由。 4. 检查健康检查失败原因，是否下一跳地址不可达或者链路出现故障。 5. 将IP地址从排除地址中删除。 6. 有直连路由情况下，会匹配直连路由转发，不再匹配策略路由，故对设备上有直连路由的网段配置策略路由无效。 7. 策略路由是基于流的匹配，正向报文匹配策略路由选路，反向报文不会再匹配策略路由策略，而是按照路由查找转发，同时遵循路径一致性的原则。 8. 为了避免连接断开，策略路由不会影响已建流的流量转发。可以通过重新发起一个连接来确认策略路由是否正确匹配。 9. 只有三层转发的报文才会进策略路由的匹配流程。

25.4.2 策略路由部分下一跳没有命中计数

现象	策略路由添加多个下一跳，流量情况下查看部分下一跳没有命中计数
分析	分析可能为以下几种情况： 1. 检查下一跳地址的优先级，是否有更高优先级的可用下一跳。 2. 检查是否开启了会话保持，查看会话保持设置的掩码是否和访问的目的地址网段相同。 3. 检查是否开启了会话保持，但访问的目的网段通过该下一跳地址出去不可达。为了保证会话保持表项的可靠性，会话保持表项有反向报文后才建立。当存在链路故障导致走该故障链路没有反向报文回应时，则会话保持表项不会建立。
解决	1. 当有可用的高优先级的下一跳时，低优先级下一跳不会参与调度，若希望参与调度，则将优先级调高。 2. 开启会话保持后，相同目的掩码网段的地址都会走相同的下一跳转发，可以依据需要对子网掩码的位数进行适当调整。 3. 检查下一跳出接口链路是否发生故障。

26 第26章 会话保持

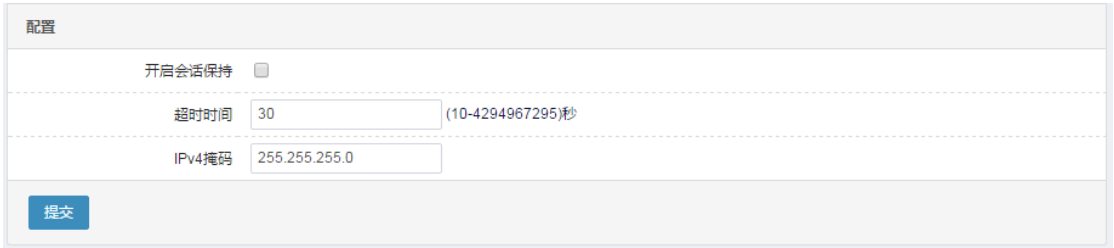
26.1 会话保持概述

在大多数电子商务的应用系统或者需要进行用户身份认证的在线系统中，一个客户与服务器经常要经过多次的交互过程才能完成一笔交易或者是一个任务。由于这几次交互过程是密切相关的，服务器在进行这些交互过程的某一个交互步骤时，往往需要了解上一次交互过程的处理结果，或者上几步的交互过程结果，服务器进行下一步操作时需要把这些相关的交互过程都由一台服务器完成，而不能被分散到不同的服务器上。因此就需要用到会话保持的方法，把相关的请求发送到同一台服务器处理。

26.2 配置会话保持

26.2.1 配置会话保持

1. 进入**网络>路由>会话保持**。



参数说明：

开启会话保持：是否开启目的会话保持。

超时时间：会话保持表项超时时间，范围 10-4294967295 秒。若到达超时时间后仍然没有报文命中会话保持表项，则该表项自动删除。

IPv4 掩码：把掩码和目的 IP 地址进行“AND”运算，若结果相同，则调度到相同的下一跳。

2. 点击**提交**。

26.2.2 会话保持配置说明

1. 会话保持配置中的开启会话保持对除策略路由外的其他等价路由有效。
2. 会话保持表项中的超时时间和 IPv4 掩码设置全局有效。

3. 会话保持开关对策略路由不生效，策略路由会话保持需要在策略路由配置中单独开启。
4. 所有会话保持均为目的会话保持。

26.3 常见故障分析

26.3.1 策略路由会话保持不生效

现象	策略路由会话保持不生效
分析	1、 策略路由的会话保持需要在每条策略中单独开启。
解决	可根据需要在对应策略路由中开启会话保持。

26.3.2 会话保持不生效

现象	配了会话保持访问相同的目的子网掩码网段没有走相同的下一跳
分析	有可能是以下几种情况导致的： 1. 访问目的网段命中了策略路由规则，按照策略路由规则匹配策略路由转发。 2. 到达目的网段有更加细化的路由，按照路由选路原则，匹配细化路由转发。 3. 路由已经失效，不再向失效的路由转发。
解决	检查上面分析中的配置是否正确。

27 第27章 配置 NAT

27.1 NAT概述

NAT 即网络地址转换，最初是由 RFC1631(目前已由 RFC3022 替代)定义，用于私有地址向公有地址的转换，以解决公有 IP 地址短缺的问题。后来随着 NAT 技术的发展及应用的不断深入，NAT 更被证明是一项非常有用的技术，可用于多种用途，如：提供了单向隔离，具有很好的安全特性；可用于目标地址的映射，使公有地址可访问配置私有地址的服务器；另外还可用于服务器的负载均衡和地址复用等。

NAT 分为源 NAT 和目的 NAT。源 NAT 是基于源地址的 NAT，可细分为动态 NAT、PAT 和静态 NAT。动态 NAT 和 PAT 是一种单向的针对源地址的映射，主要用于内网访问外网，减少公有地址的数目，隐藏内部地址。动态 NAT 指动态地将源地址转换映射到一个相对较小的地址池中，对于同一个源 IP，不同的连接可能映射到地址池中不同的地址；PAT 是指将所有源地址都映射到同一个地址上，通过端口的映射实现不同连接的区分，实现公网地址的共享。静态 NAT 是一种一对一的双向地址映射，主要用于内部服务器向外提供服务的情况。在这种情况下，内部服务器可以主动访问外部，外部也可以主动访问这台服务器，相当于在内、外网之间建立了一条双向通道。

T 系列防火墙设备提供了源地址转换、目的地址转换和静态地址转换功能。

27.2 配置NAT

系统中把 NAT 的配置分为：源地址转换（Source）、目的地址转换（Destination）、静态地址转换（Static）三种基本类型，另外还有一种同时可以配置源和目的转换的双向 NAT。目前支持 IPv4 地址之间的互转，以及 IPv6 地址之间的互转。

每条 NAT 规则都是和某个特定的接口关联的，需要注意的是，源地址转换是在离开接口时进行转换的，所以配置源地址转换的时候必须和对应的出接口关联，目的地址转换是在进入接口时进行转换的，所以配置目的地址转换的时候必须和对应的入接口关联。

如果两条 NAT 规则的“源地址”、“目标地址”、“服务”以及“出接口”这四元组相同的话，优先匹配第一条 NAT 规则。

27.2.1 配置地址池(NATPool）

地址池中存放供动态 NAT 使用的地址范围的集合。地址池的使用支持轮询方式，源地址保持方式以及默认方式；同时支持地址池分段。

在进行地址转换后，报文的真实地址将被转换为地址池中的地址。

配置步骤：

1. 进入**网络>NAT>NAT 地址池**，点击**新建。**

名称：NAT 地址池的名称，可以是中文，不得超过 63 个字符。

描述：关于该 NAT 地址池的描述，可以是中文，不得超过 127 个字符。

选择算法：依据所选的算法从地址池中选取地址，包含以下三种选项：

默认：随机从地址池中选取一个地址作为转换后地址。

轮循：地址池中地址数量大于一个时，在进行地址转换的时候会依次进行循环使用。

源地址保持：随机从地址池中选取一个地址，相同的源地址的报文选取的地址相同。

协议类型：设备目前支持配置 IPv4 和 IPv6 协议类型的地址池，每个地址池中只能包含所选协议类型的地址。

起始地址：NAT 地址池中的起始地址。

结束地址：NAT 地址池中的结束地址，结束地址不能小于起始地址。从起始地址到结束地址这个范围内的地址都会作为地址池中的地址。

地址检查：检查地址池中地址的可用性。勾选之后，将会请求输入服务器 IP 和下一跳地址。默认情况下不开启地址池检查功能。

类型：地址检查所用的协议类型。

服务器 IP：地址池中的地址依次向服务器发送报文，来判断该地址是否可用。可通过命令行 show snat-pool-check list 查看地址可用性信息。

下一跳地址： 用于 NAT 地址池检查的下一跳地址。

注意	结束地址不能小于起始地址；池段范围不能出现重叠现象。起始地址与结束地址之间包含的地址数目必须不超过 10000。

2. 点击**提交**。

27.2.2 编辑地址池

已经创建的地址池可以编辑修改。

编辑步骤：

1. 进入**网络>NAT>NAT 地址池**。

点击地址池名称。

可以对地址池进行编辑修改。其中名称与协议类型是不允许变更的。

2. 点击**更新**。

27.2.3 删除地址池

地址池删除步骤：

1. 进入**网络>NAT>NAT 地址池。**

2. 点击 ，删除选定的地址池。

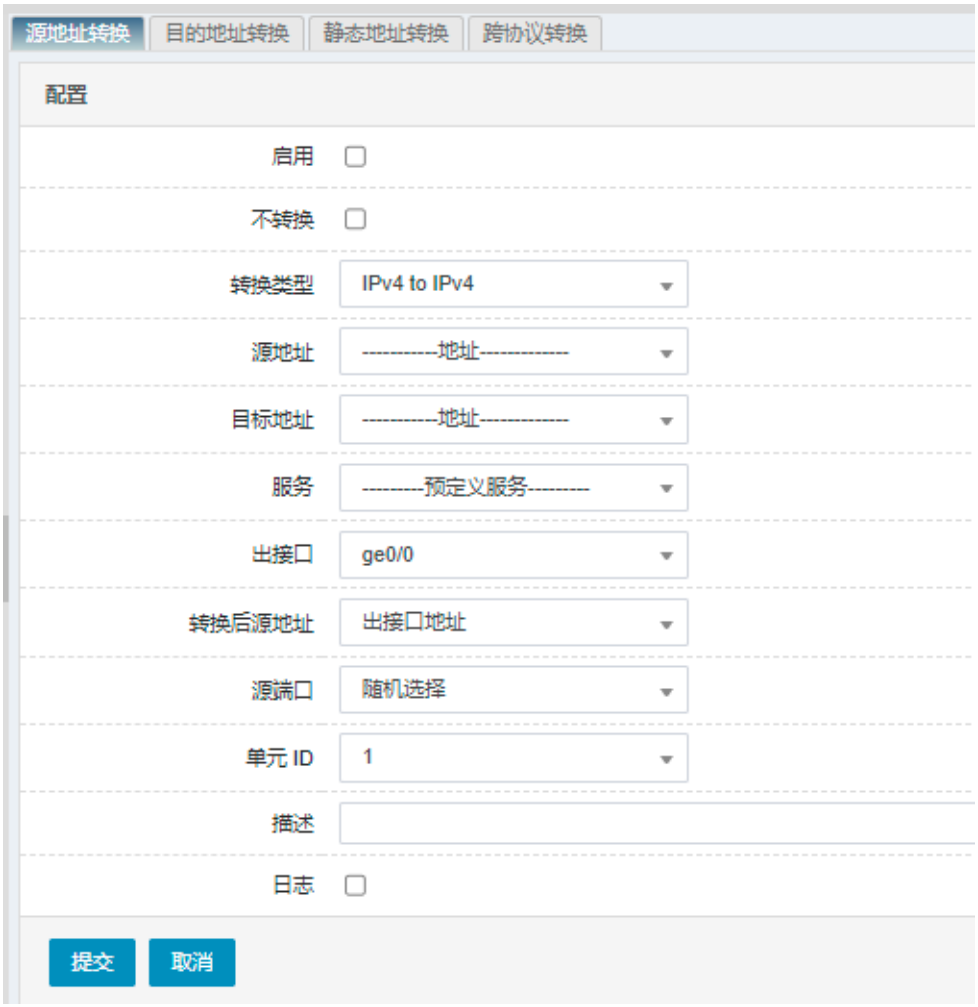
> 注意
>
> 当删除按钮为灰色时，表明该地址池正在被某处引用，不能被删除。

27.2.4 配置源地址转换

源地址转换是一种单向的针对源地址的映射，主要用于内网访问外网，减少公有地址的数目，隐藏内部地址。

配置步骤：

1. 进入网络>NAT>NAT 规则>源地址转换，点击新建。



启用：规则是否生效。

不转换：匹配这条 NAT 规则的会话，不进行地址转换。

转换类型：设备支持 IPv4 协议类型的地址之间的互转，以及 IPv6 协议类型地址之间的互转。

源地址：NAT 规则匹配的源地址，可以是地址对象或地址组。其中地址对象的类型必须与转换类型一致，比如转换类型配置为 IPv4 to IPv4 时，地址对象也必须选择 IPv4 类型的。

目标地址：NAT 规则匹配的目的地址，可以是地址对象或地址组。地址对象的类型必须与转换类型一致。

服务：NAT 规则匹配的服务名，可以是服务对象或服务组。

出接口：NAT 规则匹配的出接口名。

转换后源地址：需要转换成的地址，可以是出接口的地址或地址池名称或者一个单独的 IP 地址。选择的地址池类型必须与转换类型一致。

源端口：

随机选择：根据分流算法，随机选择发送源端口。

保持：转换前后，保持源端口不变，如果冲突，就改变源端口。

严格保持：转换前后，保持源端口不变，如果冲突，就丢包。

单元 ID：选择该条规则的单元 ID，该 ID 在高可靠性功能（HA）启用时生效，比如启用 HA 的主主模式时，如果主机的 ID 与该 NAT 规则不一致，则该规则不生效。默认为 1。

描述：对该转换规则的描述，最长不得超过 127 个字符。

日志：是否需要对该规则启用日志。

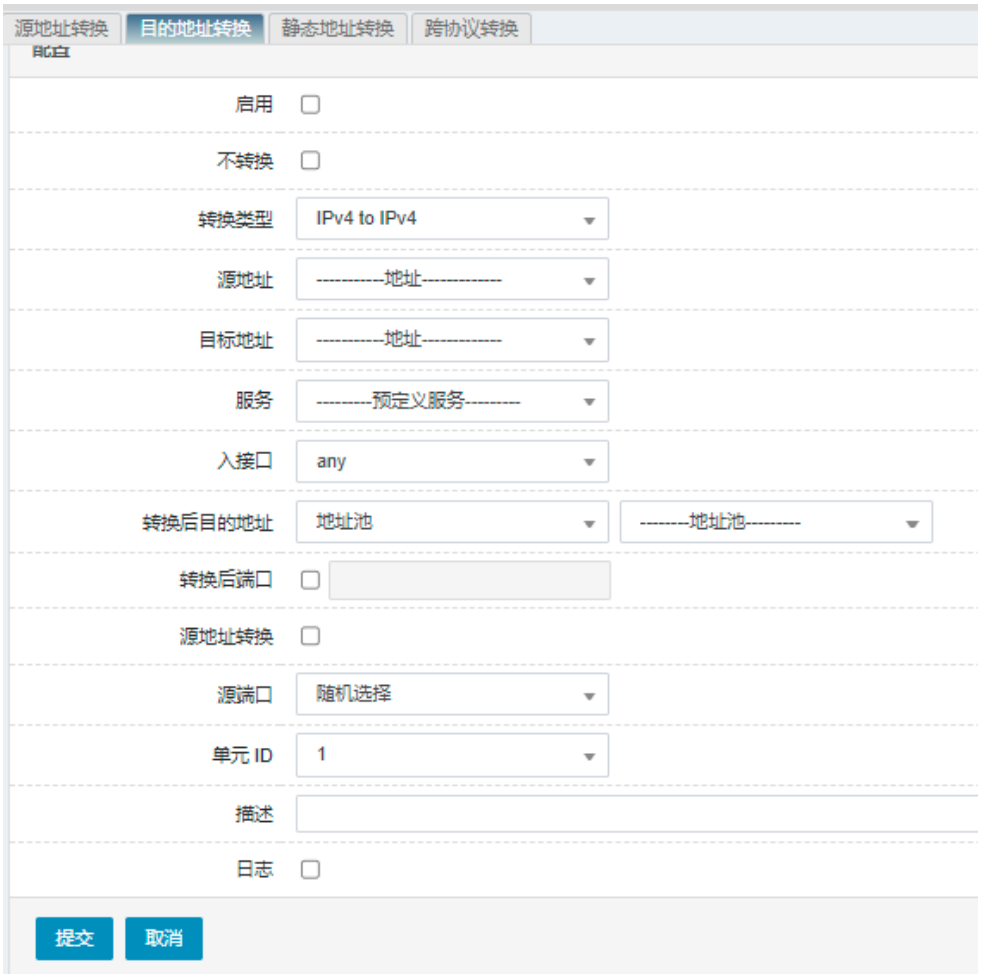
2. 点击**提交。**

27.2.5 配置目的地址转换

目的地址转换是一种单向的针对目的地址的映射，主要用于外网访问内网，主要用于内部服务器向外部提供服务的情况，外部可以主动访问内部，内部却不可以主动访问外部。

配置步骤：

1. 进入**网络>NAT>NAT 规则>目的地址转换**，点击**新建。**



启用：规则是否生效。

不转换：匹配这条 NAT 规则的会话，不进行地址转换。

转换类型：设备支持 IPv4 协议类型的地址之间的互转，以及 IPv6 协议类型地址之间的互转。

源地址：NAT 规则匹配的源地址，可以是地址对象或地址组。

目标地址：NAT 规则匹配的目的地址，可以是地址对象或地址组。

服务：NAT 规则匹配的服务名，可以是服务对象或服务组。

入接口：NAT 规则匹配的入接口名。

转换后目的地址：需要转换成的地址，可以是地址池名称，也可以直接配置 ip。

转换后端口：需要转换成的端口。

源地址转换：双向 NAT 中源需要转换成的地址池或者 ip，配置目的 NAT 时不勾选。

源端口：

随机选择：根据分流算法，随机选择发送源端口。

保持：转换前后，保持源端口不变，如果冲突，就改变源端口。

严格保持：转换前后，保持源端口不变，如果冲突，就丢包。

单元 ID：选择该条规则的单元 ID，该 ID 在高可靠性功能（HA）启用时生效，比如启用 HA 的主主模式时，如果主机的 ID 与该 NAT 规则不一致，则该规则不生效。默认为 1。

描述：对该转换规则的描述，最长不得超过 127 个字符。

日志：是否需要对该规则启用日志。

2. 点击**提交。**

27.2.6 配置双向地址转换

双向 NAT 是一条规则中既有源地址转换，也有目的地址转换。内部 pc 访问内部服务器，内部服务器提供一个虚地址，此时，需要同时做源 NAT 和目的 NAT。

配置步骤：

1. 进入**网络>NAT>NAT 规则>目的地址转换**，点击**新建。**

启用：规则是否生效。

源地址：NAT 规则匹配的源地址，可以是地址对象或地址组。

目标地址：NAT 规则匹配的目的地址，可以是地址对象或地址组。

服务：NAT 规则匹配的服务名，可以是服务对象或服务组。

入接口：NAT 规则匹配的入接口名。

转换后目的地址：需要转换成的地址，地址池名称。

转换后端口：需要转换成的端口。

源地址转换：双向 NAT 中源需要转换成的地址池或者 ip，配置双向 NAT 时勾选。

源端口：

随机选择：根据分流算法，随机选择发送源端口。

保持：转换前后，保持源端口不变，如果冲突，就改变源端口。

严格保持：转换前后，保持源端口不变，如果冲突，就丢包。

单元 ID：选择该条规则的单元 ID，该 ID 在高可靠性功能（HA）启用时生效，比如启用 HA 的主主模式时，如果主机的 ID 与该 NAT 规则不一致，则该规则不生效。默认为 1。

描述：对该转换规则的描述，最长不得超过 127 个字符。

日志：是否需要对该规则启用日志。

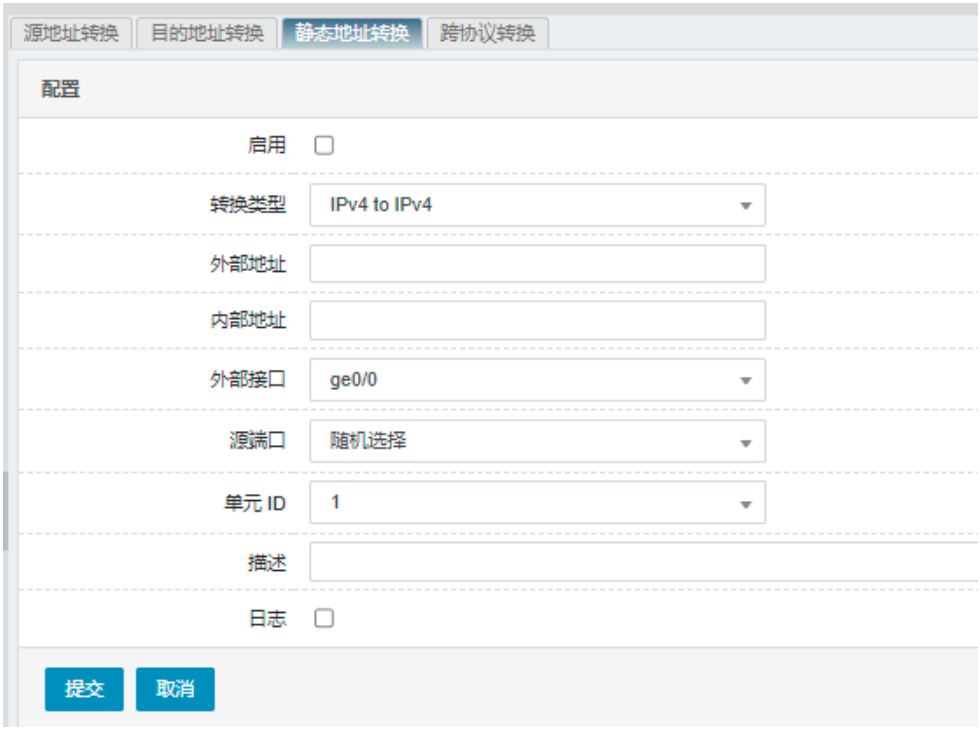
2. 点击**提交**。

27.2.7 配置静态地址转换

静态地址转换是一对一的双向地址映射。在这种情况下，被映射的内部主机可以主动访问外部，外部也可以主动访问这台内部主机，相当于在内、外网之间建立了一条双向通道。

配置步骤：

1. 进入**网络>NAT>NAT 规则>静态地址转换**，点击**新建**。



启用：规则是否生效。

转换类型：设备支持 IPv4 协议类型的静态 NAT，以及 IPv6 协议类型的静态 NAT。

外部地址：需要转换的外部地址。

内部地址：需要转换的内部地址。

外部接口：和外部网络相连的接口名。

源端口：

随机选择：根据分流算法，随机选择发送源端口。

保持：转换前后，保持源端口不变，如果冲突，就改变源端口。

严格保持：转换前后，保持源端口不变，如果冲突，就丢包。

单元 ID：选择该条规则的单元 ID，该 ID 在高可靠性功能（HA）启用时生效，比如启用 HA 的主主模式时，如果主机的 ID 与该 NAT 规则不一致，则该规则不生效。默认为 1。

描述：对该转换规则的描述，不得超过 128 个字符。

日志：是否需要对该规则启用日志。

2. 点击**提交。**

27.2.8 启用NAT规则

1. 进入**网络配置>NAT>NAT 规则>源地址转换。**

2. 勾选**启用**

27.2.9 编辑NAT规则

已经创建的 NAT 规则可以编辑修改。

源 NAT 转换编辑步骤：

1. 进入**网络配置>NAT>NAT 规则>源地址转换。**

2. 点击**规则编号。**

可以对原有的规则进行编辑。其中转换类型不允许更改。

3. 点击**提交。**

27.2.10 删除NAT规则

源 NAT 转换删除步骤：

1. 进入**网络配置>NAT>NAT 规则>源地址转换。**

2. 点击 ，删除选定的 NAT 规则。

27.2.11 移动NAT规则

相同转换类型的 NAT 规则可通过移动操作，调整匹配的顺序。

源 NAT 转换移动步骤：

1. 进入**网络配置>NAT>NAT 规则>源地址转换。**

2. 点击规则后的 ：

规则 ID：移动的目标规则 ID。

移动到：指定要移动的位置。

注意

规则移动时，只能在相同转换类型的规则之间移动。比如 IPv4 to IPv4 类型的规则只能移动到 IPv4 to IPv4 类型的规则前后，IPv6 to IPv6 类型的规则只能移动到 IPv6 to IPv6 类型的规则前后。

27.3 NAT监控与维护

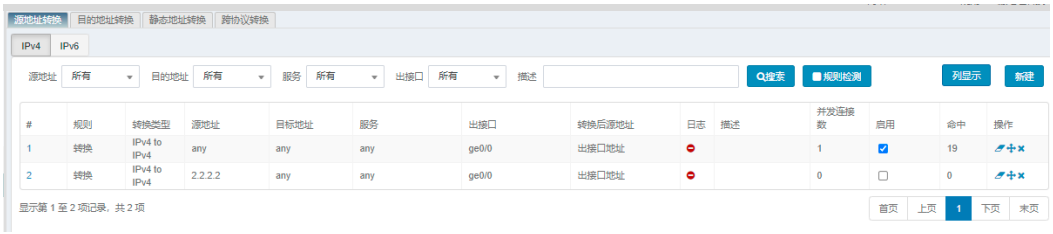
27.3.1 查看地址池

1. 进入**网络>NAT>NAT 地址池**，可以查看已经配置的地址池。

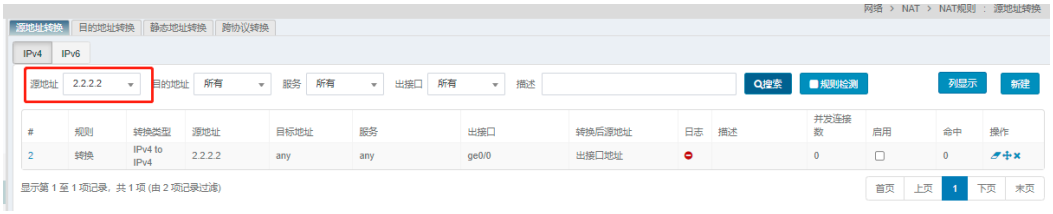
2. 点击检查结果，可以查看地址池检查情况。

27.3.2 查看源、目的NAT规则

1. 进入**网络>NAT>NAT 规则**



2. 输入过滤条件，点击**搜索**

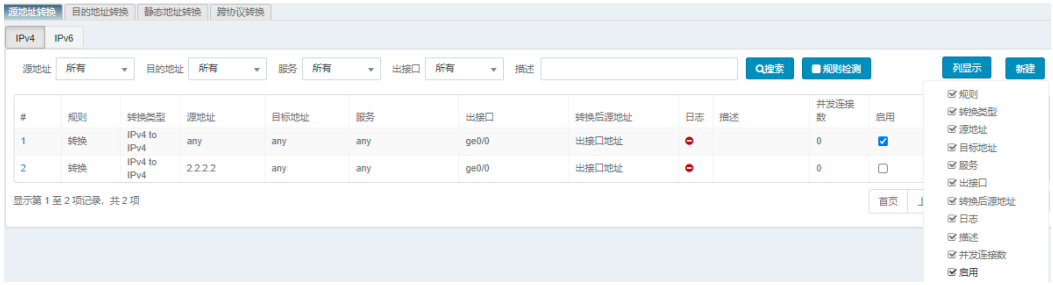


3. 点击 **规则检测**，进行冗余检查

1）检查当前规则的配置（源地址、目的地址、服务以及接口）是否被前面的规则覆盖，如果被覆盖，就在当前规则的“冗余/冲突规则”列显示覆盖规则的 id。

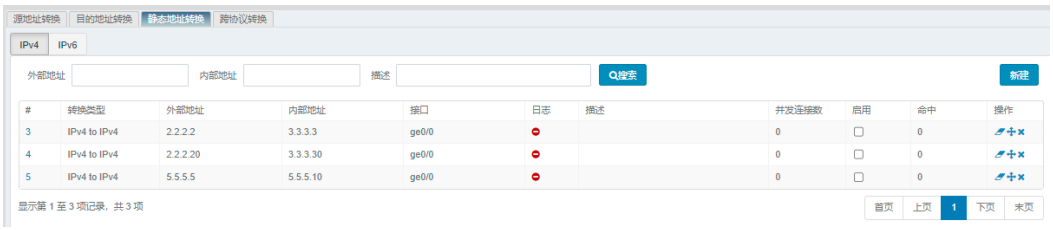
2）每条规则最多显示 100 个覆盖规则的 id， 每页最多显示 1000 个覆盖规则 id。

4. 点击 **列显示**，展示或者隐藏某些列

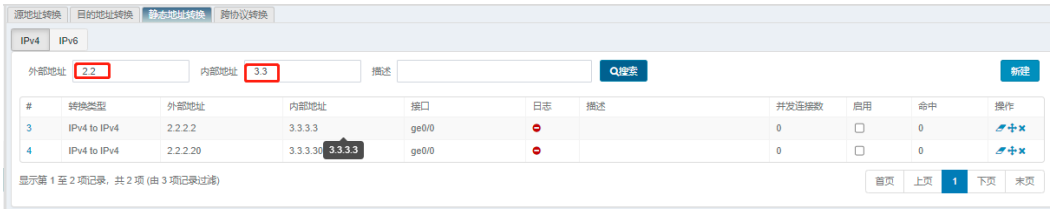


27.3.3 查看静态NAT规则

1. 进入**网络>NAT>NAT 规则>静态地址转换**



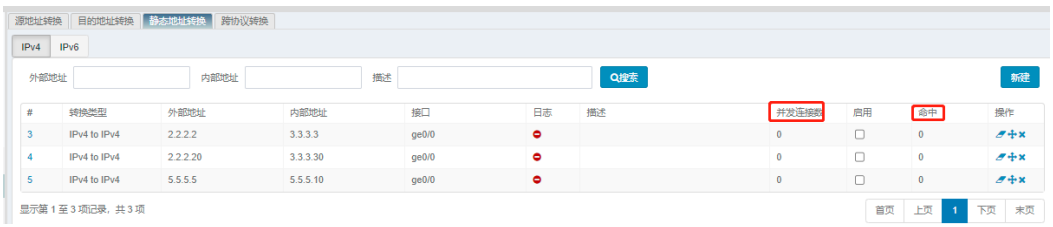
2. 输入过滤条件，点击**搜索**



静态 nat 地址搜索支持模糊搜索。

27.3.4 查看NAT规则并发连接数和命中数

1. 进入**网络>NAT>NAT 规则**，可以分别查看 NAT 规则的并发连接数和命中数。



2. 点击  ，可以清空命中数。

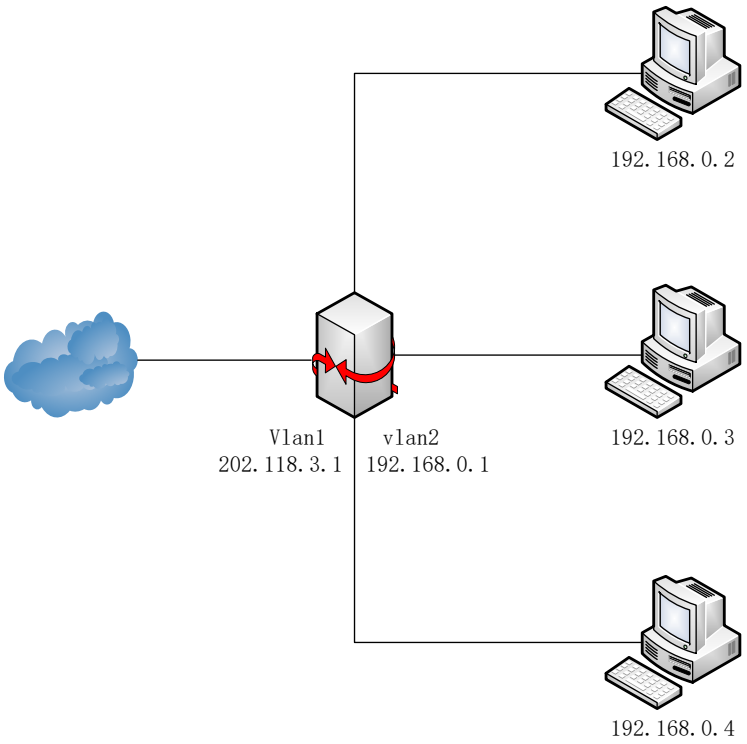
27.4 配置案例

27.4.1 配置源地址转换

案例描述：

公司内部局域网需要通过应用设备访问外部网络。内网地址为 192.168.0.0/24 网段，公网地址为 202.118.3.1

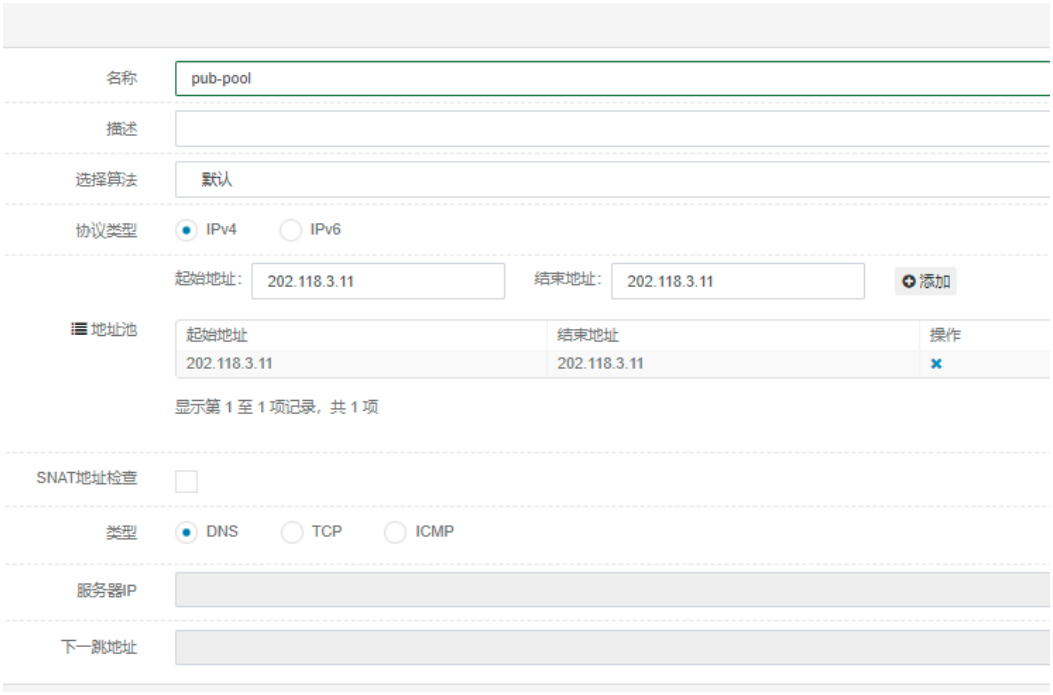
案例组网图：



配置步骤：

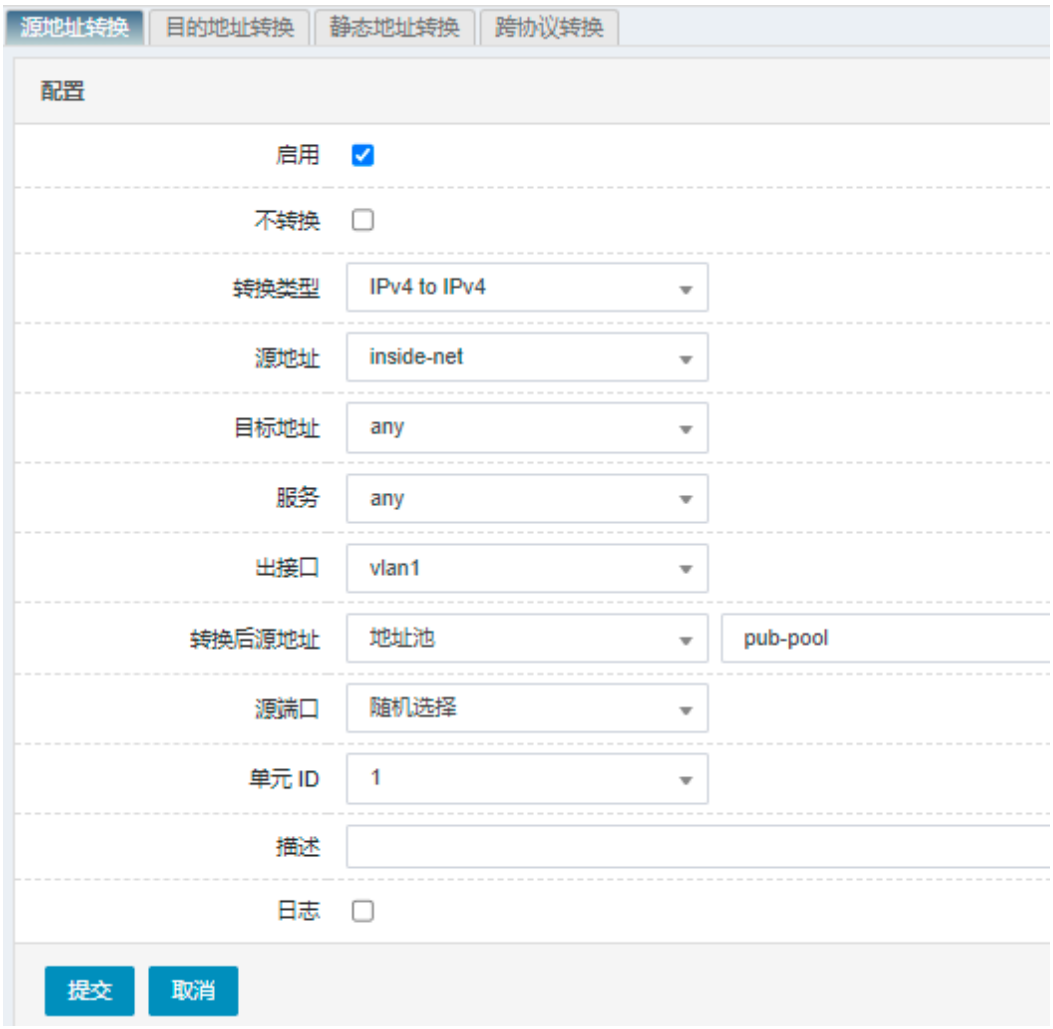
1. 进入**对象->地址对象->地址节点**，创建 IPv4 类型的地址对象“inside-net”。

2. 进入**网络>NAT>NAT 地址池**，创建地址池“pub-pool”。



点击**提交。**

3. 进入**网络>NAT>NAT 规则>源地址转换**，点击**新建。**



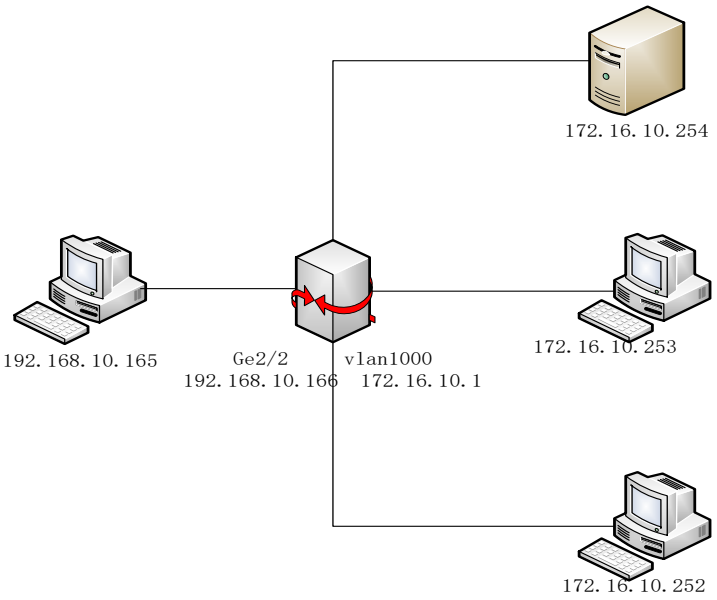
4．点击**提交**。

27.4.2 配置目的地址转换

案例描述：

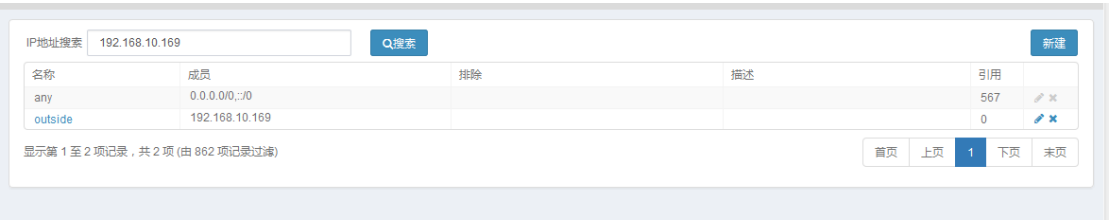
内网有一台服务器对外提供服务，服务器的内网地址为 172.16.10.254，映射的外网地址为 192.168.10.169。

案例组网图：

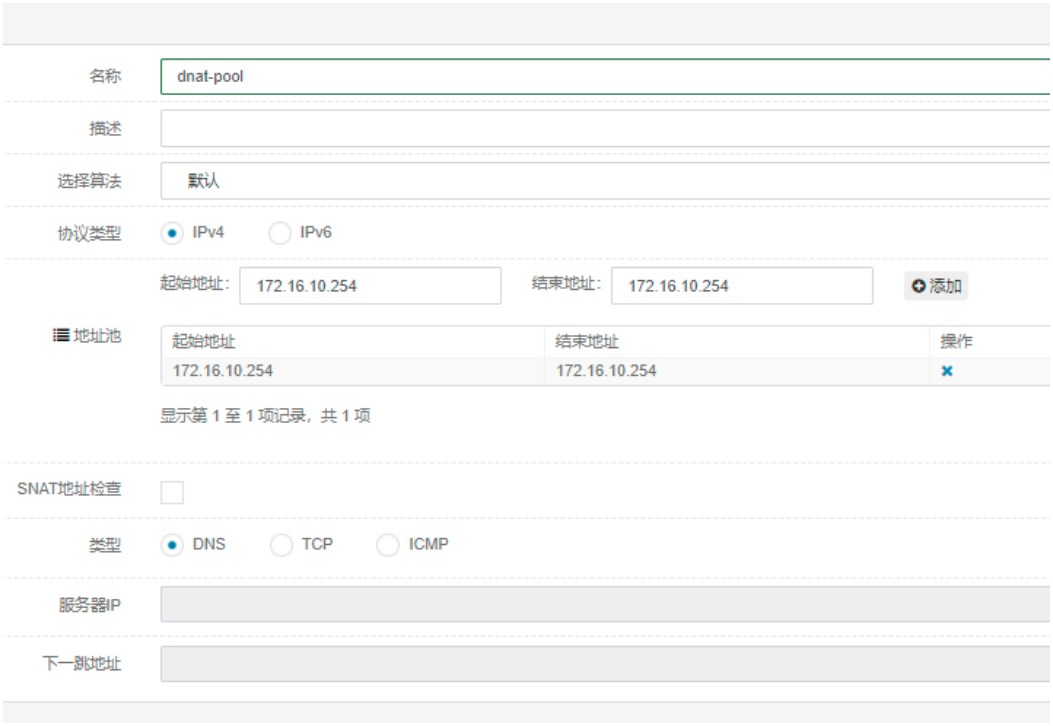


配置步骤：

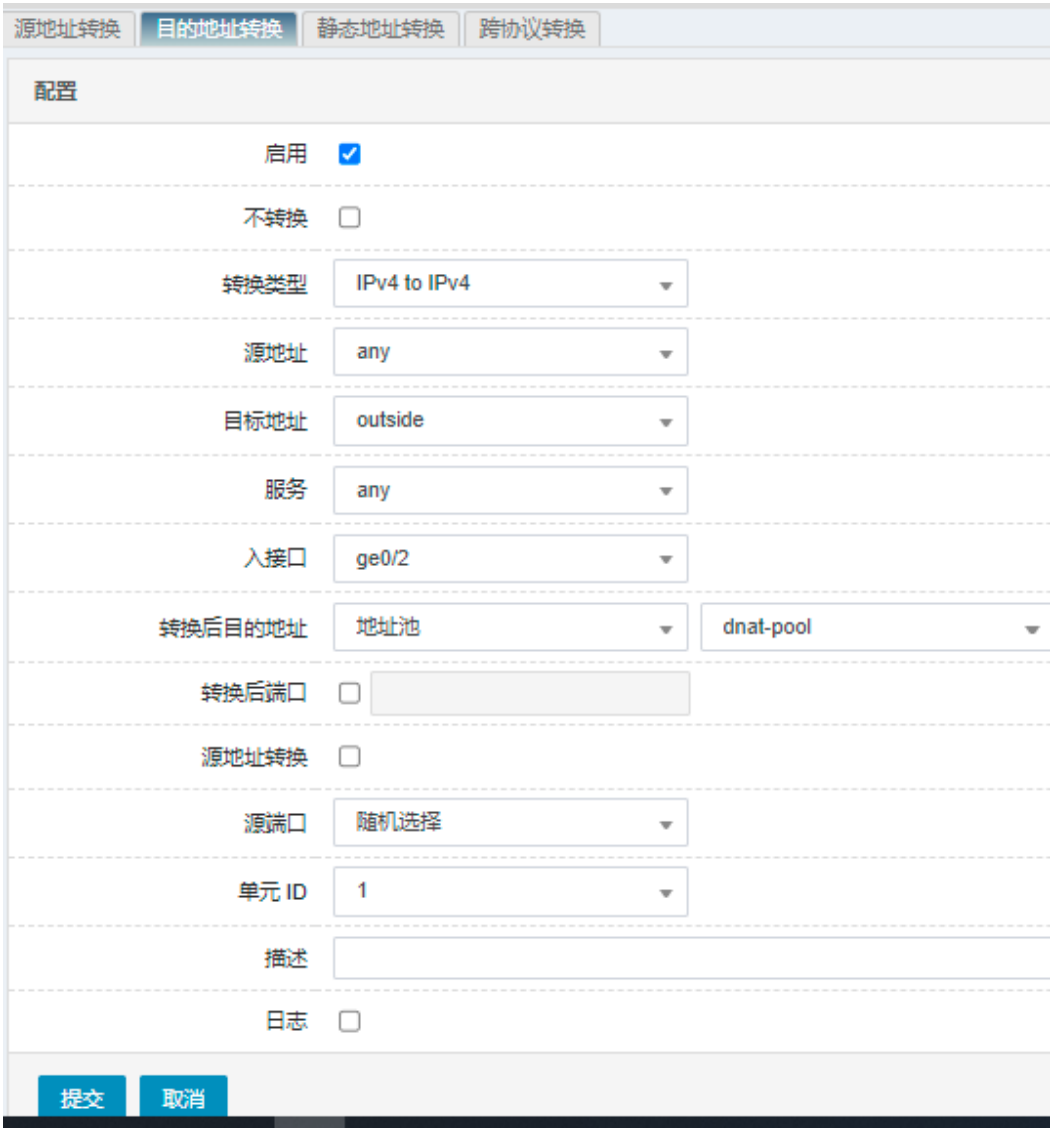
1. 进入**对象->地址对象->地址节点**，创建 IPv4 类型的地址对象“outside”。



2. 进入**网络>NAT>NAT 地址池**，创建地址池“dnat-pool”。



3. 进入**网络>NAT>NAT 规则>目的地址转换**，点击**新建。**



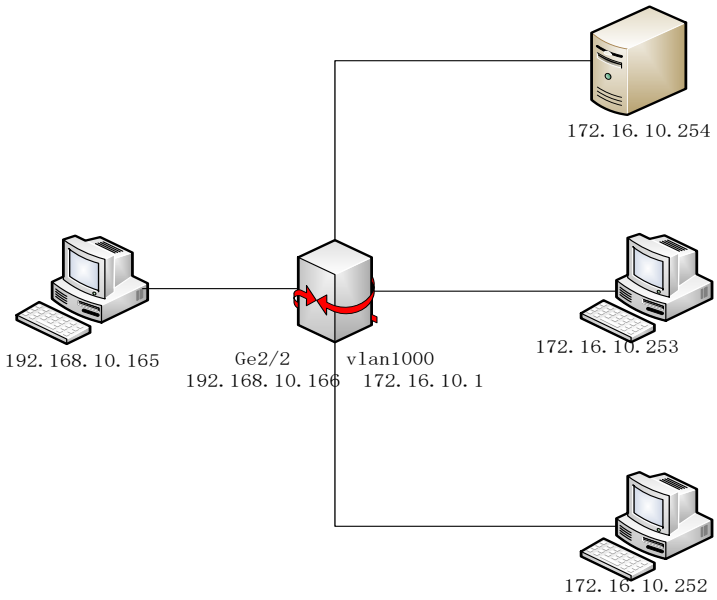
4. 点击提交。

27.4.3 配置双向地址转换

案例描述：

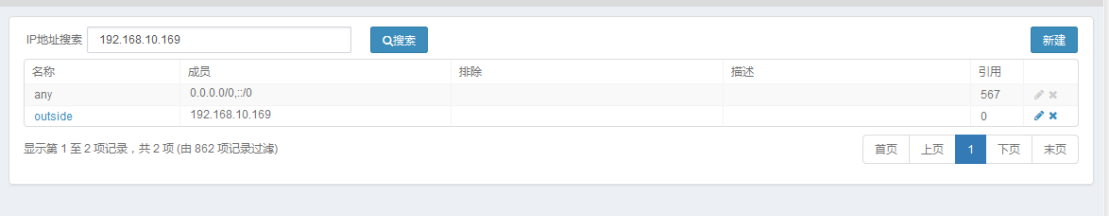
内网有一台服务器对外提供服务，服务器的内网地址为 172.16.10.254，映射的外网地址为 192.168.10.169。内网用户 172.16.10.252 和外网用户 192.168.10.165 要同时访问该服务器。

案例组网图：

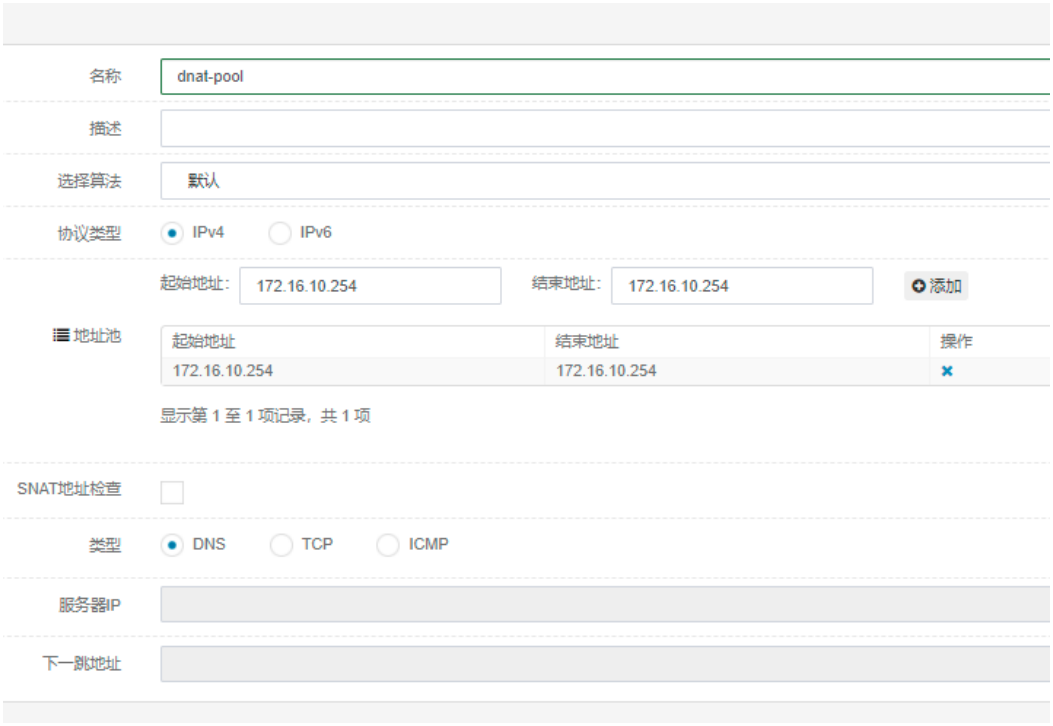


配置步骤：

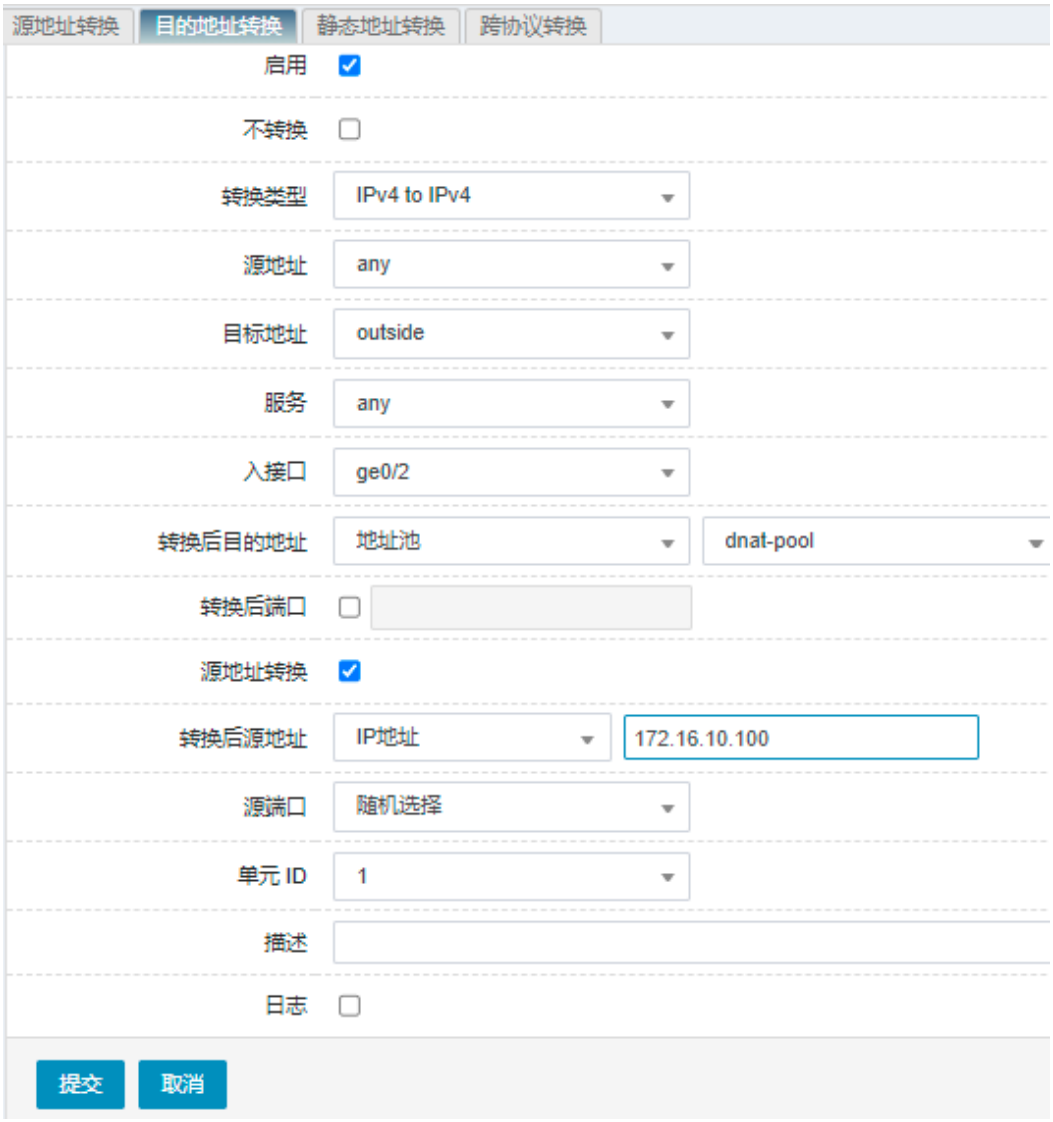
1. 进入**对象->地址对象->地址节点**，创建 IPv4 类型的地址对象“outside”。



2. 进入**网络>NAT>NAT 地址池**，创建地址池“dnat-pool”。



3. 进入**网络>NAT>NAT 规则>目的地址转换**，点击**新建。**



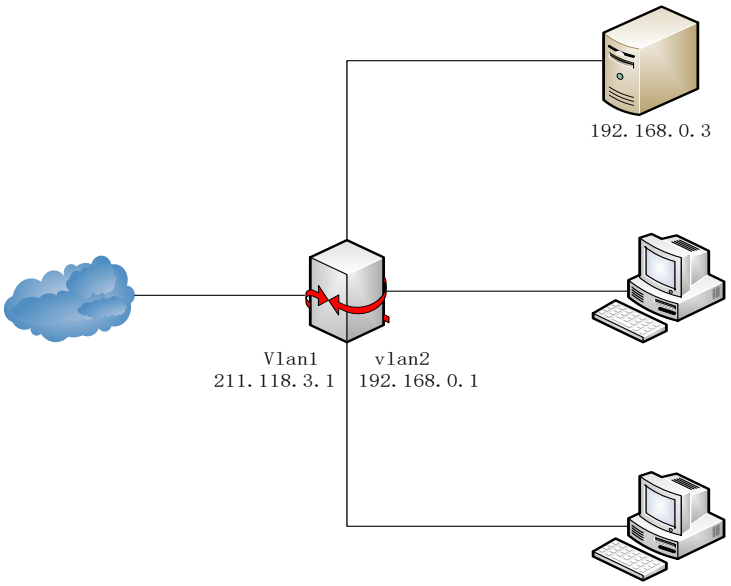
4. 点击提交。

27.4.4 配置静态地址转换

案例描述：

内网有一台服务器对外提供服务，服务器的内网地址为 192.168.0.3，映射的公网地址为 202.118.3.1。

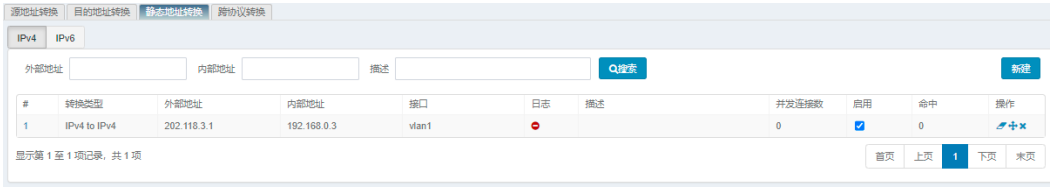
案例组网图：



配置步骤：

1. 进入**网络配>NAT>NAT 规则>静态地址转换**，点击**新建。**

2. 点击**提交**，显示如下界面。



27.5 常见故障分析

27.5.1 连接时通时断

故障现象	做了NAT之后，经过NAT PING另外网络的机器，时通时断；或刚开始是通的，一会儿又断了；或一直不通
分析与解决	1) 转换后的地址有冲突，别人已经使用。有些地址可能PING不通，但不能排除地址已被使用的可能，因为对方可以禁止了PING包。 2) 可以查看被PING的机器中的ARP表项，NAT转换后的地址对应的MAC是否为设备的MAC地址，如不是，证明有其它机器使用了此IP。使用无人使用的地址作为NAT转换后的地址。

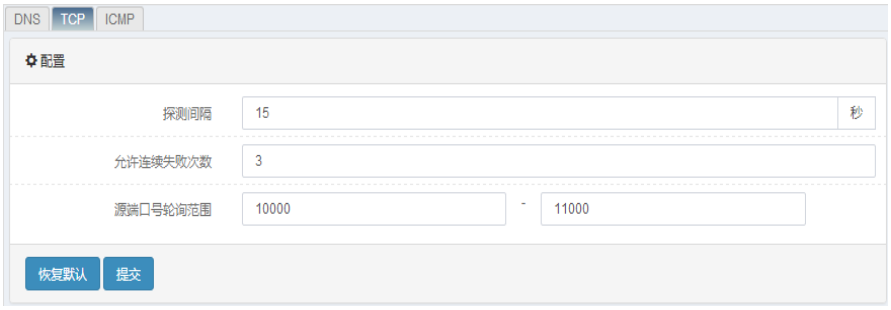
28 第28章 NAT 地址池检查

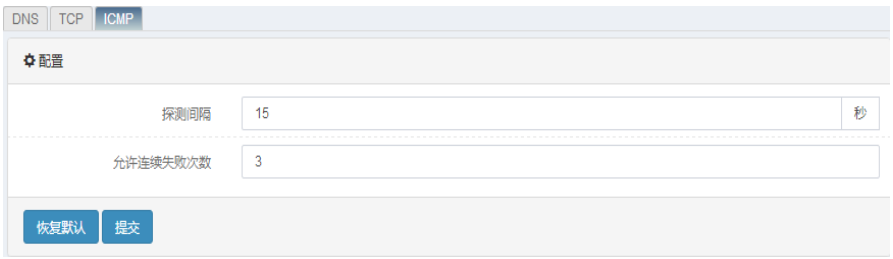
28.1 配置地址池检查功能

NAT 地址池检查功能用于检查 NAT 地址池中 NAT 地址的可用性。开启该功能后，在做源 NAT 时可以排除掉 NAT 地址池中不可用的 NAT 地址。NAT 地址池检查功能支持 DNS、TCP、ICMP 三种检查方式，每个 NAT 地址池可以根据具体情况选择其中一种方式进行检查，每种检查类型对应的参数都有默认配置。

配置步骤：

1. 进入**网络>NAT>NAT 地址池检查。**





探测间隔：默认值为 15 秒。每隔 15 秒对 NAT 地址池中地址进行一次可用

性检查。

允许连续失败次数：默认值为 3 次。举例，若探测间隔为 15 秒，每隔 15 秒对 NAT 地址池中的地址进行一次可用性检查，若地址 A 经检查，发现它的状态不可用，记为 1 次失败，15 秒后，进行第二次检查，以此类推，当地址 A 的连续失败累加次数达到 3 次时，A 的最终状态就标记为不可用。

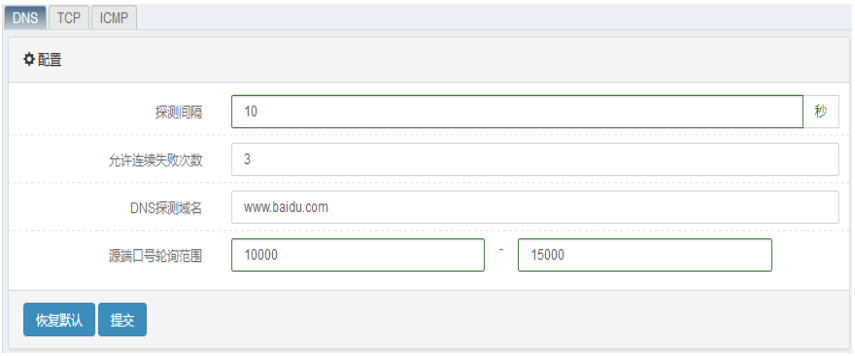
DNS 探测域名：默认值为 www.baidu.com。域名长度不可超过 128 个字符。

源端口号轮询范围：默认的范围为 10000~11000。源端口号轮询允许的范围为 1024~65535。

注意 地址池检查功能仅限于 IPv4 协议类型。

28.2 修改地址池检查配置

进入**网络>NAT>NAT 地址池检查**



选择 DNS 检查类型模板进行参数修改，完成后，点击**提交**。若想要恢复到默认配置，则点击**恢复默认**，再点击**提**交。TCP 和 ICMP 检查类型模板修改与 DNS 检查类型模板修改类似。

探测间隔：发起 NAT 地址池检查的时间间隔

允许失败次数：NAT 检查报文失败次数阈值，当达到这个数值后，认为这个地址池的地址不可用。

DNS 探测域名：NAT 地址池检查使用 dns 探测的方式进行检查时，

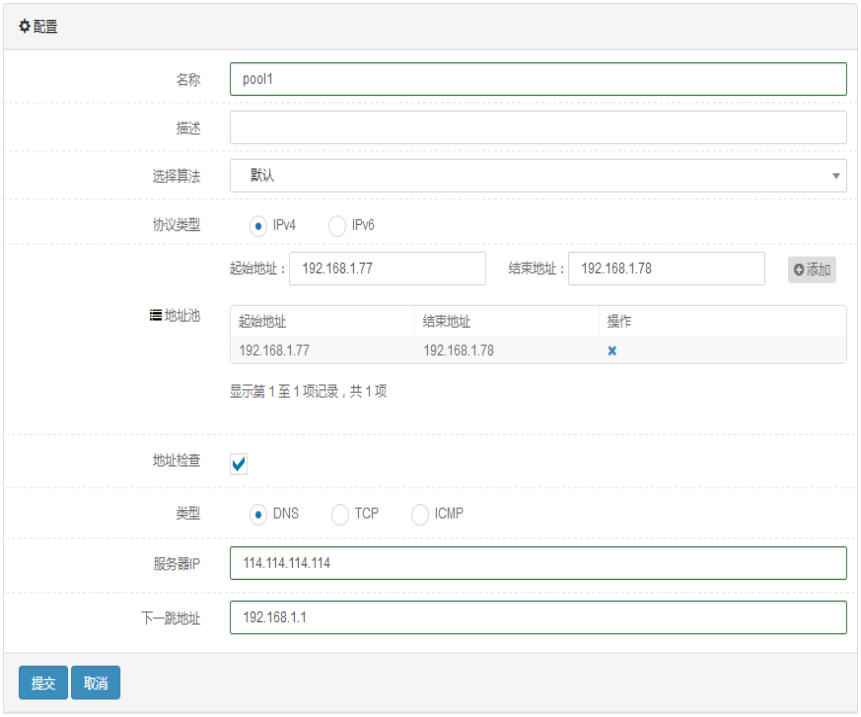
需要配置一个域名，用于检测。

源端口范围：发送报文使用的源端口，默认 10000-11000

28.3 开启地址池检查功能

进入**网络>NAT>NAT 地址池。**

未开启 NAT 检查的地址池状态栏显示探测结果为未知。点击地址池名称，进入地址池编辑页面开启检查功能。

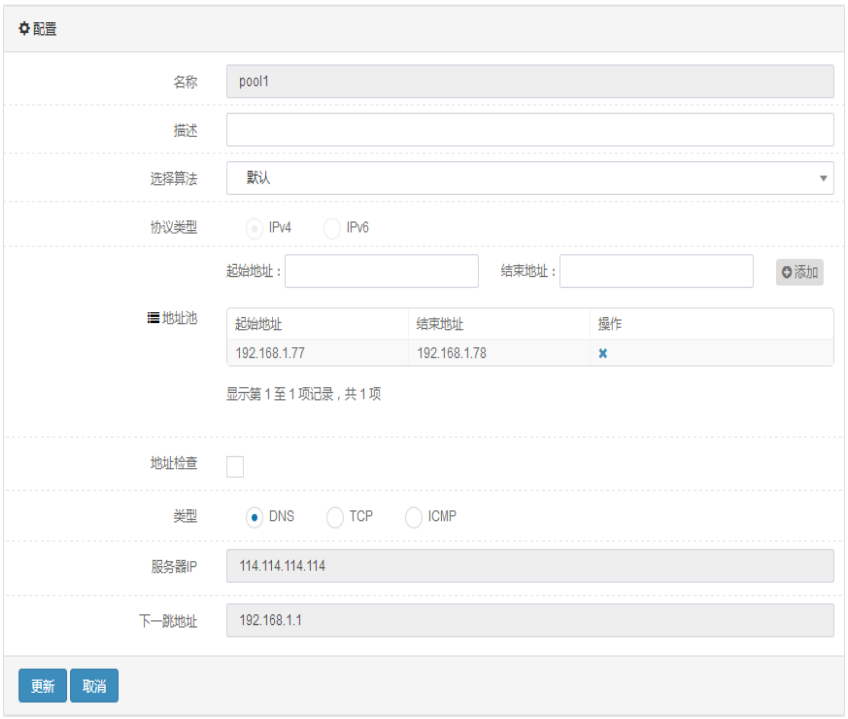


选中**地址检查**选项，填入服务器 IP 地址和下一跳地址,如果是 tcp 类型还需要配置目的端口。然后点击更新即可。

28.4 关闭地址池检查功能

进入**网络>NAT>NAT 地址池。**

选择需要关闭检查功能的地址池。

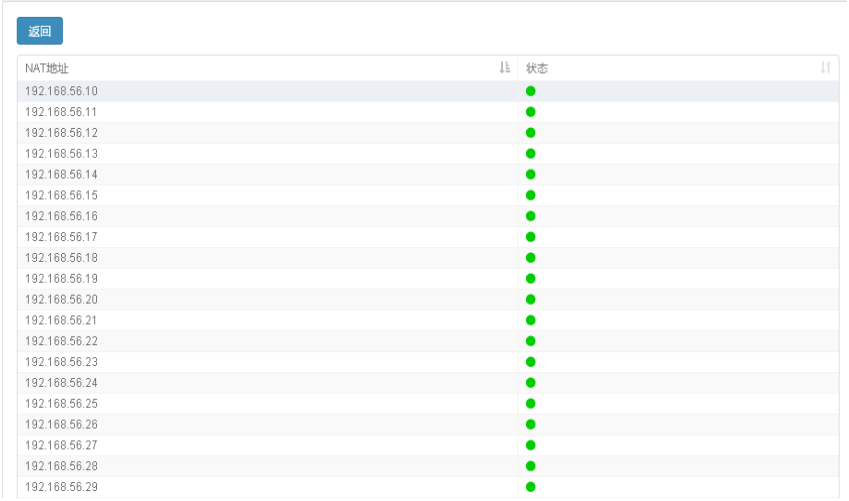


取消勾选**地址检查**这一项，点击**更新**即可。

28.5 查看地址池检查状态

进入**网络>NAT>NAT 地址池。**

可通过检查结果一栏查看地址池状态统计。点击地址池对应的检查结果可以查看某一个地址池中具体 ip 地址的详细探测结果：


返回
NAT地址
状态
192.168.56.10
192.168.56.11
192.168.56.12
192.168.56.13
192.168.56.14
192.168.56.15
192.168.56.16
192.168.56.17
192.168.56.18
192.168.56.19
192.168.56.20
192.168.56.21
192.168.56.22
192.168.56.23
192.168.56.24
192.168.56.25
192.168.56.26
192.168.56.27
192.168.56.28
192.168.56.29

29 第29章 跨协议转换

29.1 跨协议转换概述

跨协议转换，即 IPv4 与 IPv6 的相互转换，实现两种协议栈无缝对接。满足用户从 IPv4 网络环境逐步向 IPv6 网络环境过渡需要。

目前 T 系列防火墙设备实现了 NAT46，即 IPv4 端发起请求，将其转换为 IPv6 地址，以及 NAT64，即 IPv6 端发起请求，将其转换为 IPv4 地址的转换功能。并在此基础上提供了多种转换方式，可根据用户的实际环境选取合理的转换方式，实现 IPv4 网络与 IPv6 网络之间的互访。

29.2 配置跨协议转换规则

跨协议转换分为 NAT46 和 NAT64 两种转换类型，目前设备提供三种转换方式：IVI 转换，嵌入地址转换以及地址池转换。

29.2.1 配置IVI转换方式

IVI 转换方式是由中国教育和科研计算机网（CERNET）提出的一种无状态的地址映射方式，通过使用指定的前缀，可实现 IPv4 与 IPv6 地址之间的互相转换。

IVI 转换方式支持 NAT46 和 NAT64。

配置步骤：

1. 进入**网络>NAT>NAT 规则：跨协议转换**，点击**新建。**

启用：规则是否生效。

转换类型：选择当前规则是执行 NAT46 还是 NAT64 功能。

转换方式：包括 IVI，嵌入地址转换和地址池三种转换方式，这里选择 IVI。

源地址：选择匹配该规则使用的源地址对象或地址组。

目标地址：选择匹配该规则使用的目标地址对象或地址组。

服务：选择匹配该规则使用的服务对象。

入接口：匹配该规则的流量入接口。

源地址类型：该选项指定源地址采用的转换方式，包含

指定源地址前缀：源地址根据配置的前缀，采用 IVI 转换规则进行转换，必须为 32 位掩码

转换后源地址：源地址从指定的地址池中选取，或者转换为

出接口地址

指定目的地址前缀：目的地址根据配置的前缀，采用 IVI 转换规则进行转换，必须为 32 位掩码。

转换后端口：需要转换成的目的端口。

单元 ID：配置该规则的单元 ID，该 ID 在高可靠性（HA）功能启动时使用。

描述：添加对该规则的描述，最多可为 127 字节。

日志：是否开启日志功能。

响应 ARP/响应邻居请求：该规则是否响应对应的 ARP 请求或者邻居请求。(该开关控制的 NAT46 规则响应 ARP 请求的范围，以及 NAT64 规则响应邻居请求的范围由匹配的目标地址对象和入接口来决定)。


注意

NAT64 类型的 IVI 转换规则，配置时必须保证匹配的地址对象与转换前缀没有冲突，否则报文不会进行任何改变，继续进行转发。

如果匹配到 NAT64 类型 IVI 转换规则的 IPv6 数据包地址不是标准的 IVI 格式地址，报文也不会进行任何改变，直接进行转发。

2. 点击**提交**。

29.2.2 配置嵌入地址转换方式

嵌入地址转换方式，只能被用在 NAT64 的情形。转换后的目标地址是根据用户配置的前缀，从原有的 IPv6 的目标地址中取出前缀后的 32 位地址作为转换后地址。转换后的源地址可指定 NAT 地址池，或者直接转换为出接口地址。

配置步骤：

进入**网络>NAT>NAT 规则：跨协议转换**，点击**新建**，**转换类型**选择**“NAT64”**，**转换方式**选择**“嵌入地址”。**

启用：规则是否生效。

转换类型：选择当前规则是执行 NAT46 还是 NAT64 功能。嵌入地址转换必须配置 NAT64。

转换方式：包括 IVI，嵌入地址转换和地址池三种转换方式，这里选择**嵌入地址**。

源地址：选择匹配该规则使用的源地址对象或地址组。

目标地址：选择匹配该规则使用的目标地址对象或地址组。

服务：选择匹配该规则使用的服务对象。

入接口：匹配该规则的流量入接口。

转换后源地址：源地址从指定的地址池中选取，或者转换为出接口地址。

目的地址前缀：从 IPv6 目的地址中配置的前缀之后，读取嵌入的 32 位 IPv4 地址作为转换后的目的地址（前缀最长为 96 位）。

转换后端口：需要转换成的目的端口。

单元 ID：配置该规则的单元 ID，该 ID 在高可靠性（HA）功能启动时使用。

描述：添加对该规则的描述，最多可为 127 字节。

日志：是否开启日志功能。

响应邻居请求：该规则是否响应对应的者邻居请求(该开关控制的 NAT64 规则响应邻居请求的范围由匹配的目标地址对象和入接口来决定)。

进行嵌入地址转换时，如果配置的目的地址前缀与匹配到该规则的报文的目的地址不符，那么报文不会进行任何更改。

29.2.3 配置地址池转换方式

NAT64 和 NAT46 都可以使用地址池转换方式，该方式是指转换后的目的地址都从指定的地址池中选取，源地址也可从指定的地址池中选取，或者直接转换为出接口地址。

配置步骤：

进入**网络>NAT>NAT 规则：跨协议转换**，点击**新建，转换方式**选择**“地址池”。**

启用：规则是否生效。

转换类型：选择当前规则是执行 NAT46 还是 NAT64 功能

转换方式：包括 IVI，嵌入地址转换和地址池三种转换方式，这里选择**地址池**

源地址：选择匹配该规则使用的源地址对象或地址组

目标地址：选择匹配该规则使用的目标地址对象或地址组

服务：选择匹配该规则使用的服务对象

入接口：匹配该规则的流量入接口

转换后源地址：源地址从指定的地址池中选取，或者转换为出接口地址

转换后目的地址：目的地址从指定的地址池中选取。

转换后端口：需要转换成的目的端口。

单元 ID：配置该规则的单元 ID，该 ID 在高可靠性（HA）功能启动时使用

描述：添加对该规则的描述，最多可为 127 字节

日志：是否开启日志功能

响应 ARP/响应邻居请求：该规则是否响应对应的 ARP 请求或者邻居请求。(该开关控制的 NAT46 规则响应 ARP 请求的范围，以及 NAT64 规则响应邻居请求的范围由匹配的目标地址对象和入接口来决定)。

注意

转后后的目的地址中所对应的地址池中，应至少包含一个可路由的地址，否则报文会不会进行任何转换。

注意

所有的 NAT64 规则配置匹配的源地址和目的地址时，必须使用 IPv6 类型的地址对象，需要引用地址池时必须引用 IPv4 类型的地址池。

所有的 NAT46 规则配置匹配的源地址和目的地址时，必须使用 IPv4 类型的地址对象，需要引用地址池时必须引用 IPv6 类型的地址池。

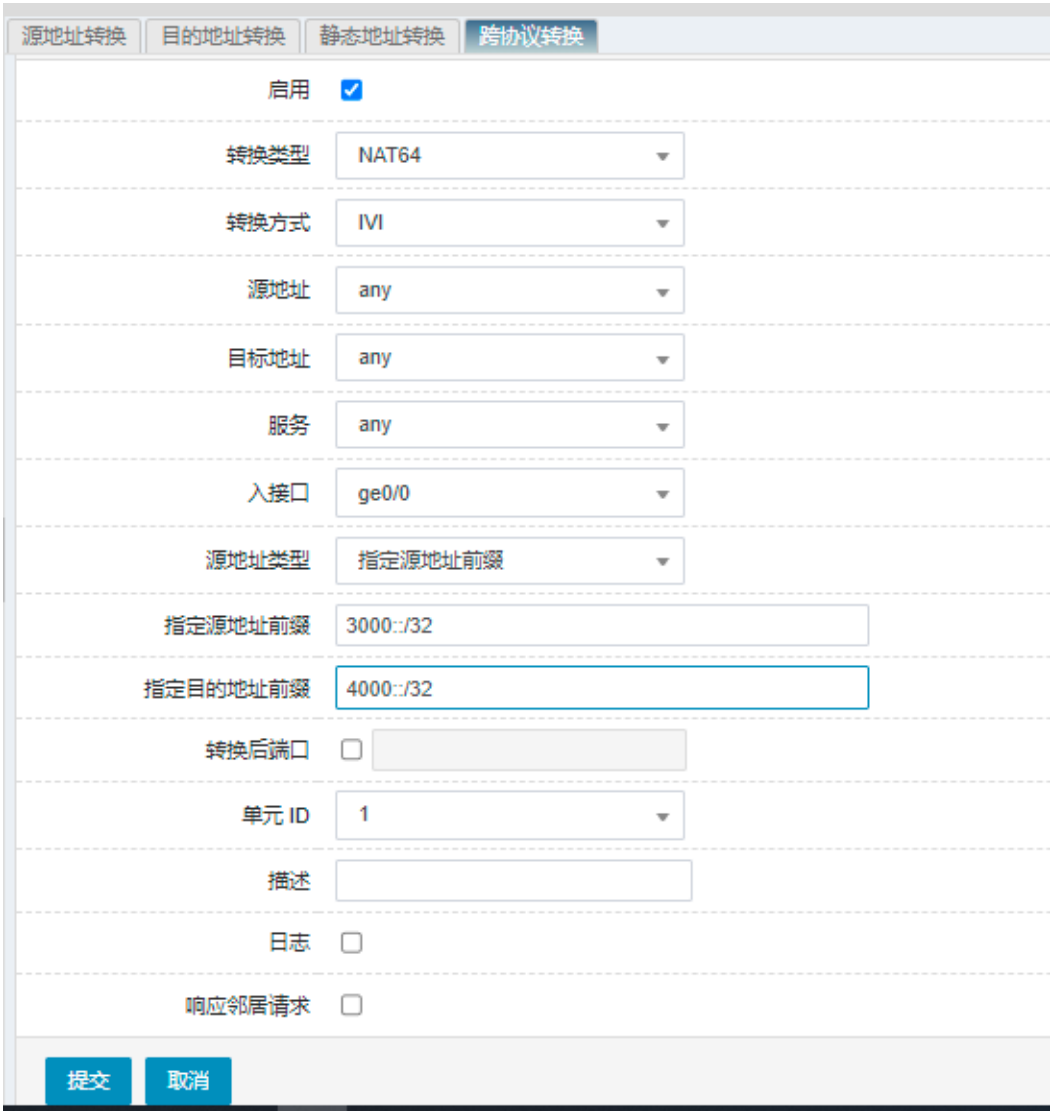
29.2.4 编辑跨协议转换规则

已经创建的跨协议转换规则可以进行编辑修改。

编辑步骤：

1.进入**网络配置>NAT>跨协议转换。**

2.点击规则编号。



3.对原有的规则进行编辑，其中**转换类型**不允许修改。

4.点击**更新**。

29.2.5 删除跨协议转换规则

删除步骤：

1. 进入**网络配置>NAT>跨协议转换**。

2. 点击规则编号后对应的✖，删除该条跨协议转换规则。

29.2.6 移动跨协议转换规则

相同转换类型（NAT64 或 NAT46）的跨协议转换规则可通过移动操作，调整匹配的顺序。

配置步骤：

1. 进入**网络配置>NAT>跨协议转换。**

2. 点击要移动的规则编号后对应的，可移动该规则。

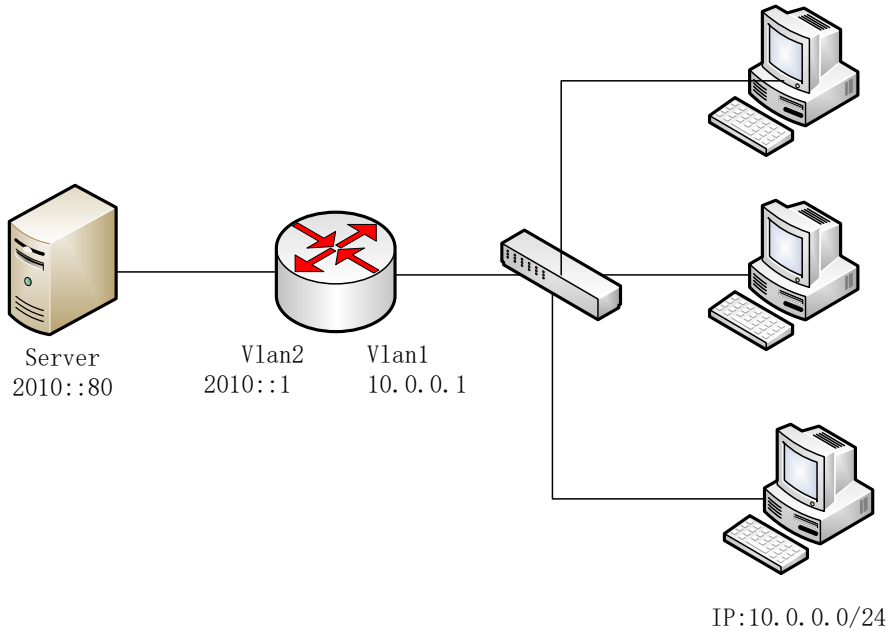
29.3 配置案例

29.3.1 配置NAT46转换

案例描述：

公司内部局域网为 IPv4 网络，需要通过 T 系列防火墙设备访问另外一个 IPv6 网络类型局域网中的一个 FTP 站点。该站点的地址为 2010::80，公司内部网段为 10.0.0.0/24。T 系列防火墙设备作为核心路由，串行接入网络。

NAT46 配置案例组网图：



配置步骤：

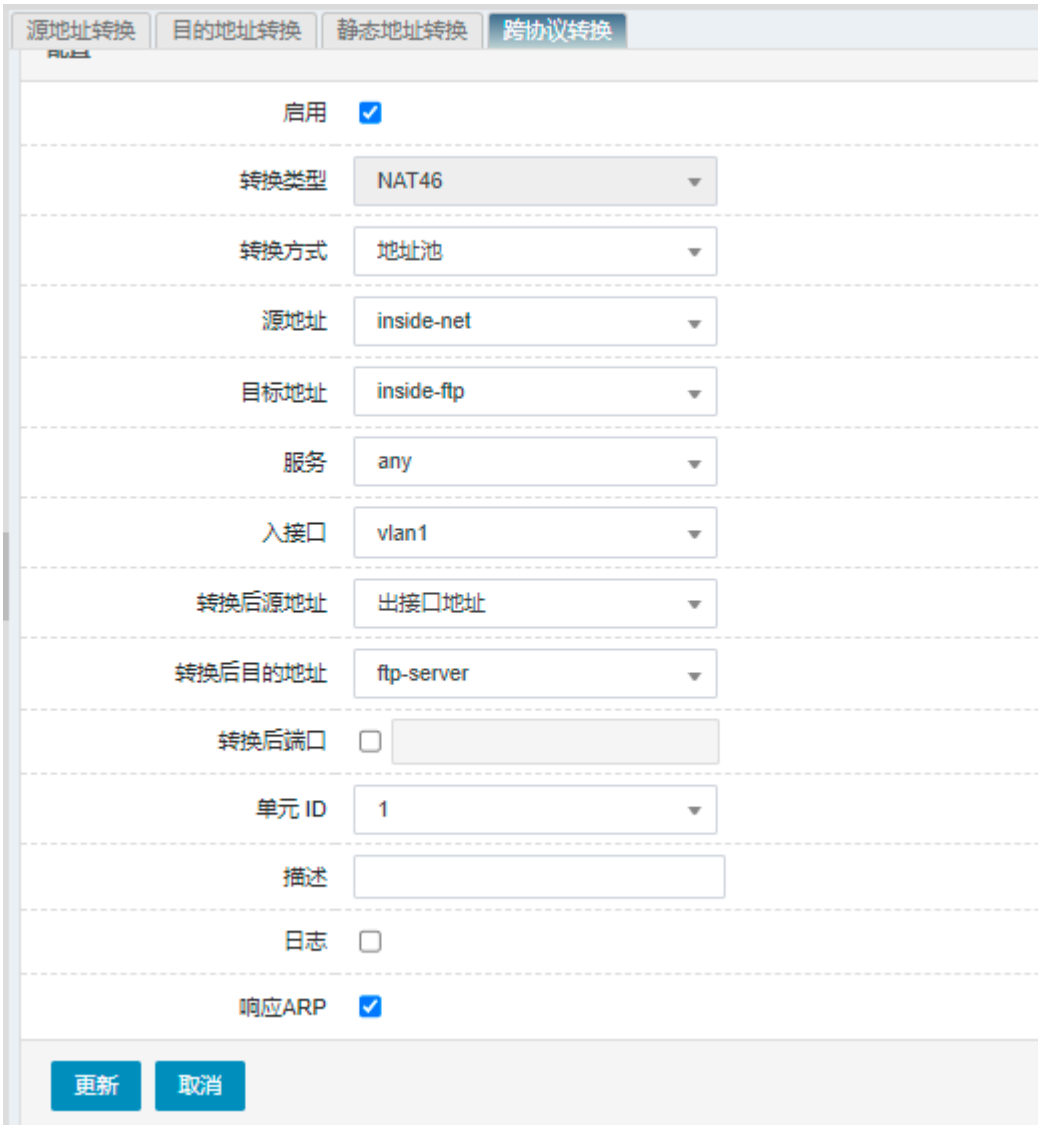
1. 进入**对象->地址对象->地址节点，**创建 IPv4 类型的地址对象“inside-net”。
2. 进入**对象->地址对象->地址节点，**创建 IPv4 类型的地址对象“inside-ftp”，该地址将作为 FTP 服务器在内网的映射地址，不能与内网任何一台 PC 的地址冲突。

名称	成员	排除	描述	引用	
any	0.0.0.0/0,::/0			1	
inside-net	10.0.0.0/24			0	
inside-ftp	10.0.0.100			0	

3. 进入**网络->NAT->NAT 地址池，**创建 IPv6 类型的地址池“ftp-server”。

ftp-server			默认		
	2010::80	2010::80			

4. 进入**网络->NAT->跨协议转换，**创建 NAT46 规则。



注意

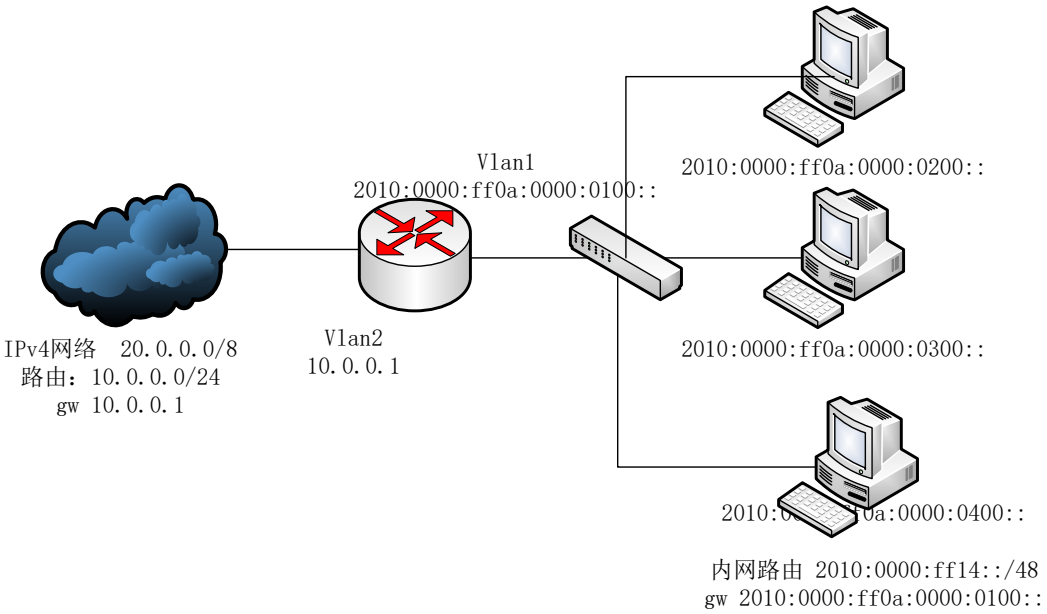
这种环境下，设备会代理 IPv6 服务器的业务，所以配置时要勾选响应 ARP，以保证 IPv4 内网向代理服务器地址 10.0.0.100 发出的请求能被发送至设备上。

29.3.2 配置NAT64转换

案例描述：

ISP 分配了一个 IVI 前缀 2010::/32 给 IPv6 类型的教育局域网，该局域网中的用户需要访问外网的 IPv4：20.0.0.0/8 网段。T 系列防火墙设备作为核心路由，串行接入设备。

配置案例组网图：

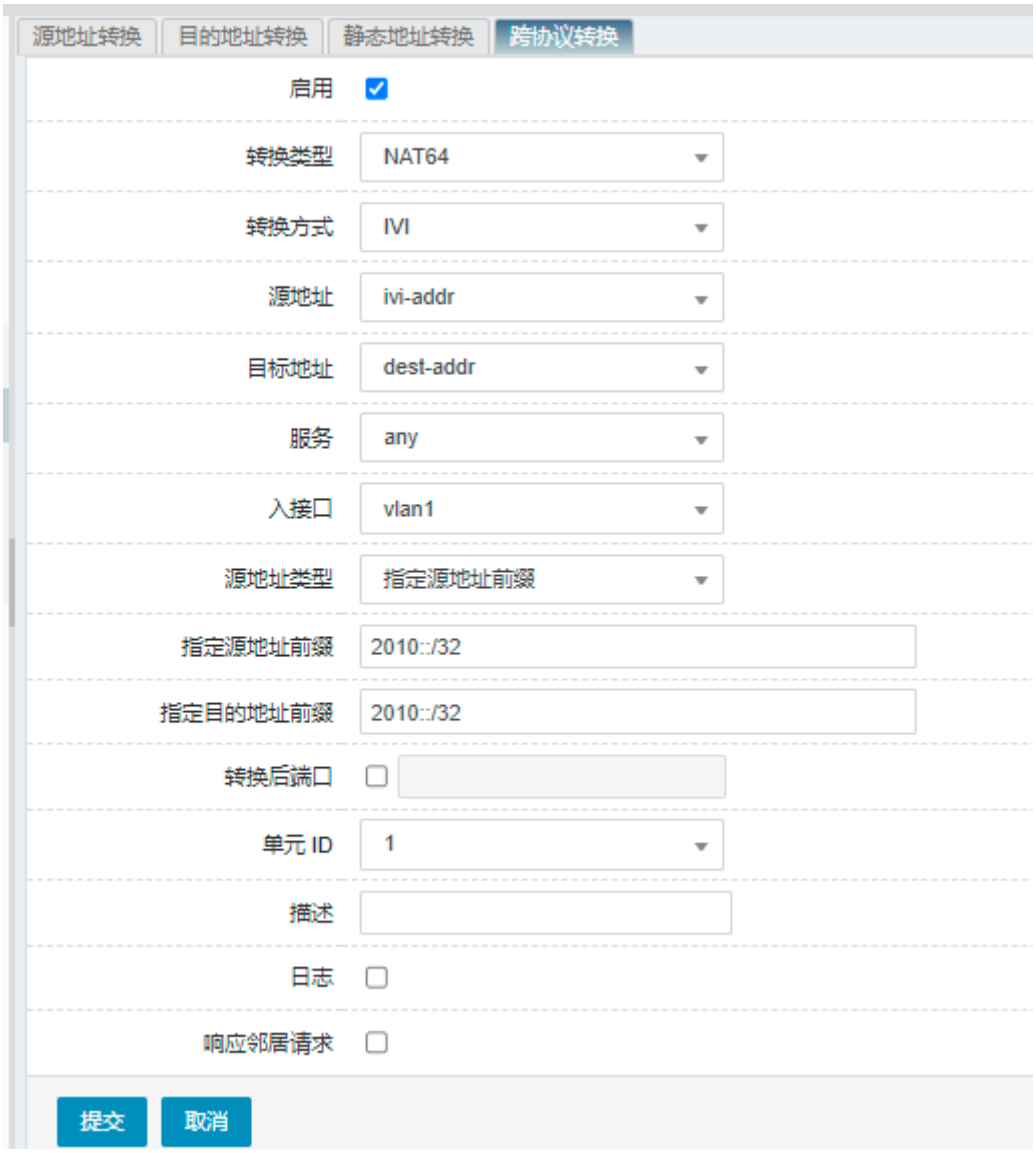


配置步骤：

1. 进入**对象->地址对象->地址节点**，创建 IPv6 类型的地址对象“ivi-addr”和“dest-addr”。

ivi-addr	2010:0:ff00::/40		0	
dest-addr	2010:0:ff14::/48		0	

2. 进入**网络->NAT->跨协议转换，**配置 NAT64 转换规则。



注意

1.该用例由于内网主机上都需配置对应的路由，所以配置 NAT64 规则时不用勾选“响应邻居请求”

2.针对 IVI 转换，设备不会响应转换后地址对应的 ARP 请求或者邻居请求，所以网络中必须配置对应的路由。

29.4 常见故障分析

29.4.1 用户发现网络中一直有地址冲突的情形

故障现象	用户发现PC一直有地址冲突的情形。
分析与解决	可查看NAT64/NAT46规则是否开启响应邻居/ARP请求，如果开启

	了，设备会响应入接口收到的匹配的目的地址的邻居/ARP请求。如果用户配置的匹配目的地址为”any”，建议不要轻易开启响应邻居/ARP请求。

29.4.2 用户发送的请求报文无法到达设备

故障现象	用户想通过NAT64/NAT46访问跨协议网络，但是抓包发现请求报文一直在发送ARP或者NS请求。
分析与解决	可查看NAT64/NAT46规则是否开启响应邻居/ARP请求，如果没有开启可能导致请求报文无法学到对应目的地址的MAC。

29.4.3 地址转换失败

故障现象	用户在设备出口抓包发现，地址没有进行任何转换
分析与解决	如果是NAT64转换，可查看配置： 1. IVI转换方式，源或目的地址如果不是严格的IVI地址格式，则地址不会进行任何转换 2. IVI转换方式，如果配置的匹配规则的地址对象，和配置的前缀有冲突，则不会进行任何转换 3. 嵌入地址转换方式，如果配置的匹配规则的目的地址对象，与配置的目的地址前缀有冲突，则不会进行任何转换 如果转换后的目的地址路由失败，那么报文也不会进行转换。

30 第30章 端口管理

30.1 端口管理概述

针对服务器有时会改变或者添加所提供服务对应的监听端口号的情况，设备需要改变或添加预置的 ALG 端口号，使设备能正确识别报文中端口号所对应的服务类型。

例如，某个 FTP 服务器除了开放 21 端口监听请求之外，也开放了 1000 端口监听 FTP 请求；当设备接收到一个报文的目的端口号为 1000 时，要识别出该报文为一个 FTP 相关报文，这样就需要设备对 ALG 的端口进行一定的处理。

30.2 端口配置

30.2.1 设置端口号

进入**网络>NAT>端口管理**，点击“新建”按钮。如下图：

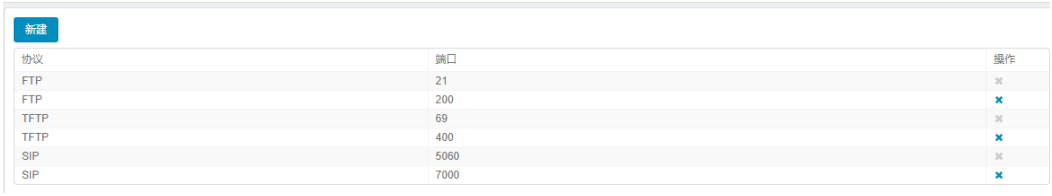
协议：协议类型，目前仅支持 FTP、TFTP 和 SIP。

端口：要添加的协议的监听端口号。

注意 每个协议，除了默认端口，最多可以添加 7 个端口号。

30.2.2 删除端口号

进入**配置>NAT>端口管理.**



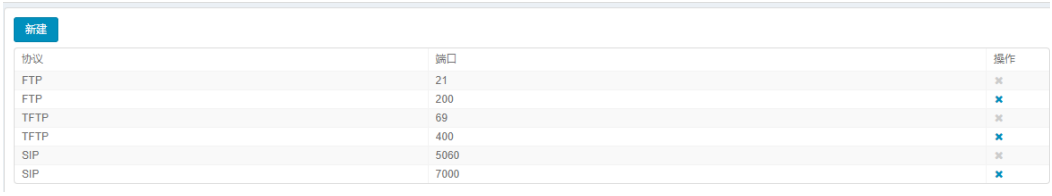
点击最后一列的图标，即可删除配置的端口号。

注意

协议对应的默认端口号无法改变或删除。

30.2.3 查看端口号

进入**配置>NAT>端口管理**，可查看到配置的所有端口号。



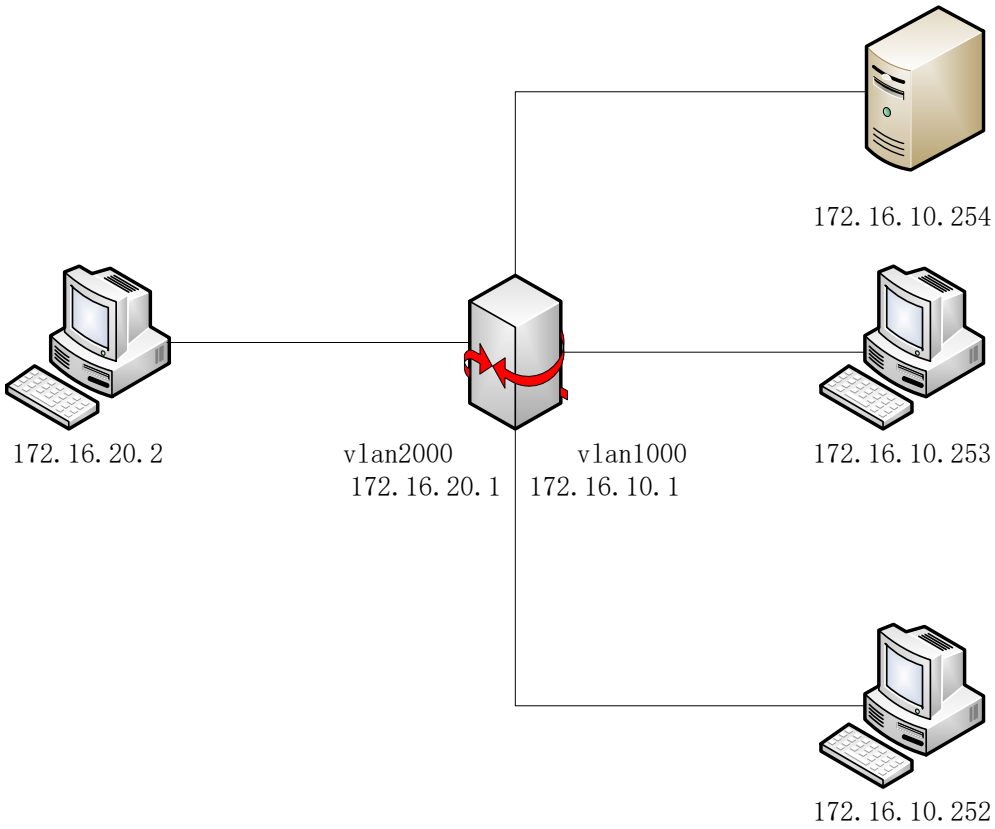
30.3 配置案例

配置案例 1

案例描述：

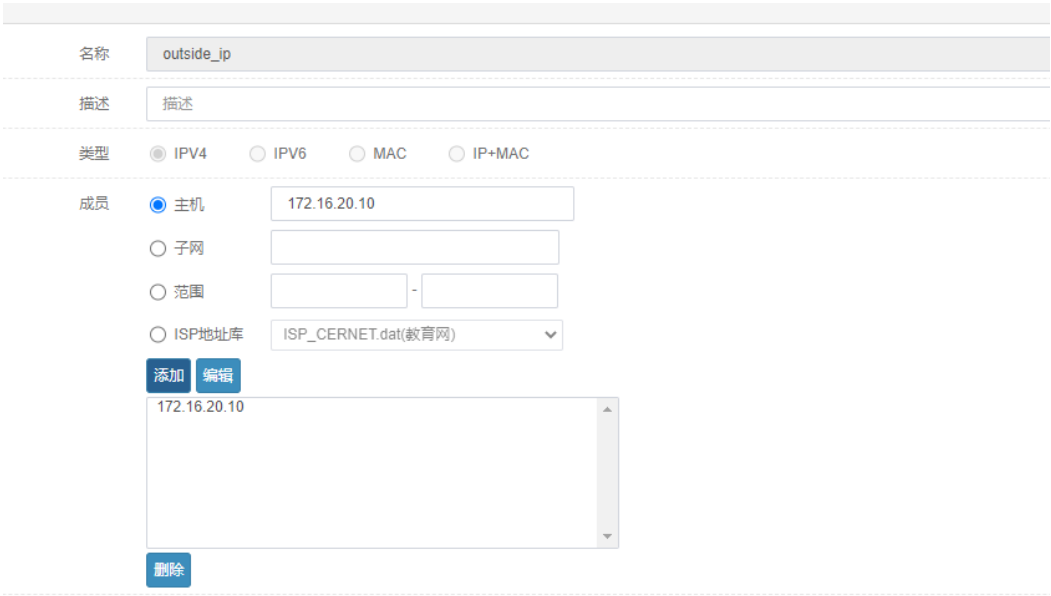
外网客户端访问内网的 FTP Server，FTP Server 端口为非默认端口 2121。

案例组网图：

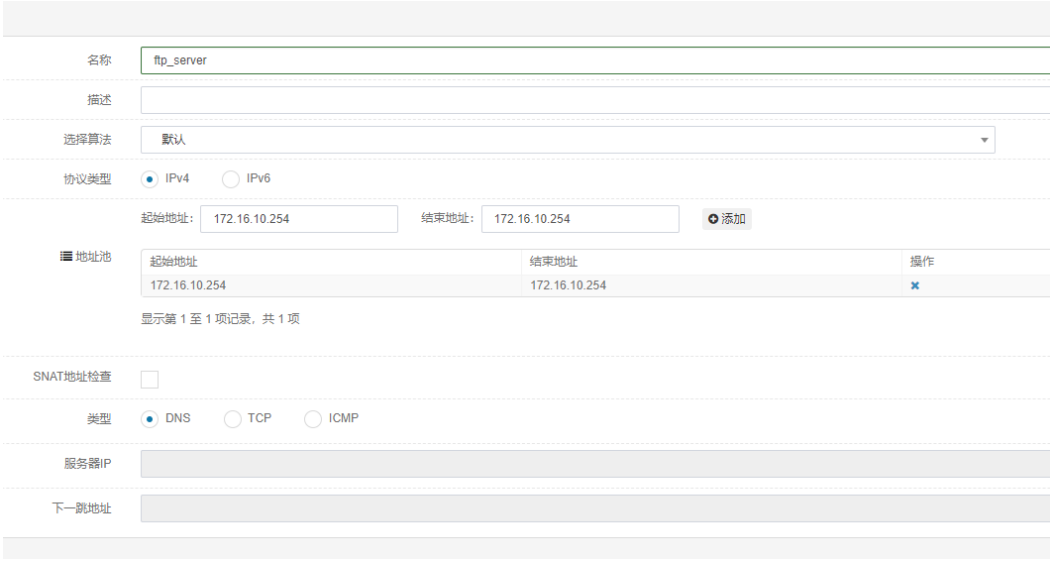


配置步骤：

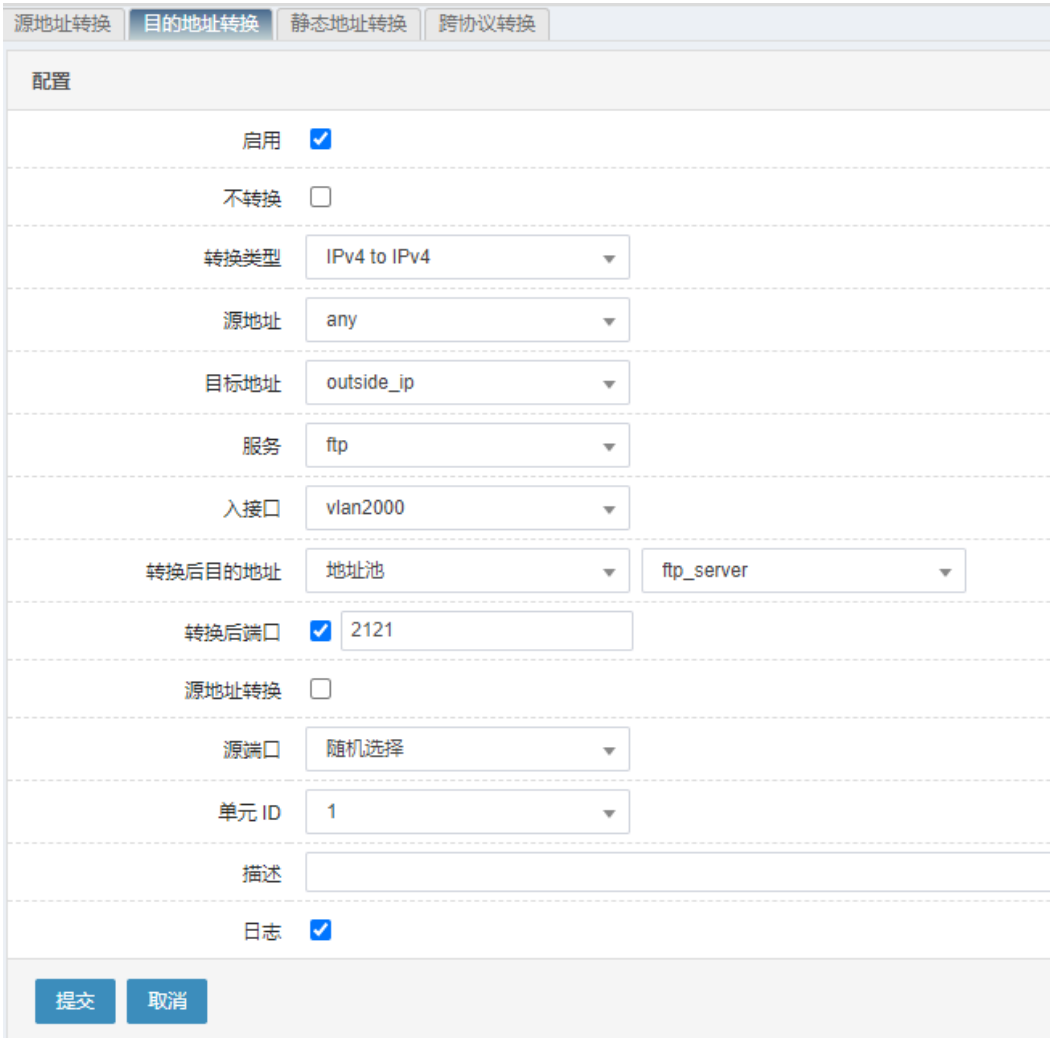
1、 新建地址对象，**对象>地址对象>地址节点**，点击**新建**。



2、 新建地址池，**网络>NAT>NAT 地址池**，点击**新建**。



3、 新建目的地址转换，**网络>NAT>NAT 规则>目的地址转换**，点击**新建**。



4、 **配置端口管理，网络>NAT>端口管理**，点击**新建**按钮。如下图：

点击“**提交**”提交配置。

注意 不同的协议添加的端口可以相同。

31 第31章 IPSec VPN

31.1 概述

IPSec 用于保护敏感信息在 Internet 上传输的安全性。它在网络层对 IP 数据包进行加密和认证。IPSec 提供了以下网络安全服务，这些安全服务是可选的，通常情况下，本地安全策略决定了采用以下安全服务的一种或多种。

- 数据的机密性—IPSec 的发送方对发给对端的数据进行加密
- 数据的完整性—IPSec 的接收方对接收到的数据进行验证以保证数据在传送的过程中没有被修改
- 数据来源的认证—IPSec 接收方验证数据的起源
- 抗重播—IPSec 的接收方可以检测到重播的 IP 包丢弃

使用 IPSec 可以避免数据包的监听、修改和欺骗，数据可以在不安全的公共网络环境下安全的传输，IPSec 的典型运用是构建 VPN。IPSec 使用 “封装安全载荷（ESP）”或者“鉴别头（AH）”证明数据的起源地、保障数据的完整性以及防止相同数据包的不断重播；使用 ESP 保障数据的机密性。密钥管理协议称为 ISAKMP ，根据安全策略数据库（SPDB）随 IPSec 使用，用来协商安全联盟（SA）并动态的管理安全联盟数据库。

相关术语解释：

- 鉴别头（AH）：用于验证数据包的安全协议
- 封装安全有效载荷（ESP）： 用于加密和验证数据包的安全协议；可与 AH 配合工作可也以单独工作
- 加密算法：ESP 所使用的加密算法
- 验证算法：AH 或 ESP 用来验证对方的验证算法
- 密钥管理：密钥管理的一组方案，其中 IKE（Internet 密钥交换协议）是默认的密钥自动交换协议

31.2 IPSec VPN配置过程

IPsec VPN 提供了网关到网关和远程接入的安全服务功能。并支持隧道模式、传输模式两种封装模式。身份认证支持证书认证、预共享密钥。

配置 IPsec VPN 基本过程如下：

1. 配置 IKE 协商策略，主要配置对端地址，认证方式，协商参数等。
2. 配置 IPsec 协商策略，主要配置 IPsec 加密算法，封装模式等。
3. 配置 IPsec 策略，通过配置 IPsec 策略来指定需要加密数据的

网络范围。

31.2.1 配置IKE协商策略

配置步骤：

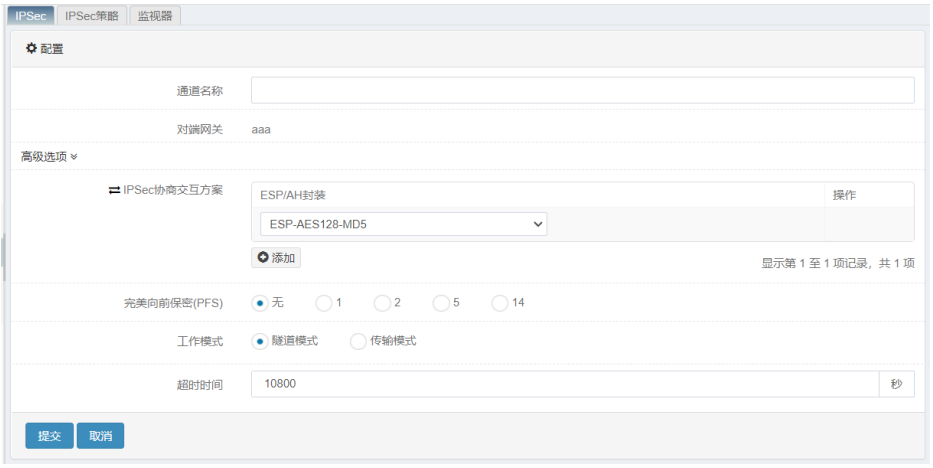
进入**网络>VPN>IPsec>IPsec**，点击 新建

1. **配置本地ＩＰ地址：**指定本地用来协商的 ip 地址。
2. **配置远程网关：**如果对端指定地址固定可以配置静态 ip 地址。如果对端地址不确定可以选择动态地址。
3. **配置认证方式：**可选预共享密钥或证书。如果是证书需要预先导入证书。预共享密钥方式需要和 IPSec VPN 对端一致。

31.2.2 配置IPSEC协商策略

配置步骤：

在 IKE 协商上，点击其对应的 ＋ 按钮，进入**新建 IPSEC 协商**



1. 配置 IPSEC 协商的**通道名称**
2. 配置 **IPSEC 协商的交互方案**。可以选择 ESP 封装算法，或 AH 的封装算法，和 IPSec 对端要保持一致。另外 Nat 穿越的情况下，不要使用 AH 封装。
3. 配置**工作模式**。网络到网络的 IPSec 传输使用隧道模式。L2tp 远程接入使用传输模式。GRE over ipsec 使用传输模式。与 IPSec 对端需要保持一致。

31.2.3 配置IPsec策略

进入**网络>VPN>IPsec>IPsec 策略**，点击**新建**

1. 配置 IPSEC 策略的名称。
2. 将需要生效的 IPSEC 策略勾选启用。
3. 配置**源地址、源端口，目的地址、目的端口，协议号**。源地址是要保护的本地私网。目的地址是要保护的对端私网。
4. 通道选择上一节 IPSEC 协商策略配置建立 VPN 隧道。

31.3 IPSec VPN配置参数

31.3.1 IKE协商参数

IKE 策略定义了 IKE 协商的一组参数。两端 VPN 设备通过 IKE 协议协商建立 ISAKMP 安全关联（IPsec 一阶段 SA） 。

配置步骤：

进入**网络>VPN>IPsec>IPsec**，点击 

网关名称：IKE 协商的名称。

类型：发起 IKE 协商的版本。

本地网关：本地网关的类型。

本地 IP 地址：本地用来接受或发起协商的地址。

对端网关：

- 静态 IP：指定对端为静态 IP 方式，会出现 **IP 地址**选项，需要配置对端 IP 地址
- 动态 IP: 指定对端为动态 IP

模式：IKE 协商的协商模式是野蛮模式还是主模式。

认证方式：在协商过程中所采用的认证方法，可选预共享密钥或证书。

预共享密钥：当采用预共享密钥的认证方法时要输入的密钥值。

本地证书：当采用证书认证方法时要选择的本地证书。

IKE 协商的交互方案：在协商过程中所采用加密算法和验证算法。

DH 组：在协商过程中做 DH 交换时采用的 group 值。

密钥周期：阶段 1 的 SA 的生存时间。

NAT 穿越保持连接的频率：设置 NAT 穿越的保活时间。

本地 ID：设置本地 ID（可选项）。主要用于 NAT 穿越中已经做静态 NAT 的情况。

对端 ID：设置对端 ID（可选项）。主要用于 NAT 穿越中已经做静态 NAT 的情况。

对等体状态检测：是否启用 DPD 功能。

DPD 穿越保持连接的频率：设置对等体检测时间。

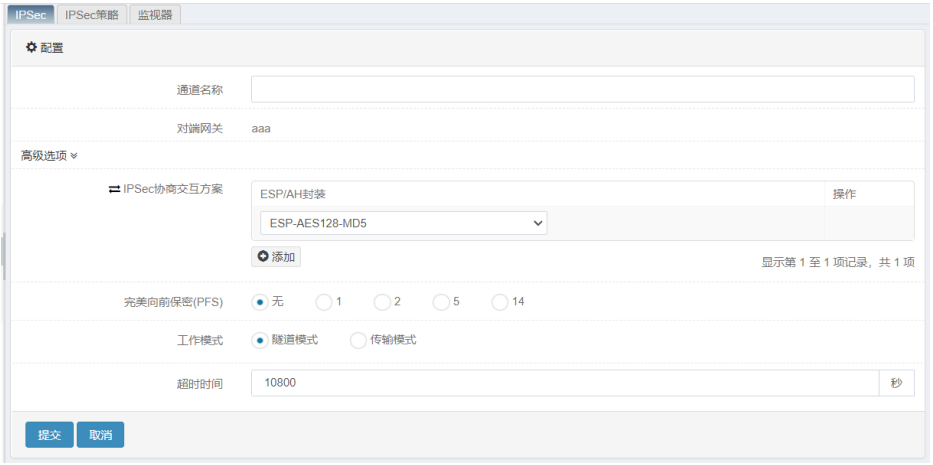
只有“类型”为“国密”，且设备上配备了硬件加密卡的情况下，才能配置“SM1”类型的加密算法。

31.3.2 IPSEC协商参数

两端 VPN 设备通过 IKE 协议协商建立 ISAKMP 安全关联后，这些参数用于协商建立 IPsec 二阶段的安全关联。

配置步骤：

进入**网络>VPN>IPsec>IPsec**，对应于已建立的 IKE 协商，点击  按钮，进入**新建 IPSEC 协商**：



通道名称：IPSEC 协商的名称

对端网关：IKE 协商的网关名称

IPSEC 协商的交互方案：协商 IPSEC 的封装方式以及算法

完美向前保密（PFS）：是否需要在 IPSEC 协商过程中采用 DH 交换

工作模式：协商 IPSEC 封装时工作方式

超时时间：阶段 2 的 IPSEC SA 的生存时间

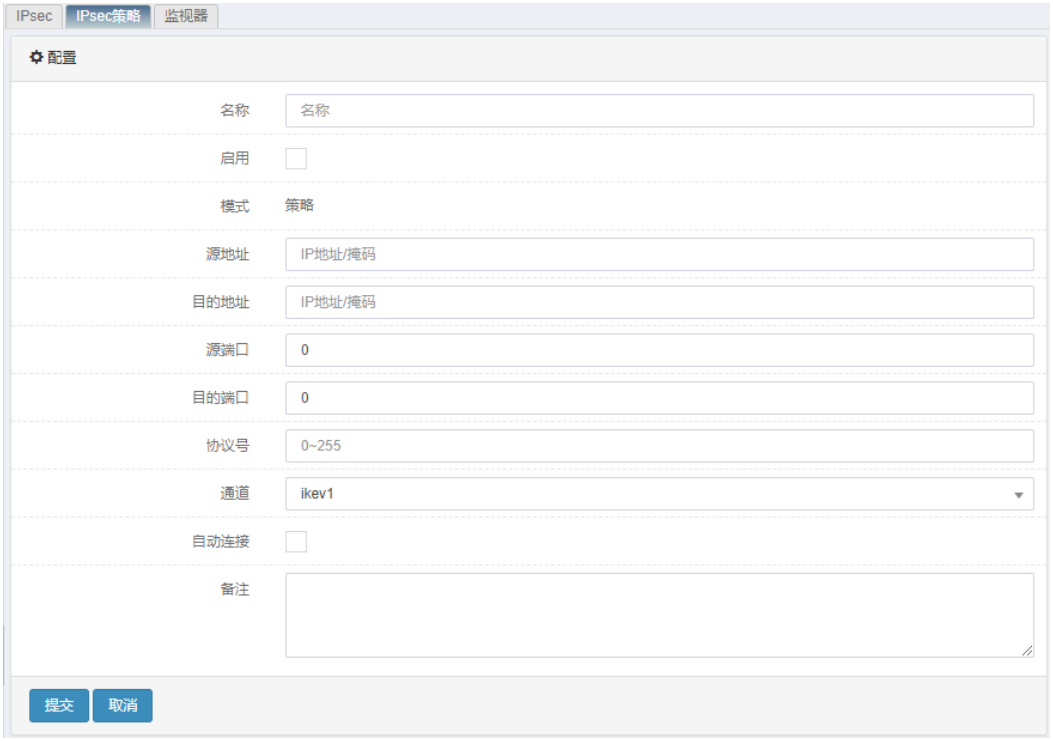

提示

只有“对端网关”的“类型”为“国密”，且设备上配备了硬件加密卡的情况下，才能配置“ESP-SM1-SM3”类型的 IPSec 协商交互方案。

31.3.3 IPsec策略

IPSEC 策略定义了 IPSEC 协商的保护子网等参数。**配置步骤：**

进入**网络>VPN>IPsec>IPsec 策略**，对应于已建立的 IKE 协商，点击  按钮，进入**新建 IPsec 策略**：



名称：IPsec 策略的名称

启用：是否启用当前策略

源地址：需要保护的本地子网的地址

目的地址：需要保护的对端子网的地址

源端口：需要保护的本地发出流量的源端口

目的端口：需要保护的本地发出流量的目的端口

协议号：需要保护的本地发出流量的目的协议号

通道：保护当前流量的阶段二

自动连接：启用后立即主动发起连接

备注：当前策略的备注信息

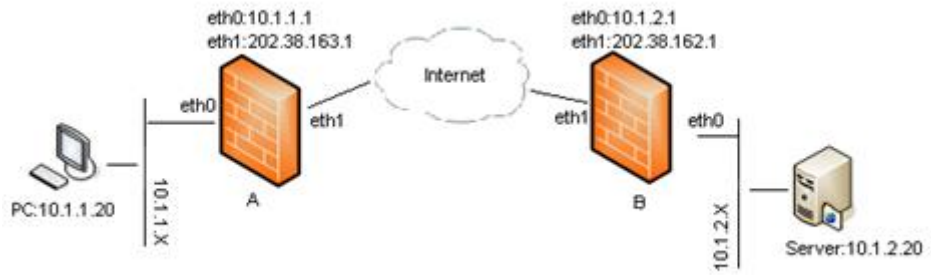
31.4 配置案例

31.4.1 配置案例1：配置IPSEC基本组网

案例描述

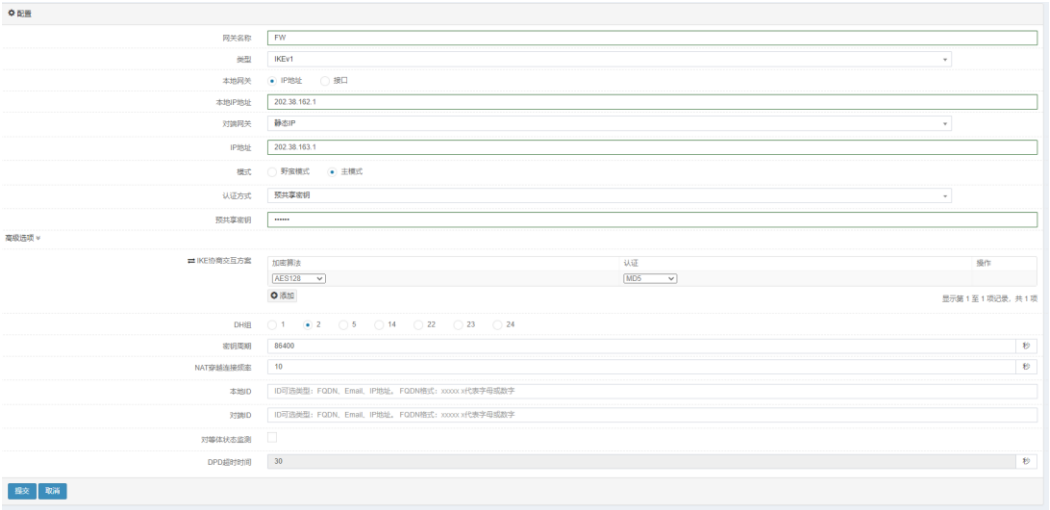
假定网络环境如下图所示，PC 机到 Server 的流量需要经过各自的 FW 设备后在 Internet 上传输，为了保证流量在 Internet 传输过程中的安全性，有必要在 FW_A 和 FW_B 之间建立 IPSec 的 VPN 隧道以保障通信安全。

图31-1 案例组网图



FW_B 配置步骤：

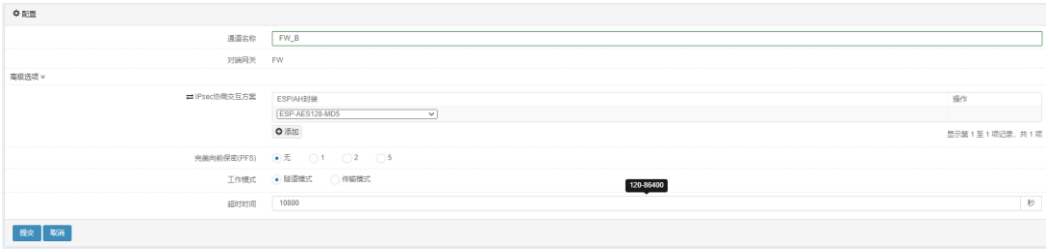
1. 进入**网络>VPN>IPsec>IPsec**，点击**新建**，参数配置如下图：



点击**提交**完成设置。

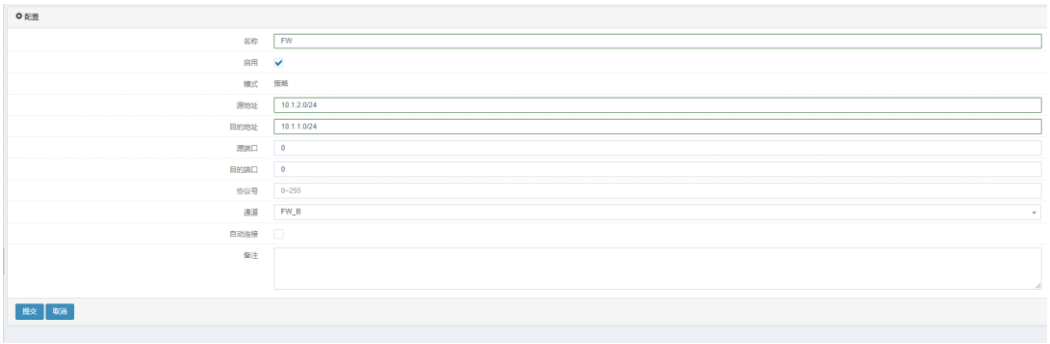
2. 进入**网络>VPN>IPsec>IPsec**，点击 **新建 IPSEC 协商**，

如下图：



点击**提交**完成设置。

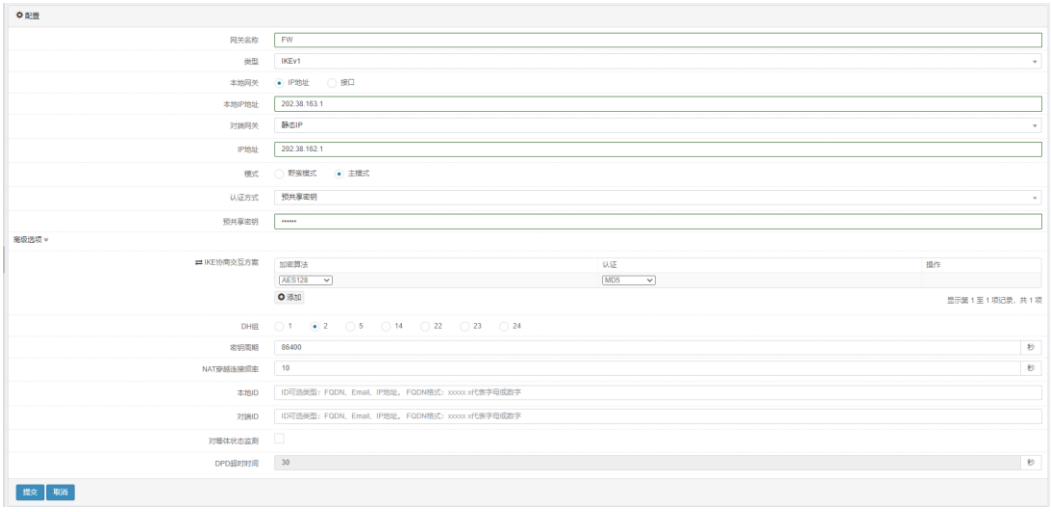
3. 进入**网络>VPN>IPsec>IPsec 策略**，建立 IPsec 策略，如下图：



点击**提交**完成设置。

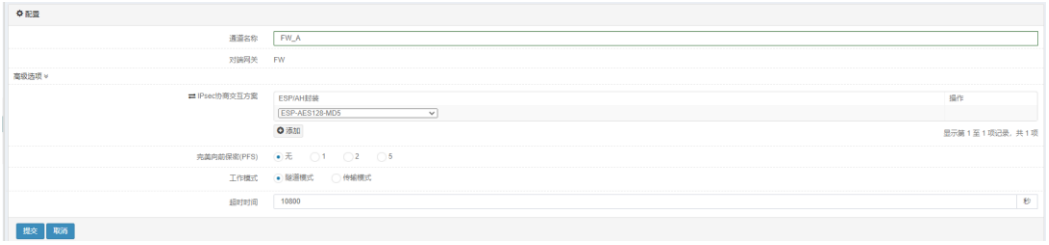
FW_A 配置步骤：

4. 进入**网络>VPN>IPsec>IPsec**，点击**新建**，如下图：



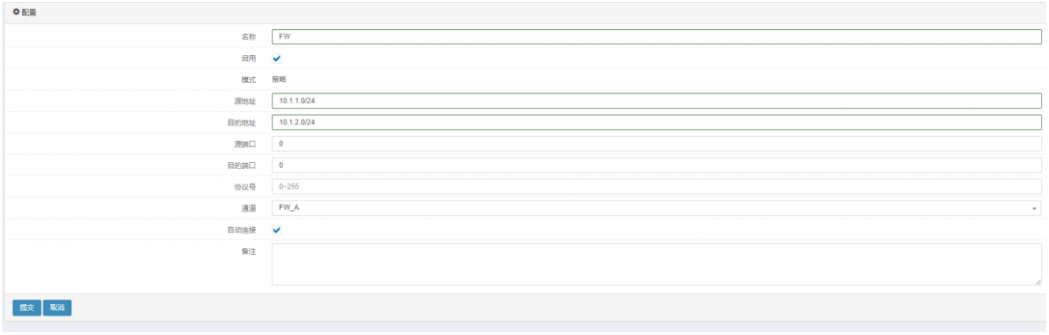
点击**提交**完成设置。

5. 进入**网络>VPN>IPsec>IPsec**，点击 **新建 IPSEC 协商**，如下图：



点击**提交**完成设置。

6. 进入**网络>VPN>IPsec>IPsec 策略**，建立 IPsec 策略，如下图：



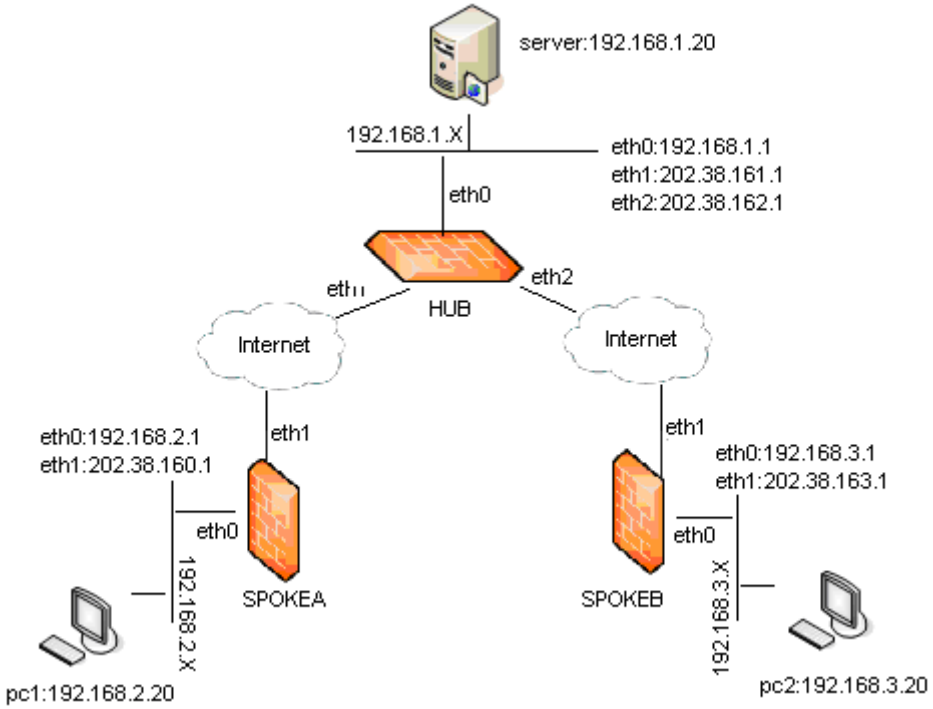
点击**提交**完成设置。

31.4.2 配置案例2：配置IPSEC HUB_SPOKE

案例描述

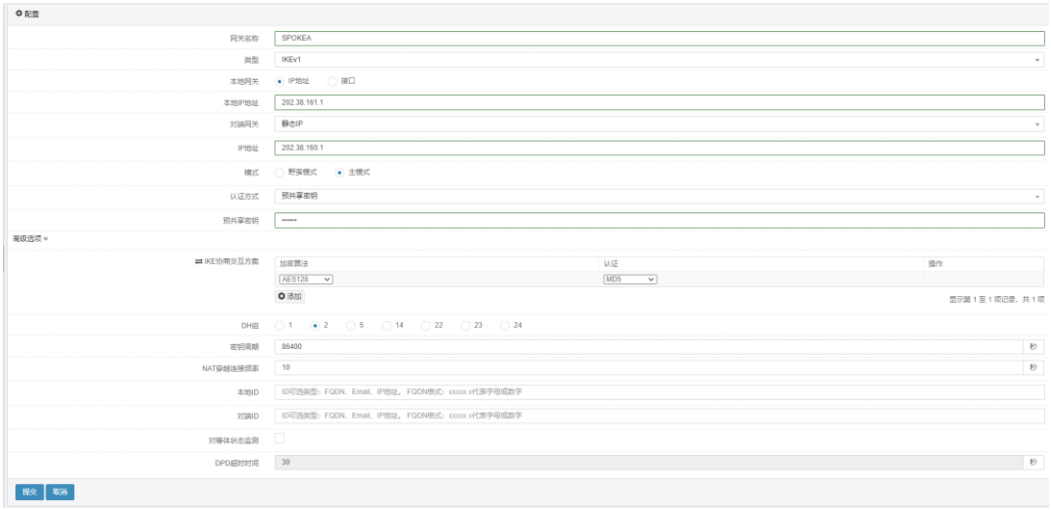
假定网络环境如下图所示， SPOKEA 想要访问 SPOKEB，但是他们之间没有网络连接。必须通过 HUB 进行转发。

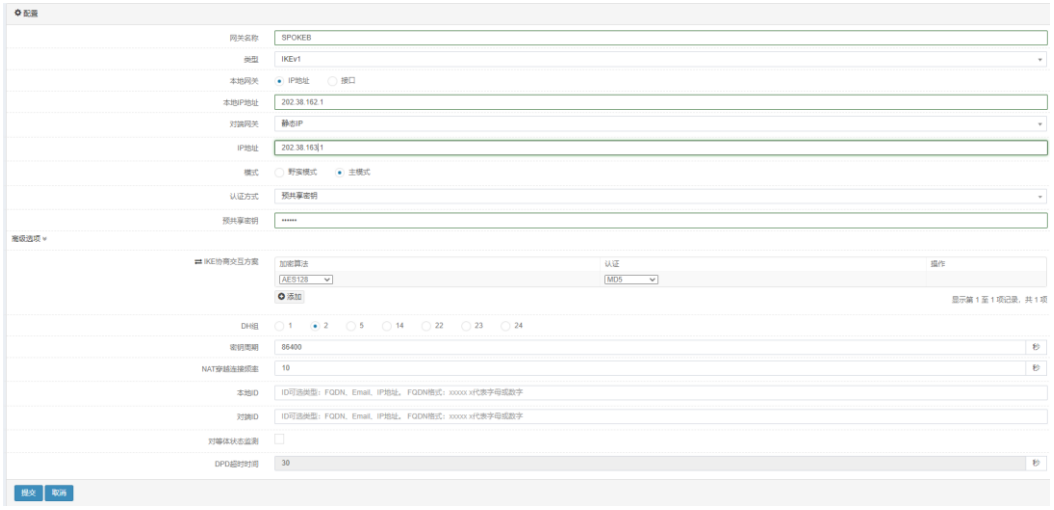
图31-2 案例组网图



HUB 配置步骤：

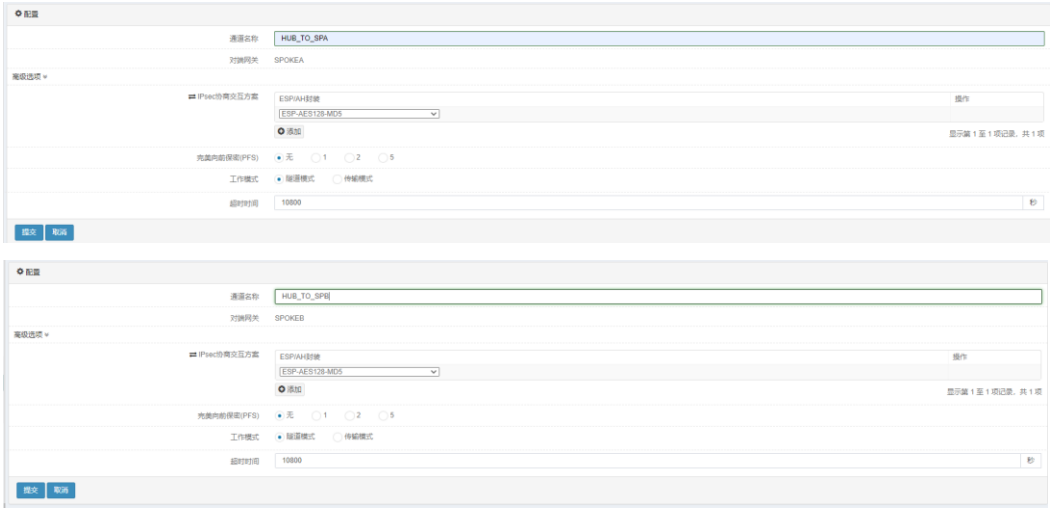
1. 进入**网络>VPN>IPsec>IPsec**，点击**新建，**如下图：





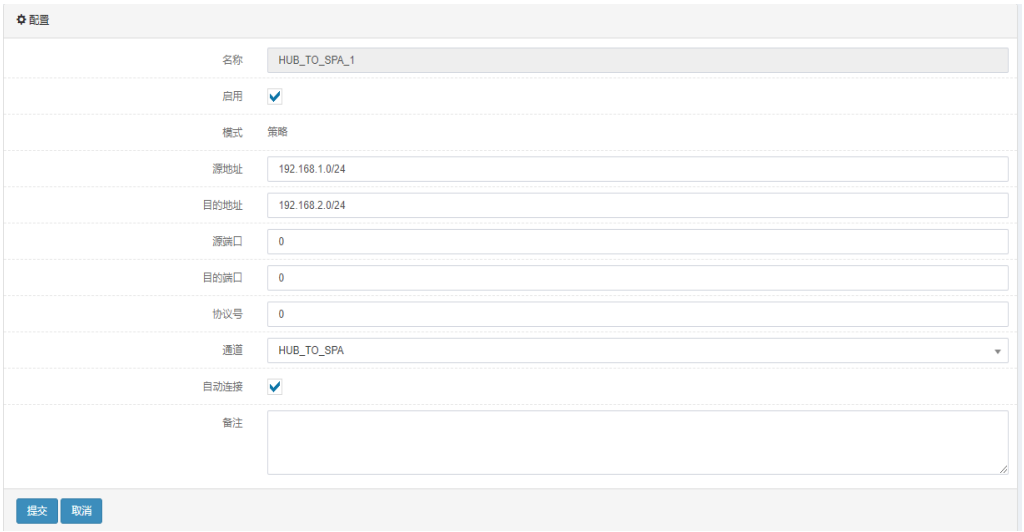
分别点击**提交**完成配置。

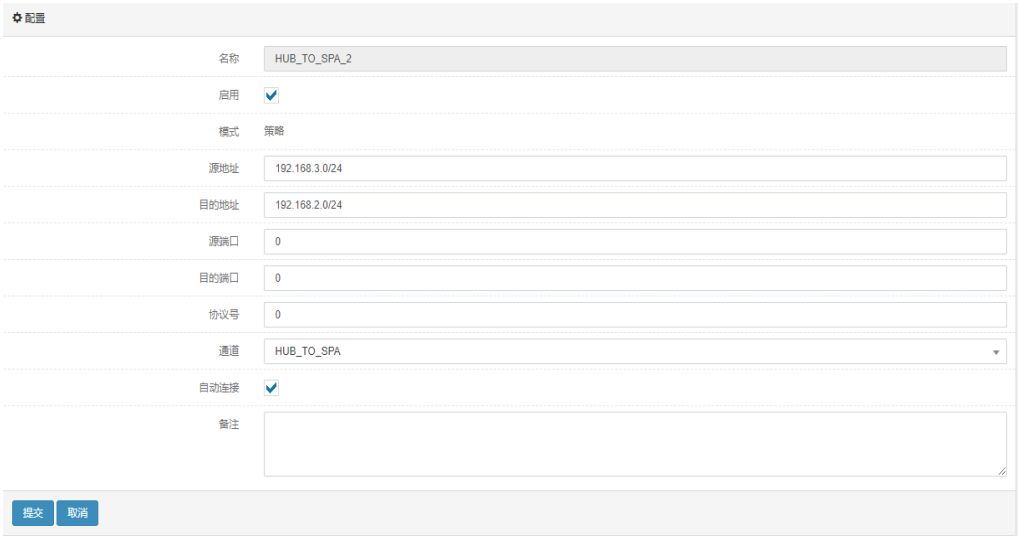
2. 进入**网络>VPN>IPsec>IPsec**，点击 新建 IPSEC 协商，如下图：

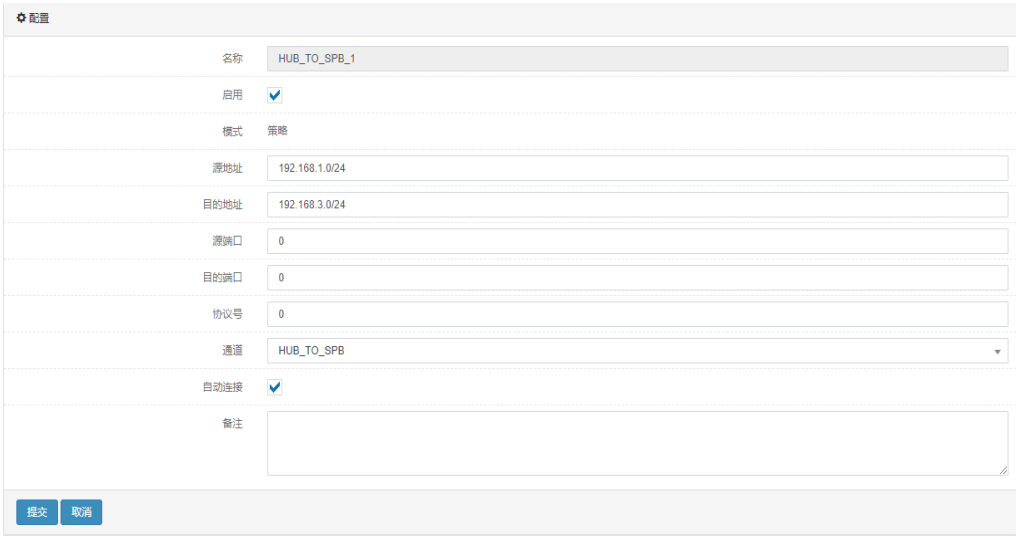


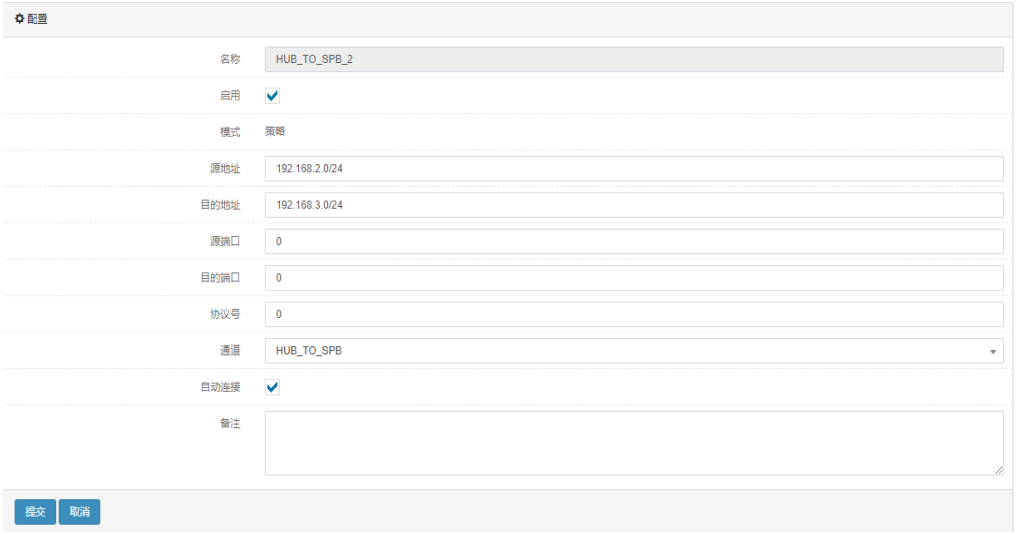
分别点击**提交**完成配置。

3. 进入**网络>VPN>IPsec>IPsec 策略**，建立 IPsec 策略，如下图：


配置
名称
HUB_TO_SPA_1
启用
模式
策略
源地址
192.168.1.0/24
目的地址
192.168.2.0/24
源端口
0
目的端口
0
协议号
0
通道
HUB_TO_SPA
自动连接
备注
提交
取消


配置
名称
HUB_TO_SPA_2
启用
模式
策略
源地址
192.168.3.0/24
目的地址
192.168.2.0/24
源端口
0
目的端口
0
协议号
0
通道
HUB_TO_SPA
自动连接
备注
提交
取消


配置
名称
HUB_TO_SPB_1
启用
模式
策略
源地址
192.168.1.0/24
目的地址
192.168.3.0/24
源端口
0
目的端口
0
协议号
0
通道
HUB_TO_SPB
自动连接
备注
提交
取消



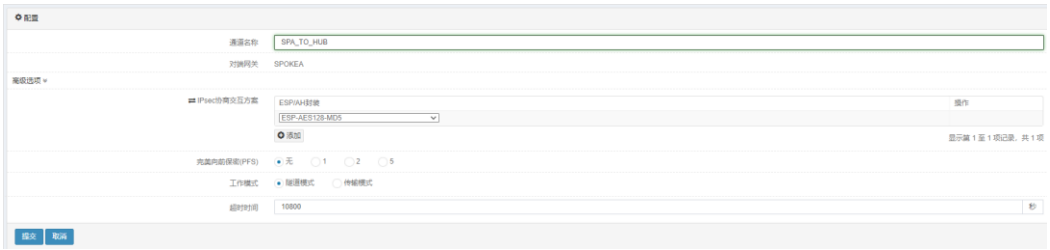
分别点击**提交**完成配置。

SPOKEA 配置步骤：

4. 进入**网络>VPN>IPsec>IPsec**，点击**新建，**如下图：

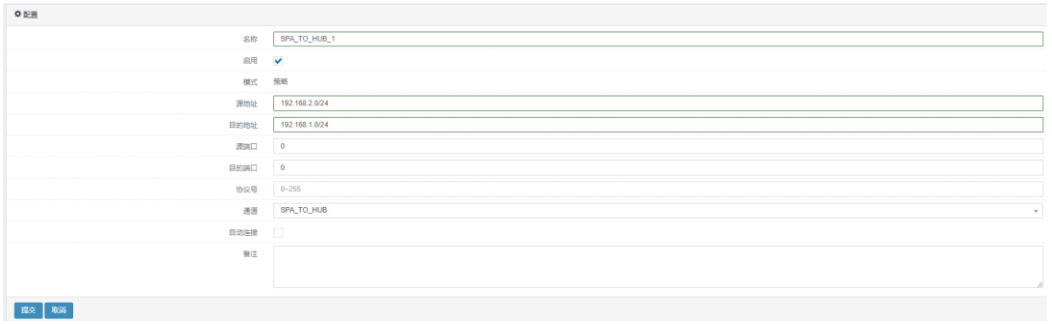
点击**提交**完成配置。

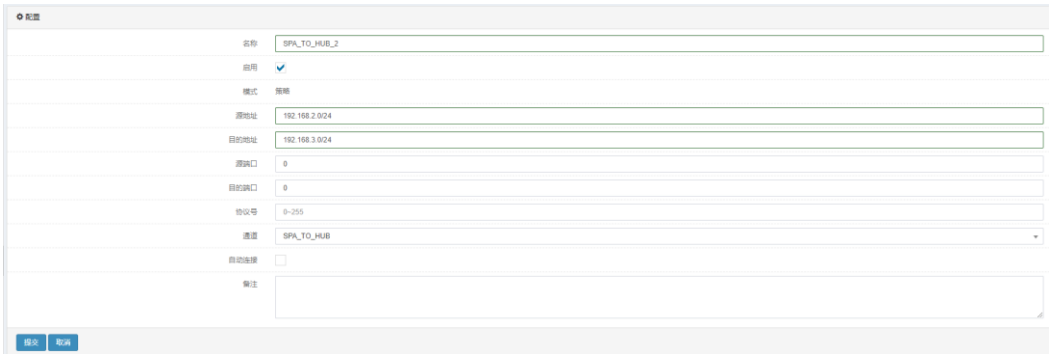
5. 进入**网络>VPN>IPsec>IPsec**，点击 新建 IPSEC 协商，如下图：



点击**提交**完成配置。

6. 进入**网络>VPN>IPsec>IPsec 策略**，建立 IPsec 策略，如下图：

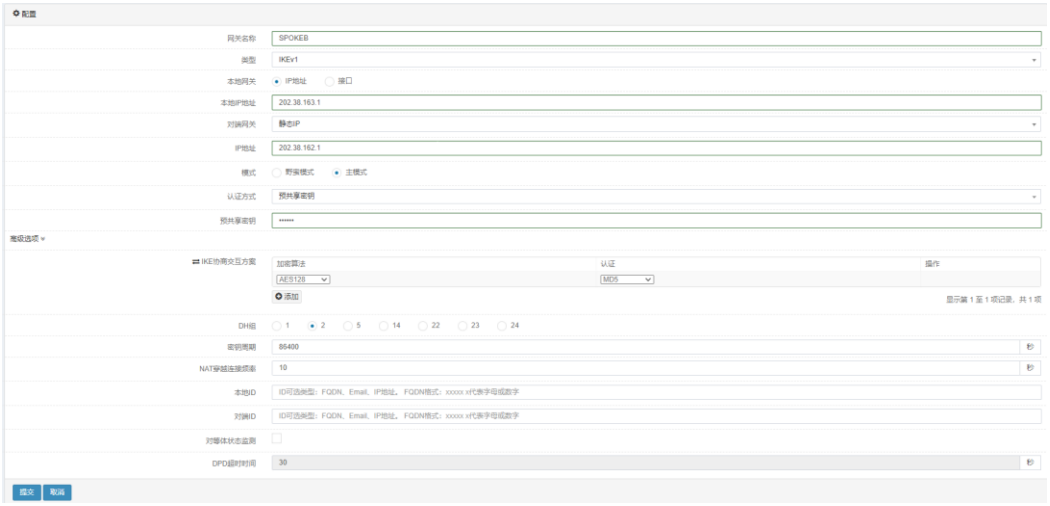




分别点击**提交**完成设置。

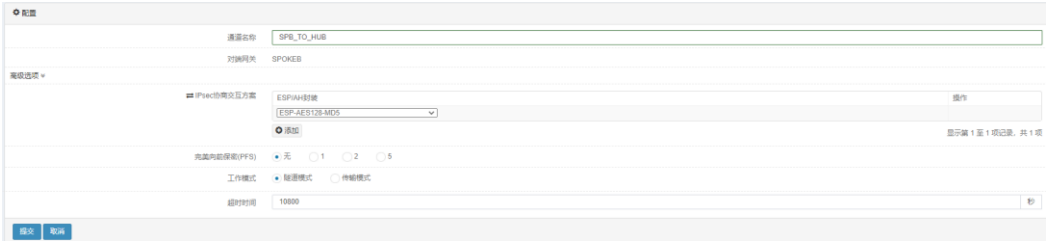
SPOKEB 配置步骤：

7. 进入**网络>VPN>IPsec>IPsec**，点击**新建，**如下图：



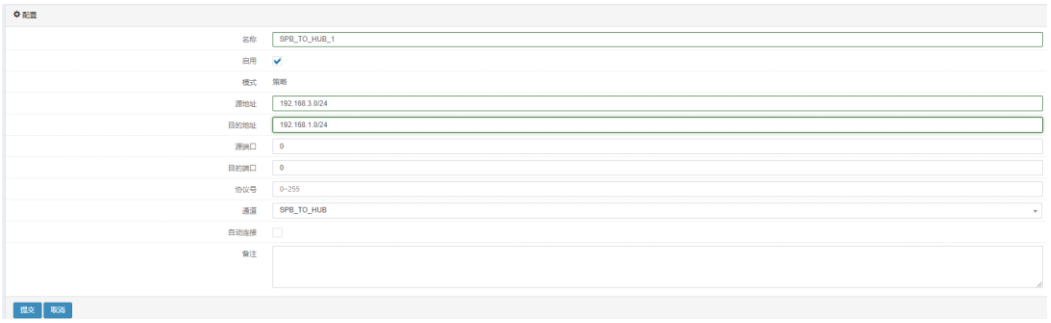
点击**提交**完成配置。

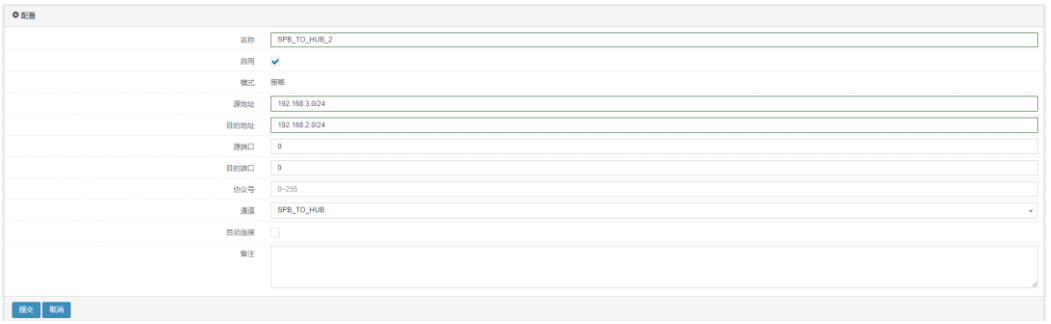
8. 进入**网络>VPN>IPsec>IPsec**，点击 新建 IPSEC 协商，如下图：



点击**提交**完成配置。

9. 进入**网络>VPN>IPsec>IPsec 策略**，建立 IPsec 策略，如下图：





分别点击**提交**完成设置。

31.5 IPSEC VPN监控与维护

31.5.1 查看SA是否建立

点击**网络>VPN>IPsec>监视器**，如下图：

31.5.2 删除建立的SA

点击 删除两个协商的 SA。

点击 查看 IPSEC 阶段 SA 的详细信息。

31.6 常见故障分析

31.6.1 故障现象：不能建立隧道

	安全联盟协商不成功，不能建立SA，在命令show crypto ipsec sa中看不到相关信息
	1）查看两端设备的相应的安全策略配置是否对称 2）IKE协商的协商策略、验证密钥是否一致 3）IPSEC协商的协商策略是否一致
	1）如果安全策略配置不对称，则修改成对称 2）IKE协商或者IPSEC协商的协商策略不一致，则修改成一致

32 第32章 SSL 远程接入

32.1 技术简介

从概念角度来说，SSL VPN 即指采用 SSL （Security Socket Layer）协议来实现远程接入的一种新型 VPN 技术。SSL 协议是网景公司提出的安全协议，它包括：服务器认证、客户认证（可选）、SSL 链路上的数据完整性和 SSL 链路上的数据保密性。对于内、外部应用来说，使用 SSL 可实现与传统 IPSec VPN 一致的真实性、完整性和保密性。

目前 SSL 协议被广泛应用于各种基于浏览器或 TCP 协议的应用。正因为 SSL 协议被内置于 IE 等浏览器中，使用 SSL 协议进行认证和数据加密的 SSL VPN 就可以免于安装客户端。相对于传统的 IPSEC VPN 而言，SSL VPN 具有部署简单，无客户端，维护成本低，网络适应强等特点，这两种类型的 VPN 之间的差别就类似 C/S 构架和 B/S 构架的区别。

T 系列防火墙上的 SSL VPN 分为两种工作模式:

- Web 模式。也叫做代理 Web 页面。它将来自远端浏览器的页面请求（采用 HTTPS 协议）转发给 Web 服务器，然后将服务器的响应回传给终端用户。支持 WEB 服务。
- Tunnel 模式。需要下载、运行客户端支持。客户端和防火墙设备建立 SSL 隧道后，防火墙为客户端分配 IP，客户端通过建立的虚接口直接通过 SSL 隧道连接到内部网络。该种方式可支持各种应用。

32.2 配置SSL VPN

SSL VPN 模块的配置主要包括以下几部分内容：

- 配置 SSL VPN 基本功能
- 配置 SSL VPN 用户和用户组
- 配置 SSL VPN 资源和资源组
- 配置 SSL VPN 准入控制
- 配置 SSL VPN 接口选项

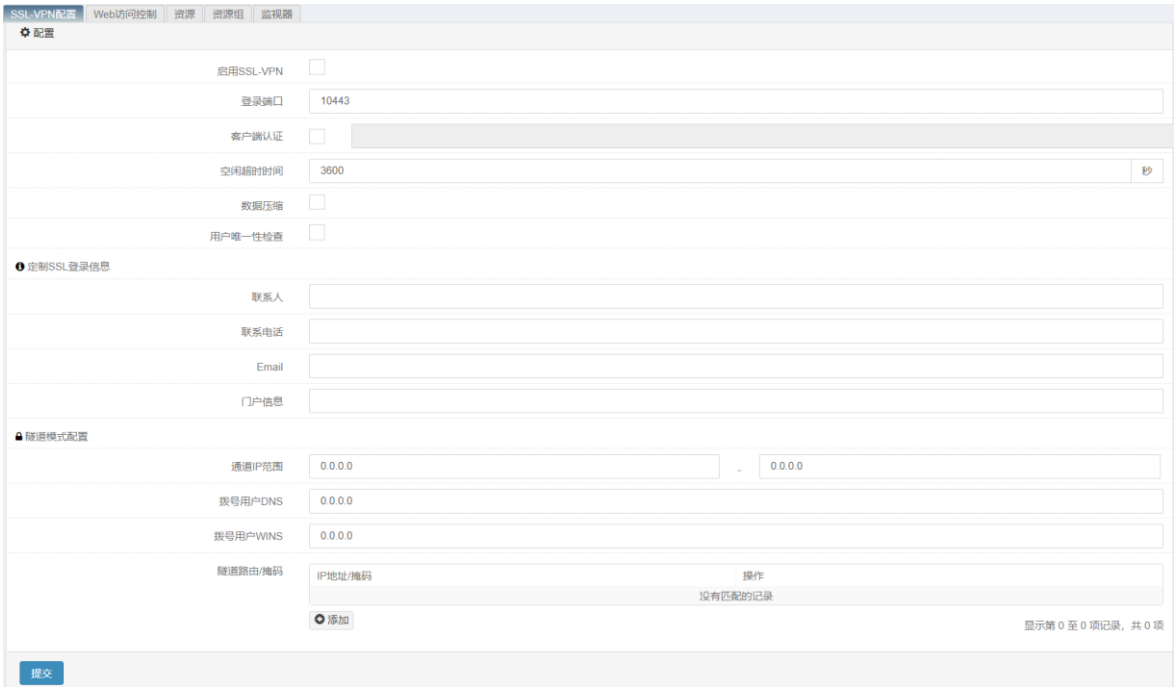
32.2.1 配置SSL VPN基本功能

1） 基本配置

SSL VPN 的基本功能包括如何启用 SSL VPN 服务，设置登录端口，用户超时时间等。

首先单击左侧功能栏 VPN→SSL 远程接入，如下图：

点击进入 SSL VPN 基本功能配置页面，如下图：



- **启用 SSL-VPN**：用以启用/关闭 SSL VPN 服务功能。
- **登录端口**：用于设置 SSL VPN 的服务端口，是客户端登录 SSL VPN 页面时采用的端口号，客户端通过此端口和 T 系列防火墙设备建立 SSL VPN 连接。默认端口为 10443。用户登录地址可表述为：“https://开启 SSL VPN 服务的端口 IP 地址:登录端口号”。
- **客户端认证**：用于开启认证客户端证书。客户端认证的 CA 证书，可以默认 CA 证书，也可以选择本地的 CA 证书。
- **空闲超时时间**：设置一段时间（秒）来控制用户超时。如果用户在登录 SSL VPN 后，在设定的时间内，没有使用 SSL VPN 传输数据，用户将自动退出。如果用户需要再次使用 SSL VPN，需要重新登录。
- **数据压缩**：是否启用数据压缩。
- **用户唯一性检查**：如果选定，检查是否存在已登录的同名用户，同名用户登录时会挤掉之前登陆的同名用户。

▲ **定制 SSL 登录信息**：SSL-VPN 添加 SSL 客户端页面信息定制功能，使管理员可以根据团队的需要，来定制 SSL 客户端页面。包括以下配置：

- **联系人**：联系人的信息
- **联系电话**：联系人的电话

- **Email：**联系人的 Email。
- **门户信息：**用户自定义的 SSLVPN 门户信息。用户配置门户信息将显示在用户登录后的 SSLVPN PORTAL 页面上。

▲ **隧道模式配置**在用户使用 SSLVPN 隧道模式时才会生效。包括以下配置：

- 通道 IP 范围：指客户端通过隧道方式连接后分配到的 IP 地址范围。指定为 SSL VPN 隧道模式客户端分配的 IP 地址范围，输入 IP 地址范围的起始和结束地址即可。
- **拨号用户 DNS：**指定客户端通过隧道方式连接后使用的域名服务器，如果访问的资源均通过 IP 地址直接访问则可不填。
- **拨号用户 WINS：**指定客户端使用的 WINS 服务器。
- **隧道路由/掩码：**配置隧道模式用户可以访问的私有网络，指客户端通过隧道方式连接后，在客户端 PC 上设定的访问路由，可配置多条。

2） 注意事项

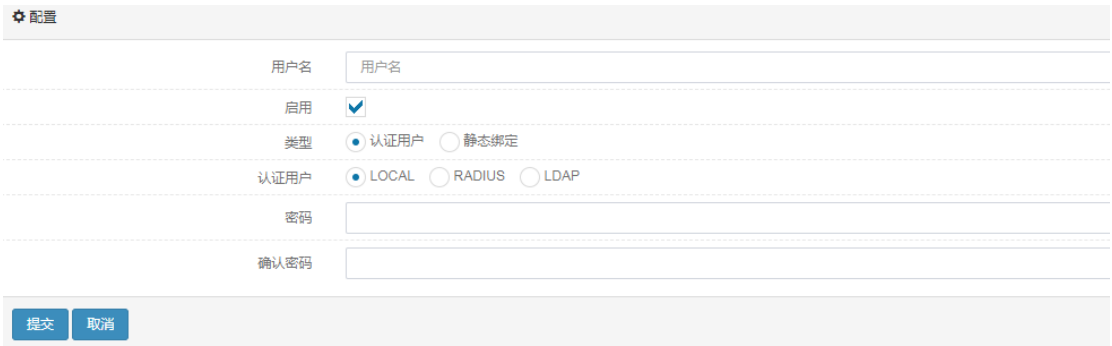
➢ 在配置登录端口时，不能与 T 系列防火墙其他服务所占用的端口冲突。

32.2.2 配置SSL VPN用户和用户组

远程用户在使用 SSL VPN 服务访问网络资源之前，需要通过 HTTPS 方式进行身份认证。用户需要使用指定的用户账户和用户组登录，才能成功认证。下面讲述了如何为远程用户配置 SSL VPN 登录用户和用户组。

1） 配置用户

配置用户账户：进入对象→用户对象→用户，点击“新建”。如下图：



配置过程：

1) 输入远程用户的用户名（如 user_1）；

2) 选中启用；

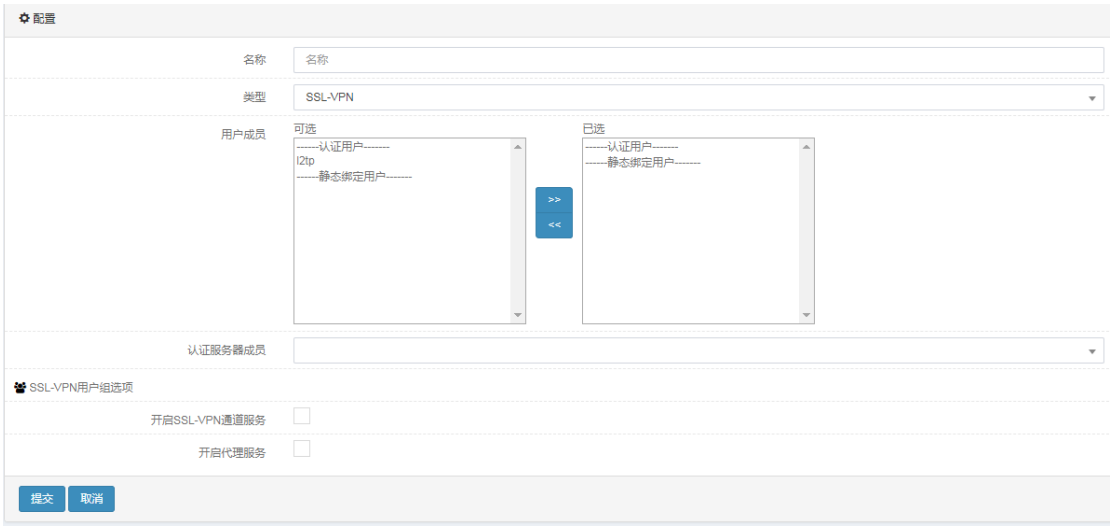
3) 如果使用本地密码验证，勾选 LOCAL，并输入密码和确认密码；如果使用 RADIUS 认证，勾选 RADIUS，并选择指定的 RADIUS 服务器；如果使用 LDAP 认证，勾选 LDAP，并选择指定的 LDAP 服务器；

4) 提交；

5) 重复以上过程，可以添加多个远程用户。

2） 配置用户组

配置 SSL VPN 用户组：进入对象→用户对象→用户组， 点击“新建”。如下图：



配置过程：

1) 输入用户组名（如 employee_group）；

2) 选择类型为：SSL- VPN；

3) 要向该用户组中加入用户。从“可选”列表中选择用户，然后单击右箭头或双击用户名称，将该用户添加到组员列表中；

4) 选择开启 SSL VPN 通道服务，使该组用户可以使用 SSL VPN 隧道模式（可选）；

5) 选择开启代理服务，使该组用户可以使用 Web 代理模式（可选）；

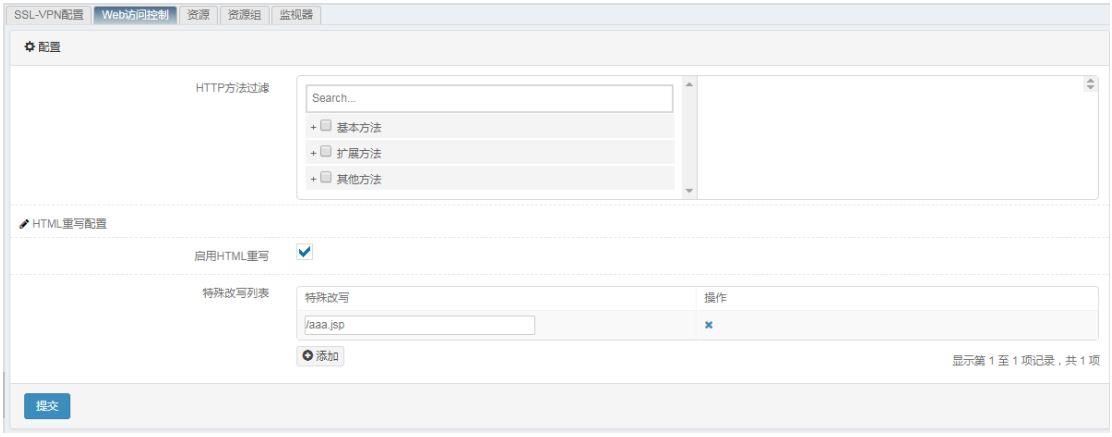
6) 提交。

32.2.3 配置SSL VPN Web访问配置

SSLVPN Web 访问配置功能，包括：配置要过滤的 HTTP 方法和启用 HTML 重写功能。

1） 配置 Web 访问配置

配置 SSLVPN Web 访问，进入 VPN>SSL 远程接入>Web 访问配置。如下图：



1) 配置需要过滤的 HTTP 方法：从 HTTP 方法列表中选择要过滤的方法，然后单击左键头选中添加方法名使其到过滤列表中。如要取消过滤只需从右侧已过滤 HTTP 方法列表中点击删除按钮，删掉要取消过滤的方法。

2) 启用 HTML 重写功能：选中即启用 HTML 重写功能。

3) 特殊改写功能：对页面中包含非标准 HTML 元素中的链接进行改写。

2） 注意事项

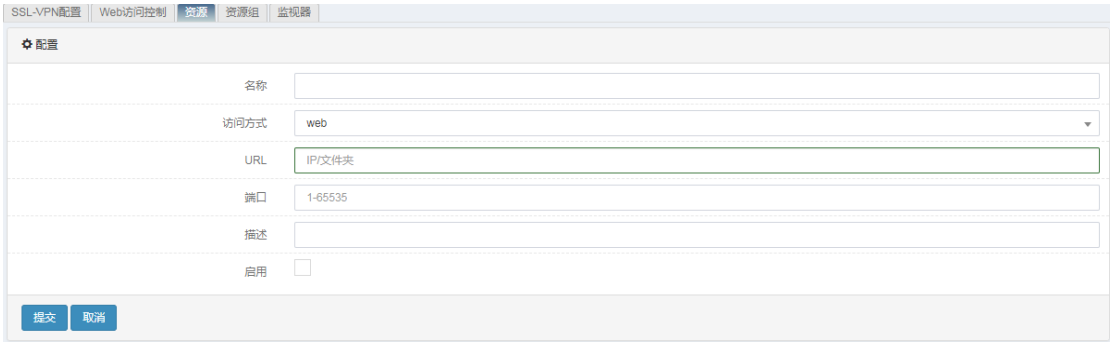
HTTP 方法过滤功能提供三类可以过滤的方法：基本方法、扩展方法和其他方法，如需要过滤的方法在基本方法和扩展方法中未给出，可以通过选择其他方法中的”other”进行过滤。

32.2.4 配置SSL VPN资源和资源组

T 系列防火墙 V4.1 的 SSL VPN 支持根据用户组配置资源组，资源组是将现有的资源进行按类别组合，可以根据用户权限级别来对 WEB 访问资源进行分类。该功能可从设备上对客户端可访问的资源方便的进行控制，随时可将新建的资源加入资源组或从资源组删除已选资源，可以限定或取消限定访问某个资源组的用户组，还可以选择是否允许违反客户端安全检查的客户端对资源的访问等等。

1） 配置可用的资源

配置或新建资源：进入 VPN →SSL 远程接入→资源（页面上方标签），点击“新建”。如下图：



配置过程：

1) 输入资源名称；

2) 选择访问方式：如该资源为 WEB Server，则采用 WEB 方式；

3) 输入该资源的 IP 地址，如该资源采用 WEB 方式访问，则可输入域名；

4) 输入该资源所提供服务的对应端口号，如 WEB Server 一般为 80；

5) 输入资源描述（可选）；

6) 点击“启用”，以激活该资源；

7) 点击“提交”；

8) 重复以上过程，可以添加多个资源。

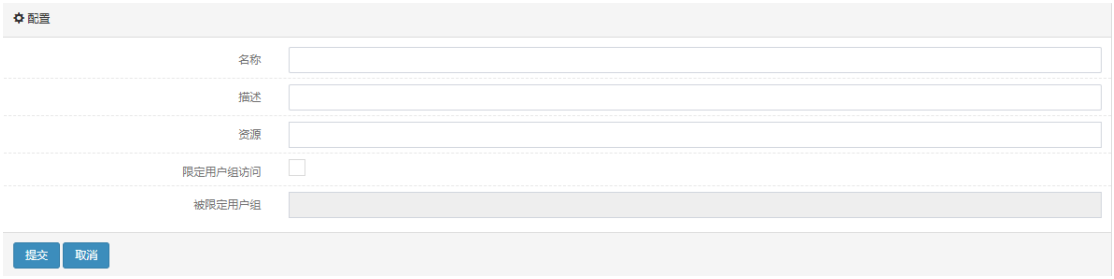
2） 注意事项

➢ 代理资源不支持域名；

3） 配置 SSL VPN 的资源组

配置或新建资源：进入 VPN→SSL 远程接入→资源组（页面上方标签），点击“新建”。

如下图：



配置过程：

1) 输入资源组名称；

2) 输入资源组描述（可选）；

3) 在资源列表栏中选择指定资源；

4) 如需要限定该资源组仅供某个用户组使用，则点击开启“限定用户组访问列表”功能（可选）；

5) 点击“提交”；

6) 重复以上过程，可以添加多个资源组。

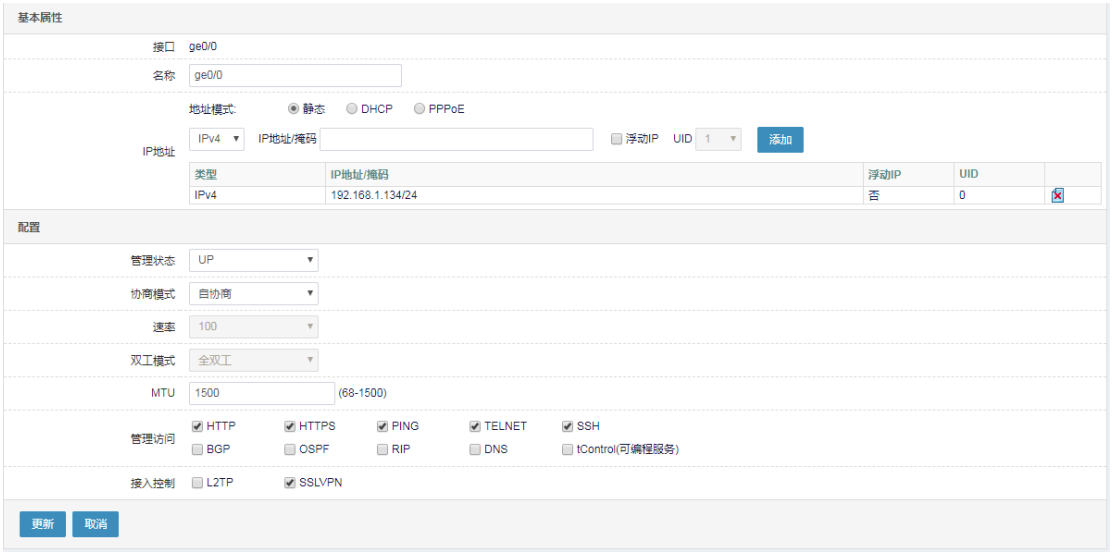
通过新建、编辑或删除资源组，可以很方便的将 SSL VPN 用户组与特定的内部资源联系起来。

32.2.5 配置SSL VPN接口选项

1） 配置 SSL VPN 选项

必须在指定的 SSL VPN 接入接口上启用 SSL VPN 选项，才可在该接口上进行 SSL VPN 认证。该接口一般为防火墙的外网口，同时该接口必须配置正确的 IP 地址。

配置接口 SSL VPN 选项：进入网络设置→接口， 点击“编辑”按钮。如下图：



2） 注意事项

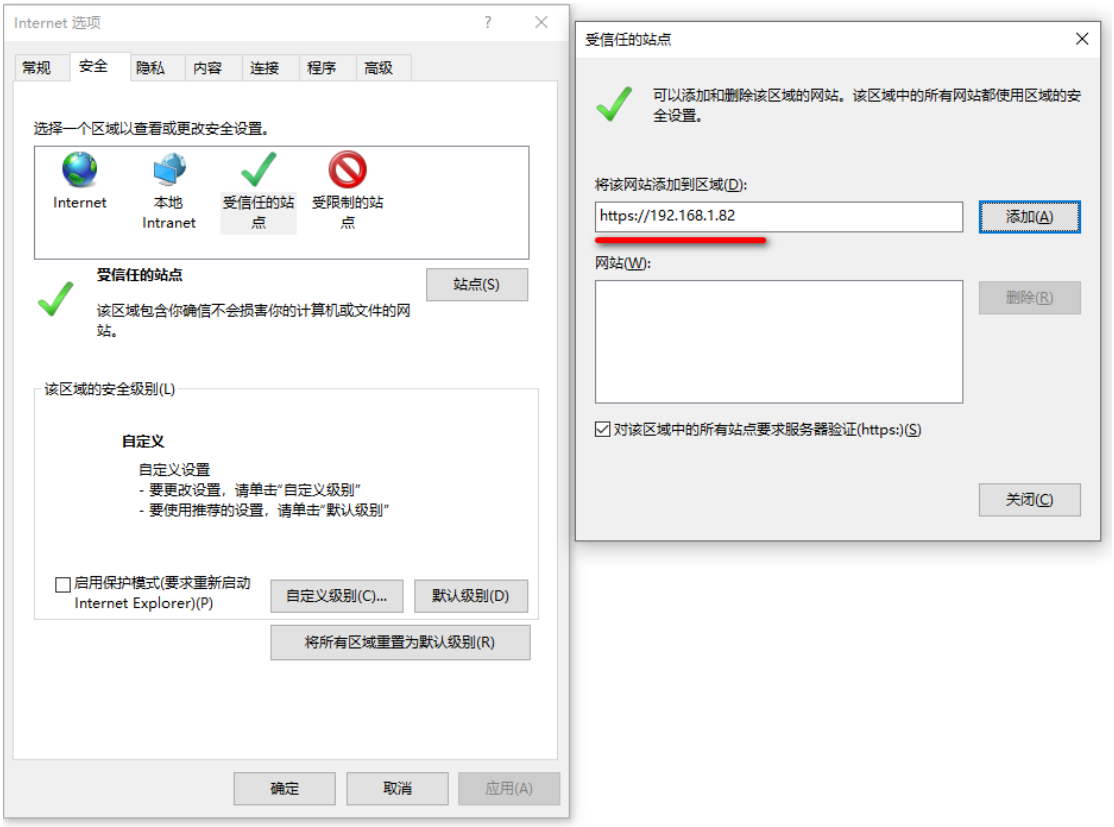
- 默认情况下，所有接口的 SSL VPN 选项默认没有启用，要使用 SSL VPN 功能，需要在接口上启用该选项。
- 隧道模式，需要配置安全策略放通隧道 IP 段到内网的流量

32.3 SSL VPN登录

32.3.1 WEB模式

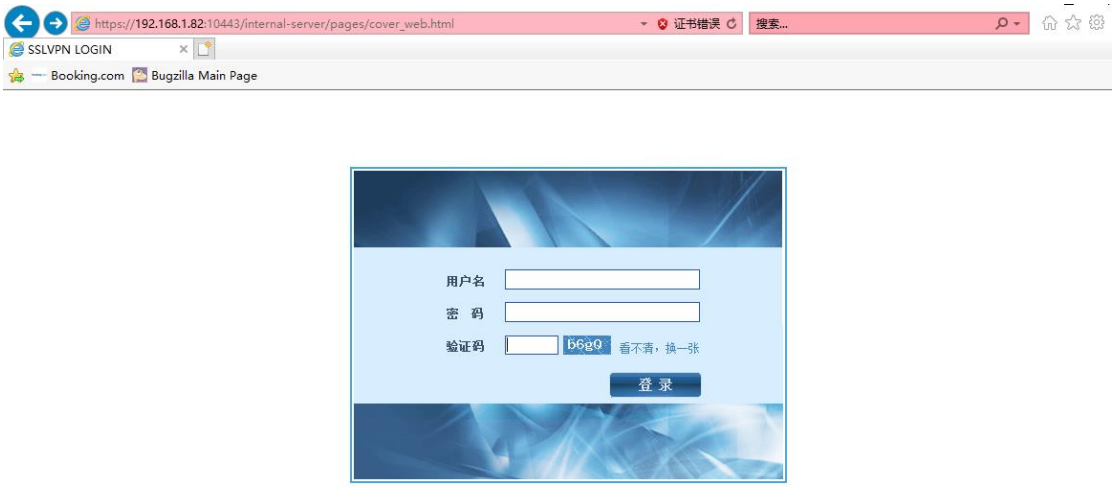
1） 打开 SSL VPN 登录页面

使用网页浏览器打开如下链接：https://开启 SSL VPN 服务的端口 IP 地址:登录端口号 。建议使用 IE8 及以上浏览器，对经常使用 VPN 业务的用户建议将该页面添加至收藏夹。在登录之前，建议将该地址添加至 IE 浏览器的“受信任的站点”列表，如下图红线处所示：



如果 sslvpn 配置中开启了客户端认证，记得给登录 sslvpn 的 pc 安装客户端证书。

SSL VPN 登录界面如下图所示：



1） 输入用户名和密码

在登录页面的“用户”和“密码”输入框中依次输入网络管理员分配的相应用户名和密码，以及验证码。需要注意的是，对于存在设备本地的用户，用户名处填写的信息为：用户名，对于需要 RADIUS 或者 LDAP 服务器认证的用户，用户名处填写的信息为：用户名@用户组。

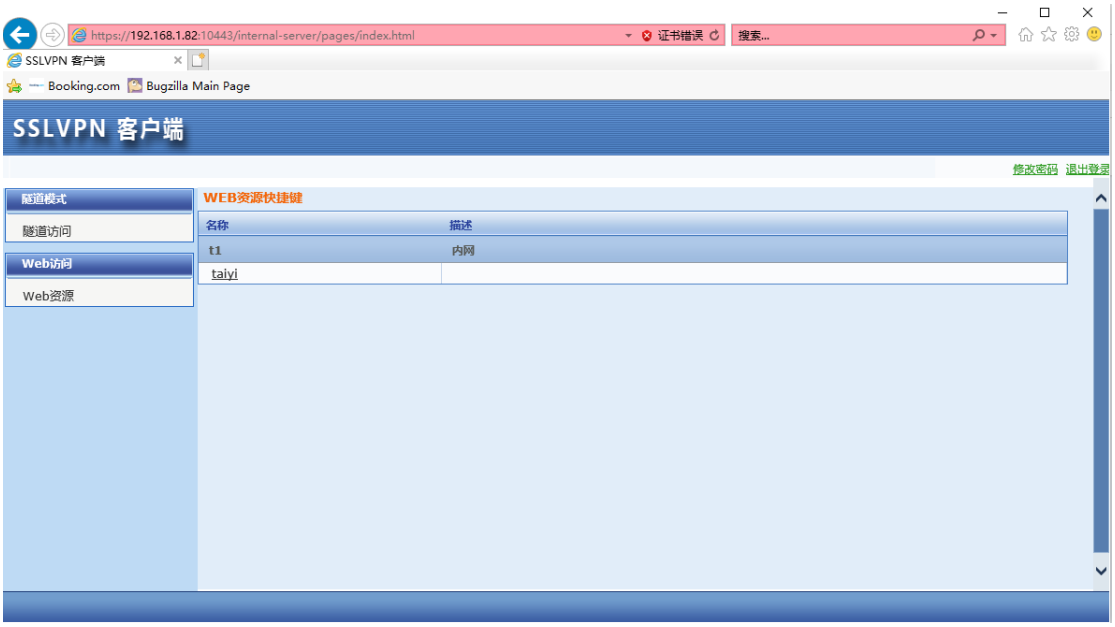
3） 成功登录

点击“登录”按钮，在输入用户名和密码正确且客户端 PC 没有违法准入控制策略的情况下，登录成功，用户会看到如下页面

。

点击左侧的“WEB 资源”按钮，则进入 WEB 资源页面，该页面列出了登录用户可访

问的 WEB 资源。



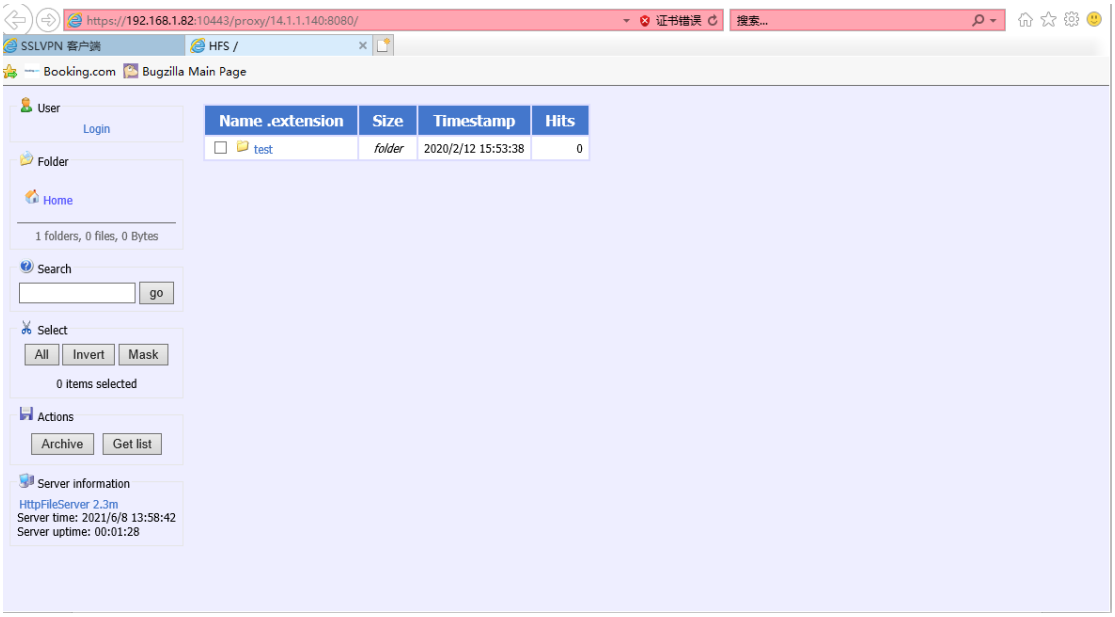
使用隧道模式访问的用户，第一次访问时需手工安装一个瘦客户端，隧道模式的使用方式下一章节做专门介绍。

4） 访问内网资源

成功登陆后，用户可直接点击“WEB 资源”下的链接跳转至内部服务器。

- **访问 Web 资源**

直接点击 web 资源列表中的链接即可：



如管理员配置该用户组允许进行隧道访问，则可点击“隧道模式”，转到隧道模式相关页面。

5） 注意事项

- 在登录页面中，存在设备本地的用户，用户名中填写的信息为“*用户名*”，需要到 RADIUS 或者 LDAP 服务器认证的用户，用户名中填写的信息为“*用户名@组名*”，其中用户名和组名分别为在 SSL VPN 配置阶段所创建的 SSL VPN 用户和 SSL VPN 用户组，详见“配置 SSL VPN 用户和用户组”部分内容。

32.3.2 Tunnel模式

由于很多业务模式较为复杂，无法以单纯的 WEB 方式或 TCP 单连接方式进行，因此建议 SSL VPN 采用隧道方式运行。在 WEB 登录成功页面中，可下载 SSL VPN 瘦客户端以支持 Tunnel 模式登录。

瘦客户端(Thin Client)：指无需用户配置与管理的客户端，它通过一些协议和服务器通信，进而接入局域网。

1） 客户端的安装

在 WEB 的登录成功页面中，点击“安装”可下载一个 SSL VPN 瘦客户端。

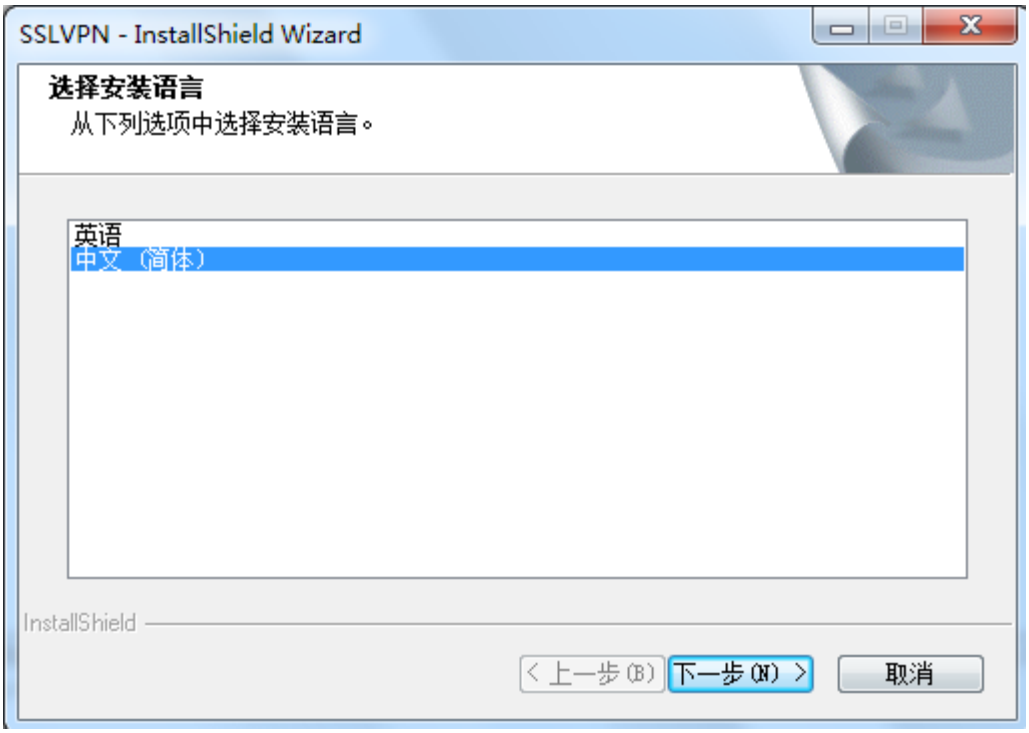
第二行的“**修改**”可以简化 sslvpn 登录时使用操作。

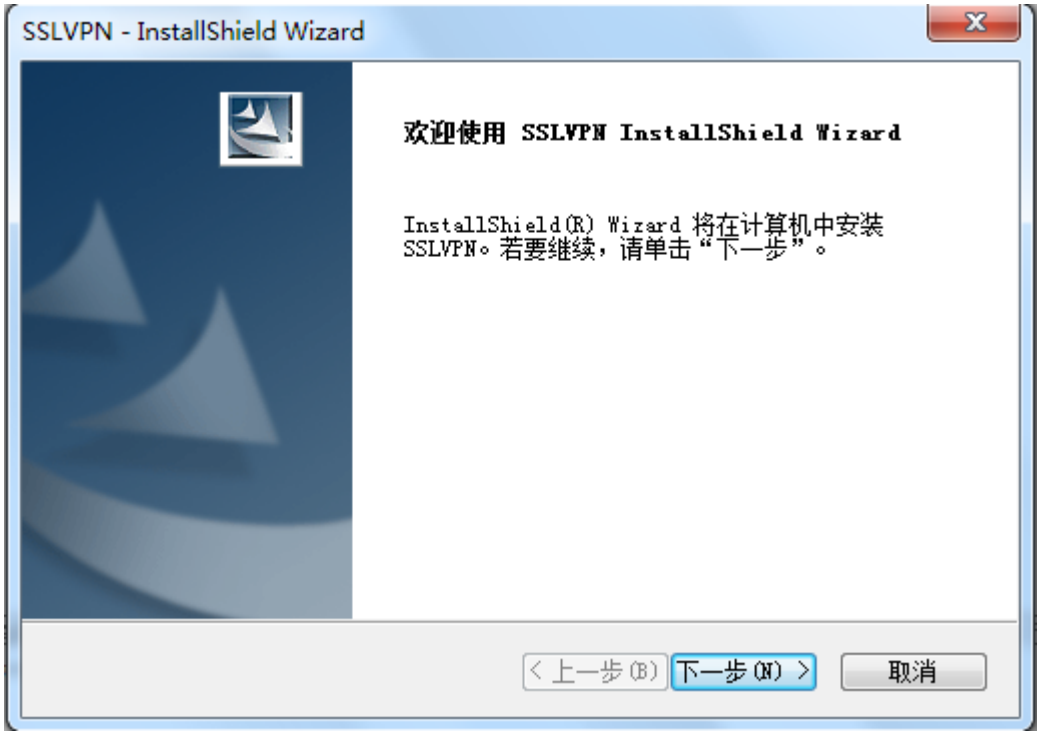
2） 安装客户端

点击“安装”后浏览器会弹出文件下载提示，如下图：

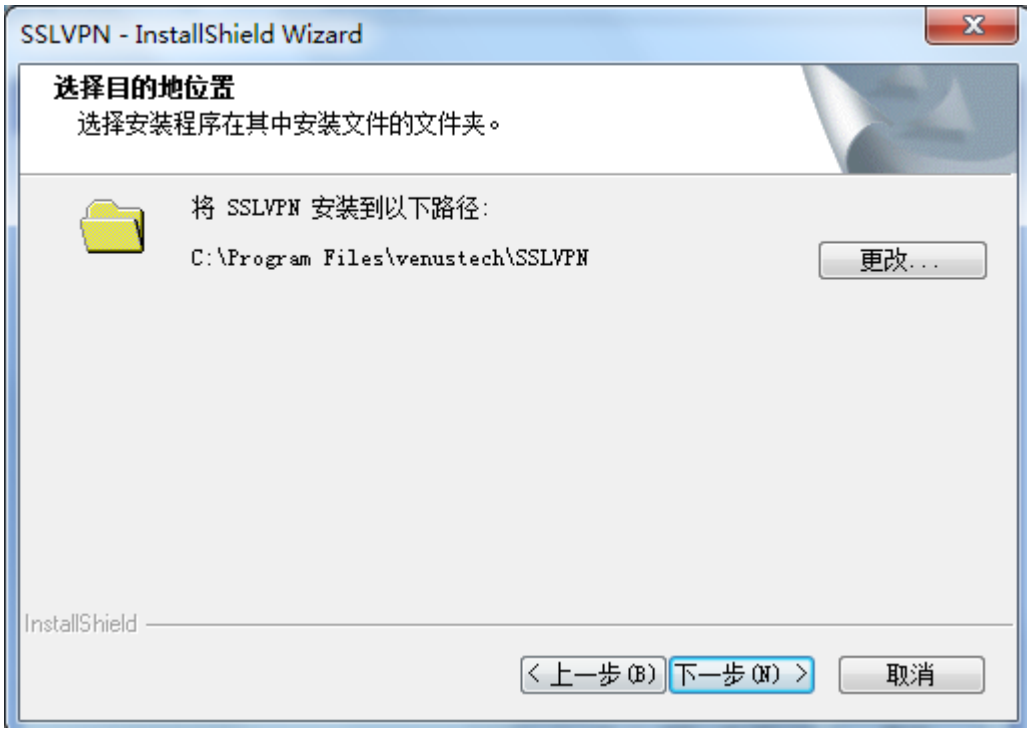
1) 选择“保存”，将 SSLVPN_Client.exe 文件下载至本机，然后双击运行该程序。某些浏览器由于捆绑了下载工具（如迅雷、FlashGet），也可用这些下载工具将 SSLVPN_Client.exe 文件下载至本地以管理员方式运行。

2) 选择运行或双击该文件后，此时会出现安装向导界面，如下图所示。选择相应的语言，“下一步”。

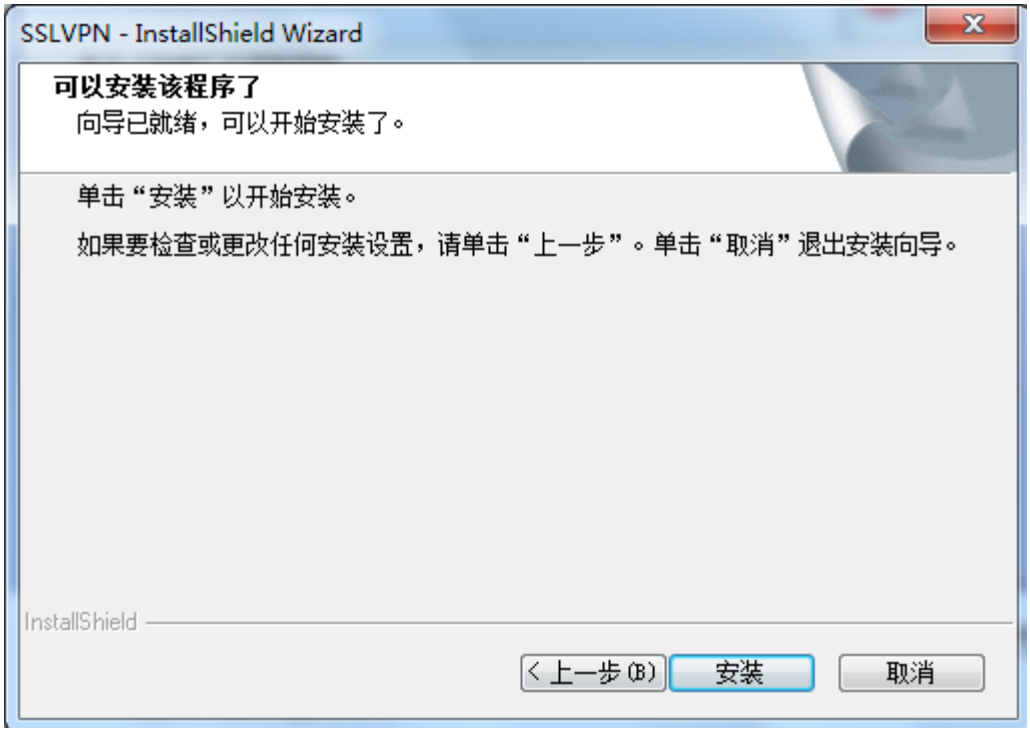




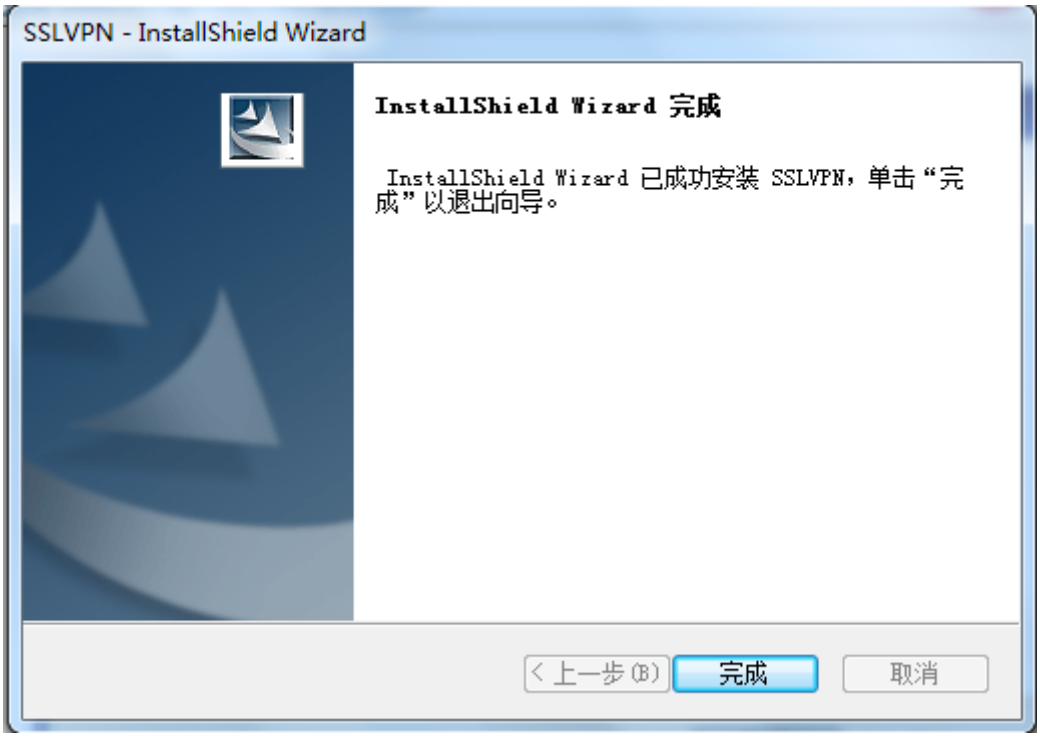
3) 此界面会提示用户选择该瘦客户端的安装路径。用户可自行选择安装目录，也可直接采用默认设置。选择好安装目录后，点击下一步。



4) 此界面提示用户安装已经就绪，点击“安装”。



5) 此时安装程序会自动进行相关设置，当程序安装完成后，会出现如下图所示界面。点击“完成”，此时 SSL VPN 瘦客户端即安装完毕。



3） Tunnel 模式登录

瘦客户端安装完成后，返回到 WEB 认证界面，点击“连接”，如下图所示。

点击“连接”后，会出现一个一闪而过的连接信息之后就自动缩小至系统右下角的图标栏内，双击这个小图标可以看到具体的隧道连接信息如下。

此时，即可开启相关软件访问 VPN 内的相关资源。

4） 注意事项

- 隧道客户端安装时，需要注意，只安装 sslvpn 的虚拟网卡，其他选择停止安装，否则有可能会有硬件上的冲突等问题，甚至出现蓝屏；
- 任何终端用户，当完成第一次的 SSL VPN 瘦客户端安装后，下次进行 SSL VPN 连接时无需重新下载，直接点击 Tunnel 模式下的“连接”即可。即，WEB 模式

登录之后直接点击“连接”，即完成了 SSL VPN 隧道方式的连接，可正常开展相关业务。

- 建议保持最初的登录页面，当需要断开 VPN 时，点击退出登录，即可完成 SSL VPN 的断开和注销工作，同时瘦客户端也会自动断开连接。
- 隧道模式一连接就断开，需要查看 pc 的服务中 DHCP 服务是否启用，所有需要使用虚拟网卡的功能都需要 pc 开启此服务；
- 隧道模式正常连接后，仍不能访问预期地址，cmd 下查看路由信息 route print，是否已经存在访问预期地址的完全匹配的一条默认路由，导致访问预期地址不走隧道路由；解决方法是禁用重新启用 pc 本地网卡，使旧的路由信息清除掉，或者手动删除该条路由信息 route delete 预期地址，确保访问预期地址走隧道路由；
- 隧道连接下发 dns 服务器，客户端有时是无法使用下发的 dns 访问，与 dns 本身的机制有关；
- 在 win2000 上面使用隧道模式如果不通，查看一下路由表的默认网关的 metric 值，如果都是 1，需要手动修改使本地网关的 metric 值大一些，再连接隧道模式使之能通。
- 对于 Vista 系统，安装控件及瘦客户端时需要关闭账户控制 UAC 功能。隧道客户端安装时，出现如图所示，无法安装时：

是由于网络原因导致安装包不完整就开始安装了，需要重新下载完整的客户端安装包。

- 对于 Win 7 或者 Win2008 操作系统，需要右键以管理员身份运行打开 ie 浏览器之后才能正常连接隧道进行访问；

- 使用 ie9 连接隧道时，会出现一连接页面就无法显示的问题，这是由于 ie9 老版本存在本身的问题，解决方法有两种：1、升级 ie9 补丁到编号为 KB2586448；2、采用右键打开新窗口的方法连接隧道。

32.4 SSL VPN监控与维护

32.4.1 SSL VPN监视器

SSL VPN 监视器显示所有 SSL VPN 在线的用户信息，包括用户名、用户登录 IP、隧道 IP 登录时间、空闲时间、数据流量等。此外通关 SSL VPN 监视器可以强制用户下线。

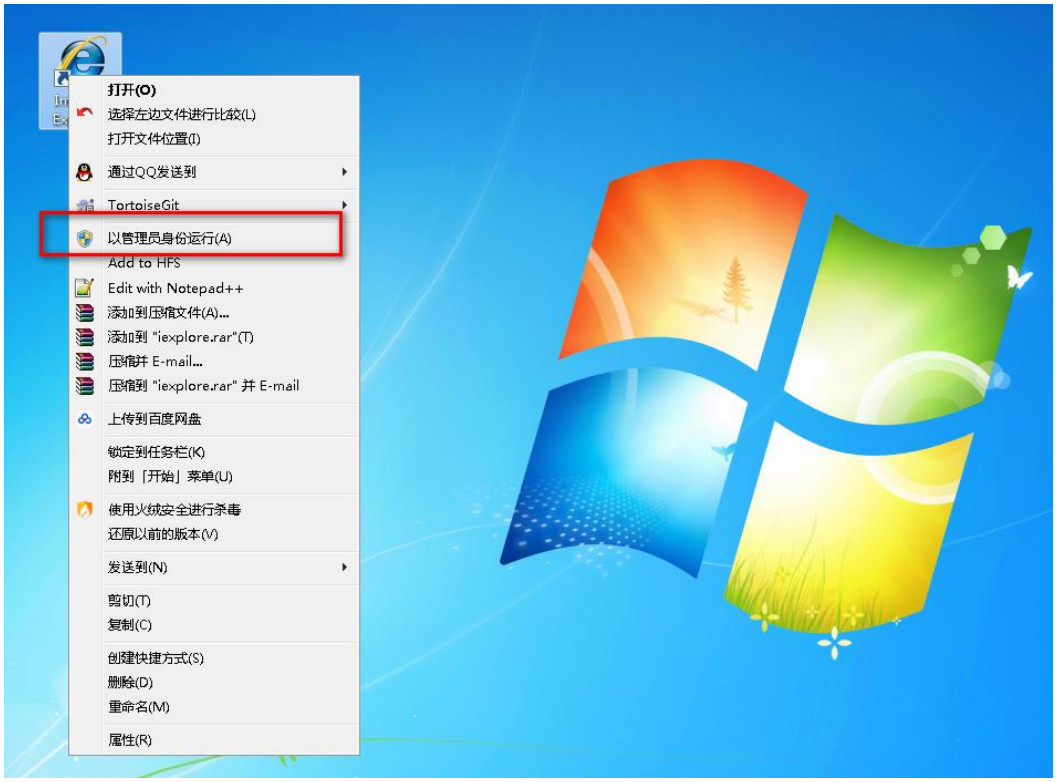
要显示在线用户 SSL VPN 用户信息，进入 VPN→SSL 远程接入→监视器。如下图：

点击用户列表最右侧的 ✖ 可以强制用户下线。

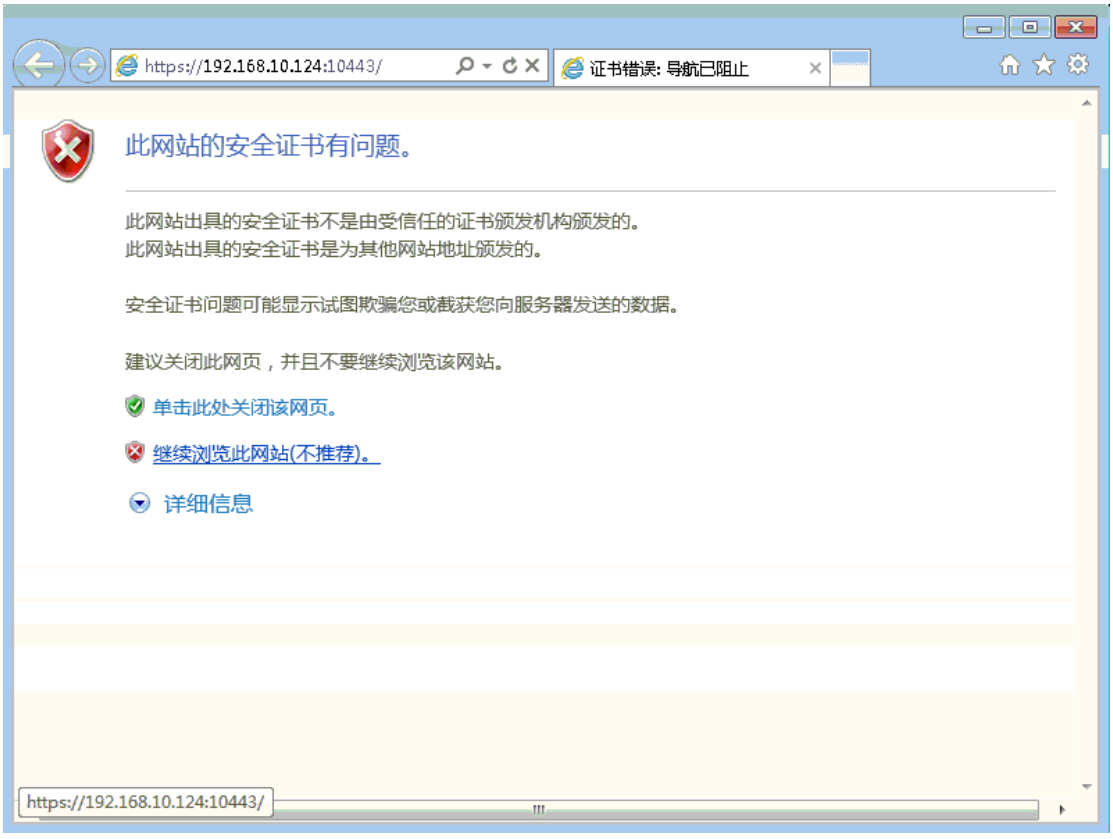
32.5 WINDOWS7 下的使用注意事项

配置过程：

1) 使用 IE 打开时选择使用管理员认证的方式打开 IE，否则当使用 SSL 隧道模式时再连接后会自动断开



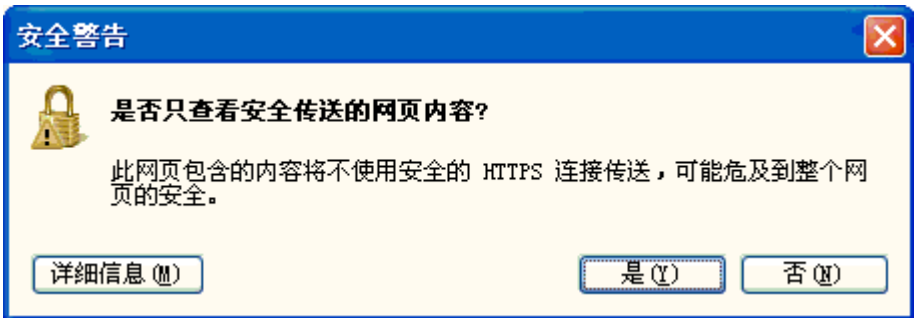
2) 输入连接的 SSL 服务的地址后选择“继续浏览此网站”



3) 输入用户名和密码、验证码并登陆

4) 选择隧道模式下载安装 SSL-VPN 客户端

5) 连接 SSL 客户端时注意事项，当使用 IE8 的用户下载并安装客户端后选择“连接”时的会弹出如下安全警告，此时选择“否”



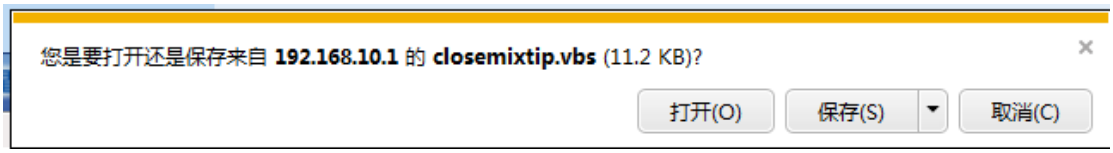
6) 出现下列选择单时选择“允许”

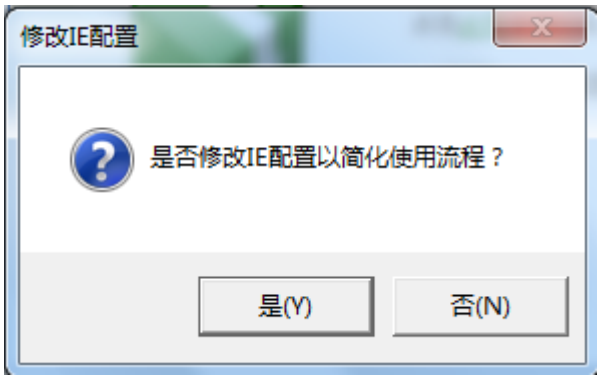
7) 出现下列图表则表明已成功连接上 SSL-VPN，可以通过 SSLVPN 隧道分到一个私网 ip，访问可达目标内的内网资源

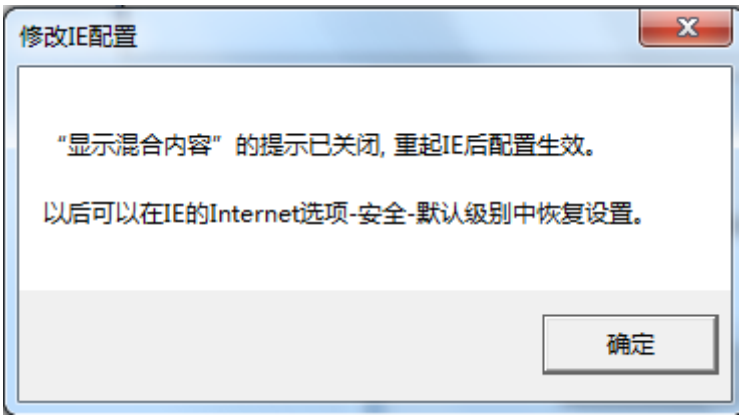
8) 对于不清楚自己 IE 版本的用户可以选择在隧道模式的界面下载一个控件用于跳过安全警告的提示，在下面的界面中选择“点击此处修改 IE 配置，简化使用流程”。

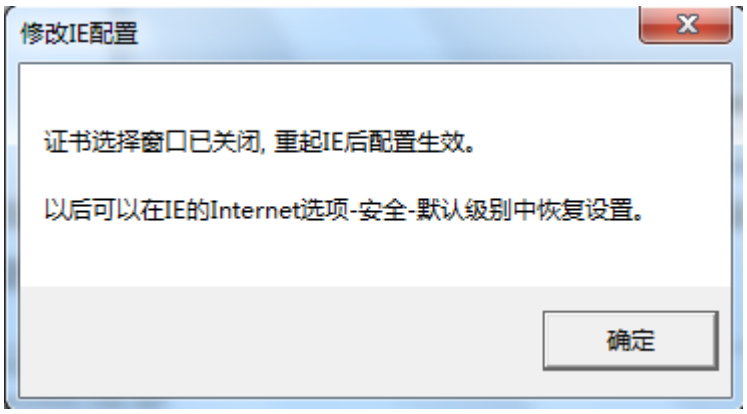
9) 点击后会下载一个名为“closemixtip.vbs”的控件，可以双击打开控件，并选择“是”

来进行控件的安装









10) 如果需要回复默认设置则在 IE 的 internet 选项中的安全中选择回复默认级别即可

32.6 SSLVPN插件、客户端与操作系统兼容性问题的FAQ

32.6.1 共性问题

现象描述 1：隧道一连就断，设备配置正确的隧道 ip 和隧道路由后，pc 成功安装了隧道客户端，结果隧道模式一连接就自动断开，

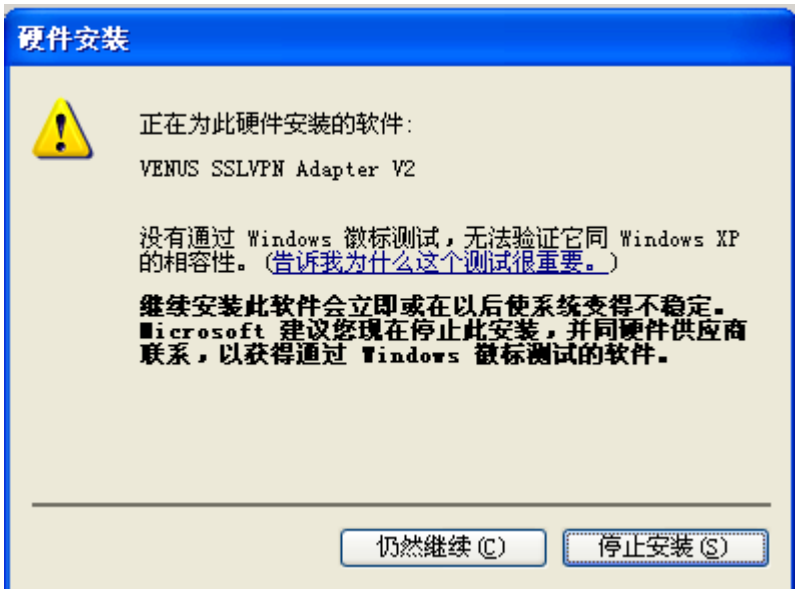
解决方法：需要查看 pc 的服务中 DHCP 服务是否启用，所有需要使用虚拟网卡的功能都需要 pc 开启此服务；

现象描述 2：隧道连接后仍无法访问，设备配置正确，隧道模式正常连接后，pc 分配到了正确的隧道 ip，但是仍不能访问预期地址

解决方法：cmd 下查看路由信息 route print，是否已经存在访问预期地址的完全匹配的一条默认路由，导致访问预期地址不走隧道路由；需要禁用重新启用 pc 本地网卡，使旧的路由信息清除掉，或者手动删除该条路由信息 route delete 预期地址，确保访问预期地址走隧道路由；

现象描述 3：隧道客户端安装出现蓝屏，pc 在安装隧道客户端时，出现了蓝屏现象

解决方法：隧道客户端安装时，需要注意，只安装 sslvpn 的虚拟网卡，只有在下图提示下选择仍然继续，如果后续还有其他类似的提示信息出现，要选择停止安装，否则有可能会有硬件上的冲突等问题，甚至出现蓝屏，



现象描述 4：隧道客户端安装出现异常信息，安装过程中出现如下图的错误信息；

解决方法：这是由于网络原因导致安装包不完整就开始安装了，需要重新下载完整的客户端安装包。

现象描述 5：隧道连接后仍无法访问，设备配置正确，隧道模式正常连接后，pc 分配到了正确的隧道 ip，但是仍不能访问预期地址，cmd 下查看 pc 的路由信息，没有干扰的静态路由信息。

解决方法：使用隧道模式如果不通，可以查看一下路由表的默认网关的 metric 值，如果都是 1，需要手动修改使原本地网关的 metric 值大一些，再连接隧道模式使之能通。

现象描述 6：隧道连接后，ftp 访问能够连接上，但是无法下载上传资源。

解决方法：请关闭操作系统的防火墙功能。

32.6.2 针对Windows 2003和Windows XP-SP3操作系统

现象描述 1：无法在 IE 上安装插件，设备配置正确，在登录之前，已经将访问地址添加至 IE 浏览器的“受信任的站点”列表，但是仍无法安装插件，一安装 IE 浏览器就崩溃。

解决方法：修改 boot.ini（隐藏在 C 盘根目录下，属性去掉只读选项），将文件中/NoExecute…改为/execute，保存后恢复 boot.ini 属性为只读。然后重新启动系统。

参照以下例子：

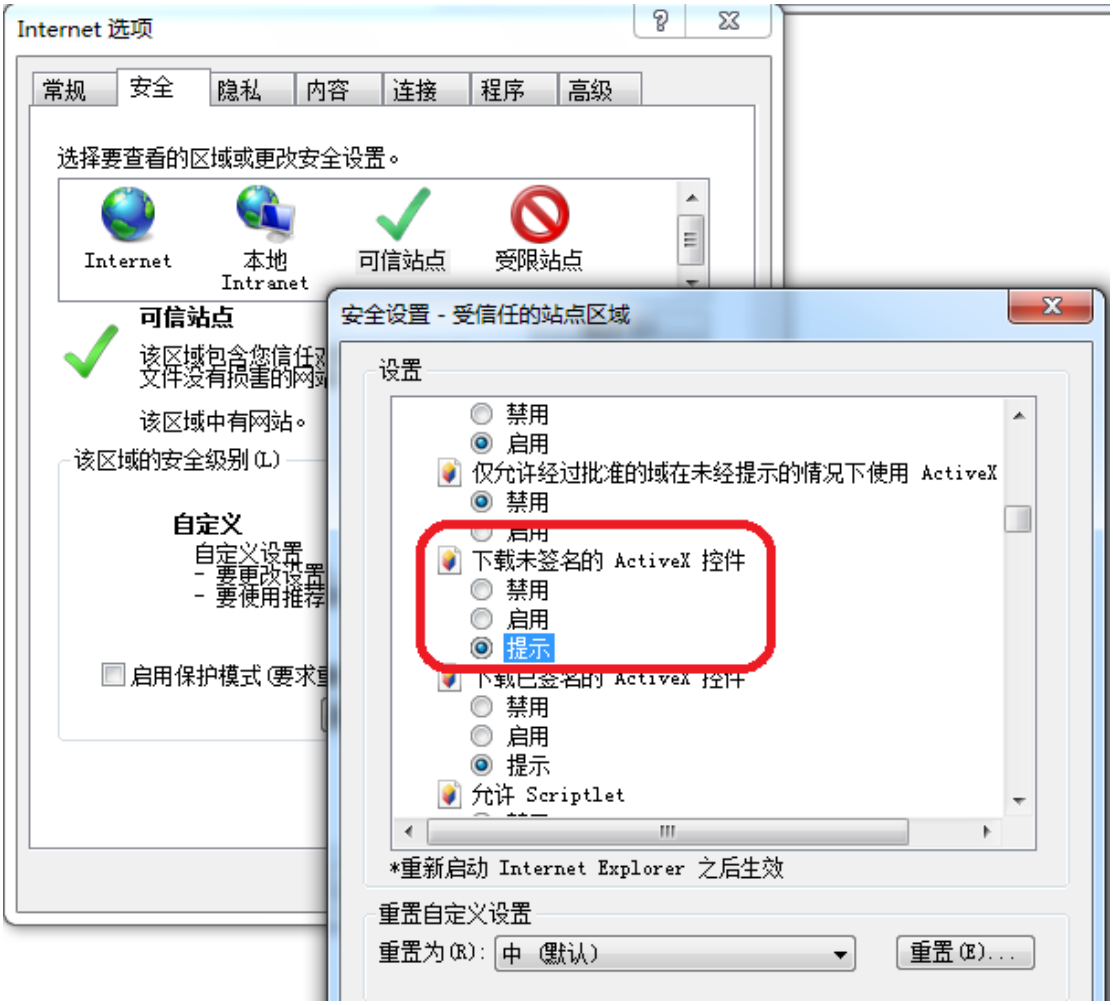
```
[boot loader]
timeout=5
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Server 2003, Standard" /fastdetect /NoExecute=OptIn
```

修改为：

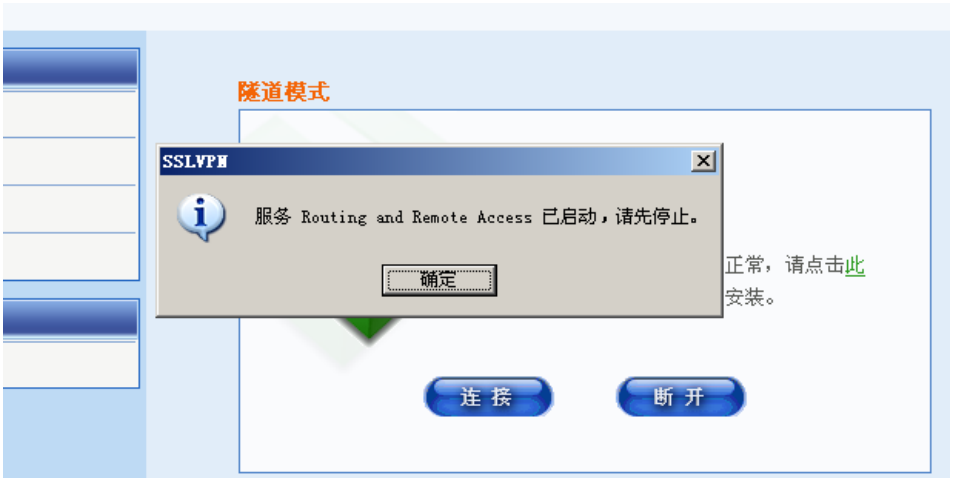
```
[boot loader]
timeout=5
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Server 2003, Standard" /fastdetect /Execute
```

现象描述 2：无法在 IE7 上安装插件，设备配置正确，但是仍无法安装插件，被浏览器认为是未识别的发行者。

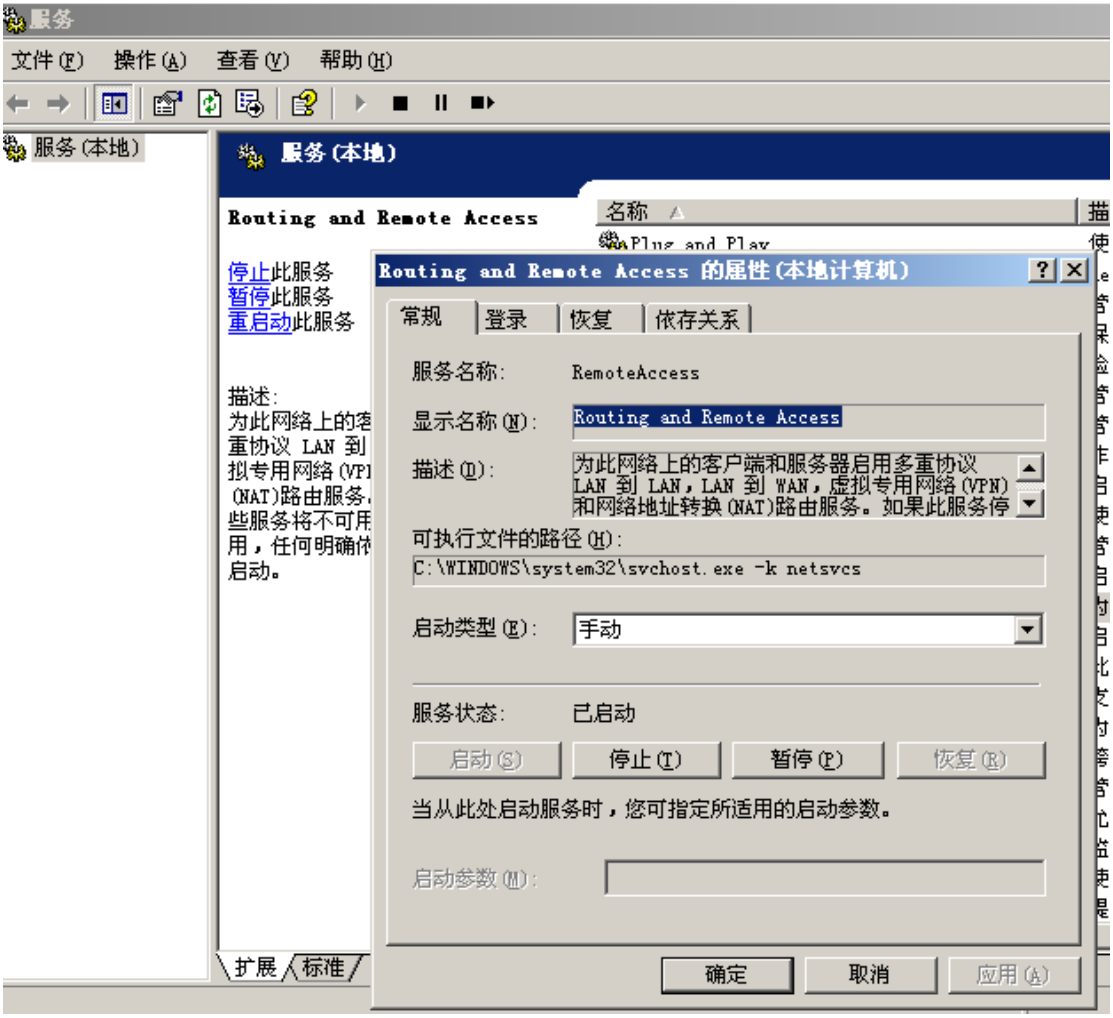
解决方法：在安全级别设定中，打开自定义级别，将“下载未签名的 ActiveX 控件”选项置为提示的状态，应用确定后打开 sslvpn 登录页面，就能够成功下载、安装、运行 ActiveX 插件了。



现象描述 3：隧道连接后弹出提示信息，设备配置正确，pc 成功安装客户端之后，连接隧道时弹出提示信息，如下图：



解决方法：到 pc 的服务中，把 Routing and Remote Access 服务停止启用，之后再次连接隧道就能正常得到 ip 进行隧道访问了。



32.6.3 针对Windows Vista、Windows 7和Windows 2008操作系统

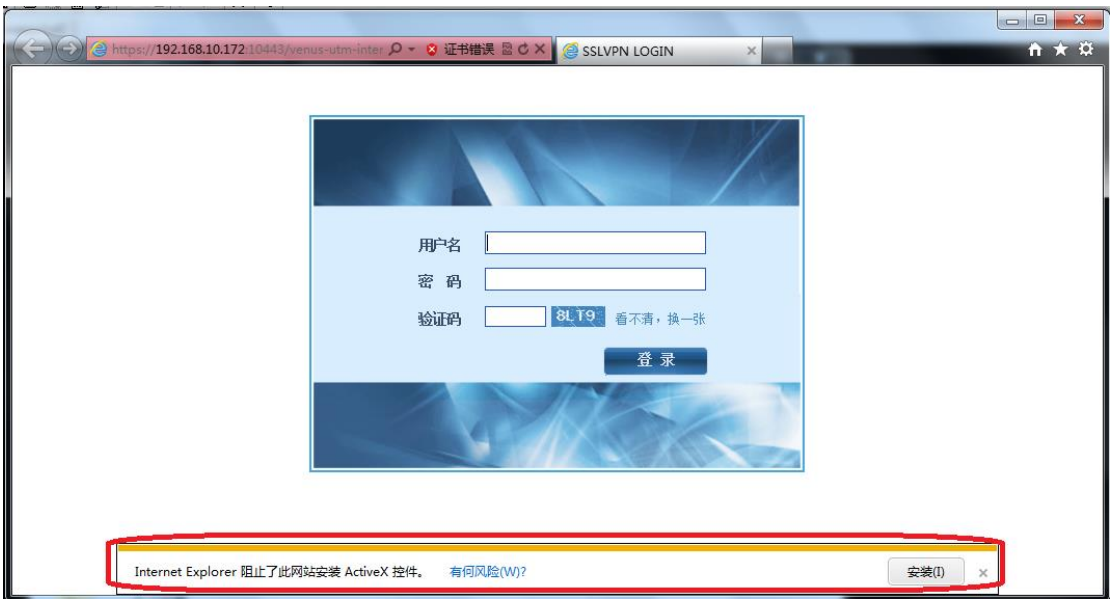
现象描述 1：无法在 IE 上安装插件，设备配置正确，但是仍无法安装插件，一安装 IE 浏览器就崩溃。

解决方法：以管理员身份执行 CloseDEP.bat 后，重新启动系统。

现象描述 2：通过 ie9 安装插件，无法安装成功

解决方法：同于使用 ie8 安装插件，必须右键以管理员身份运行 ie，

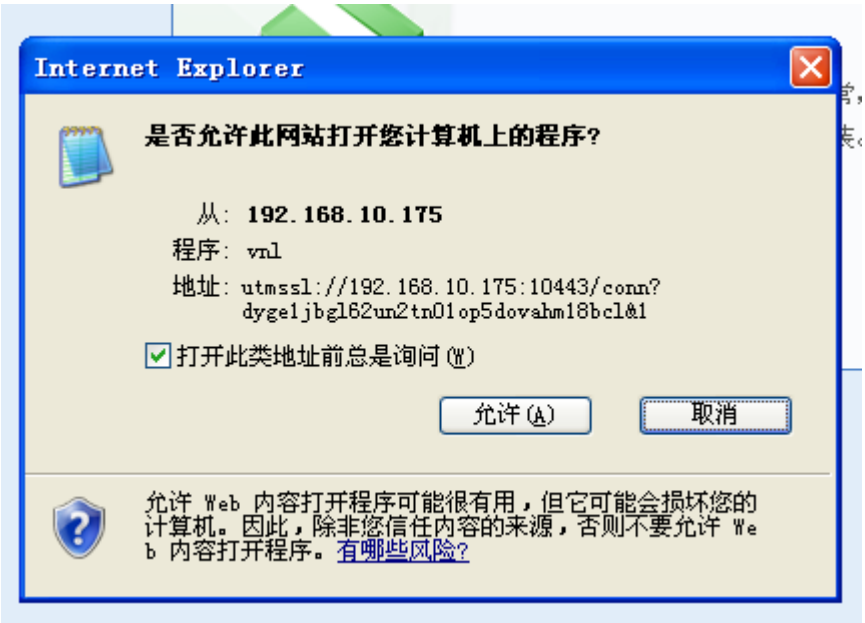
通过 ie9 安装插件过程中参考下图：



成功安装插件后，在使用的过程中当弹出以下提示时，选择“允许”来使插件能够正常监听使用：

现象描述 3：点击连接隧道后弹出安全信息，设备配置正确，pc 成功安装客户端之后，连接隧道时弹出安全信息，如下图：

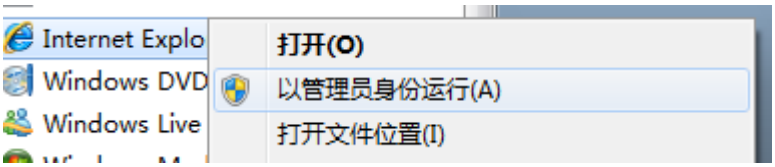
解决方法：首先**要确保以管理员的身份启动 IE**，之后在上图的安全警告下选择否，就会看到下面的提示信息：



这是再选择允许，就能够成功连接隧道了。另外可以选择点击修改 ie 配置简化使用流程的方法来避免此对话框的出现。

现象描述 4：隧道能够连接上，但是很快就断，按照上述的步骤正确连接隧道后，几秒钟隧道就自动断开了。

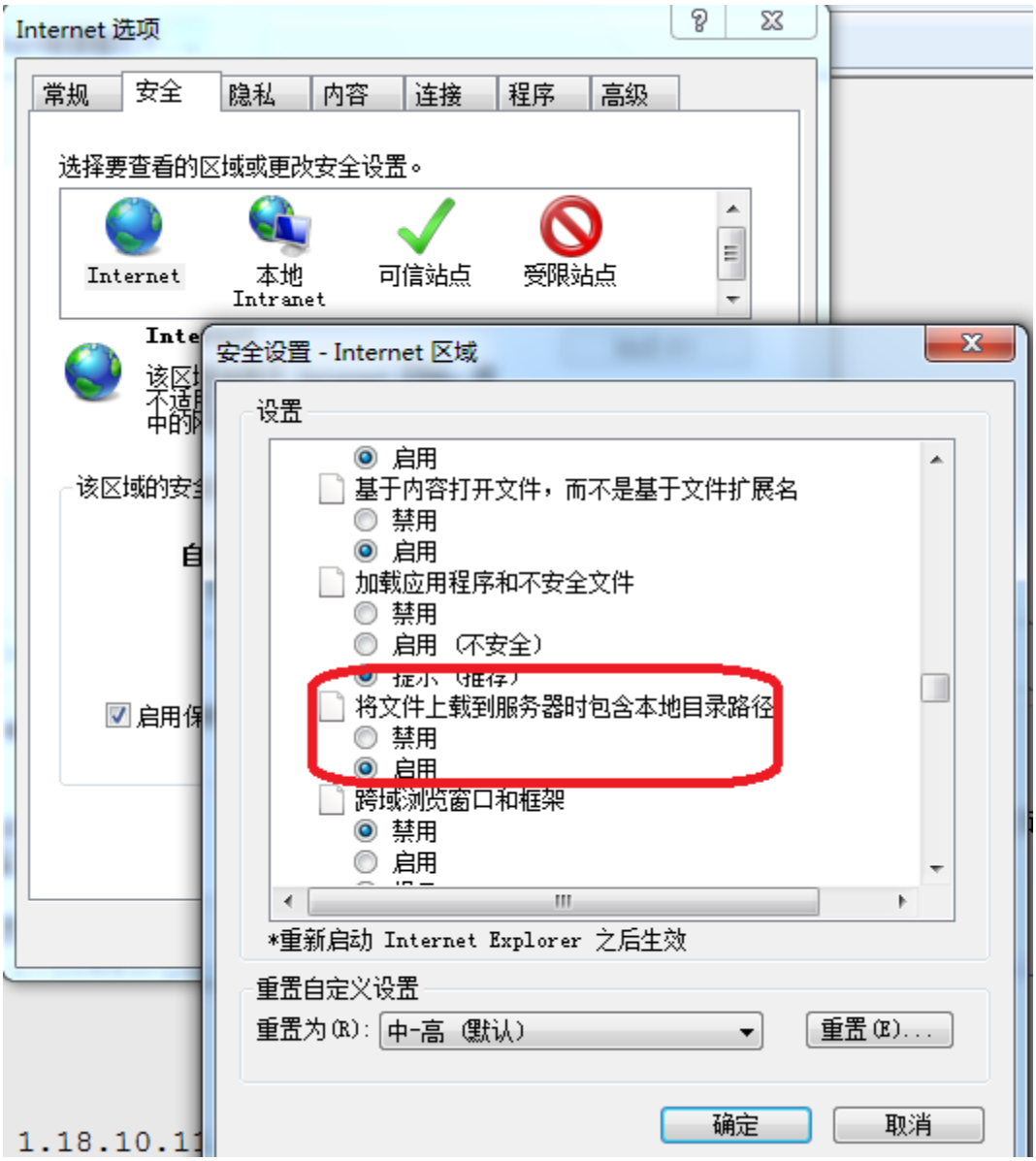
解决方法：要右键以管理员身份运行来打开 ie 浏览器，



然后登录到 sslvpn 后连接隧道，就能保持隧道不断，访问资源了。

现象描述 5：通过 ie8 或 ie9 访问 ftp 或文件共享资源时，无法上传文件，在 ftp 和文件共享都已经允许上传文件的前提下，通过 sslvpn 上传文件时，一点上传就显示该页无法显示，文件无法上传成功。

解决方法：需要将浏览器的安全级别降到中和中以下级别；如果已经将该 sslvpn 登录页面的 ip 地址加入到了可信站点中，则将可信站点的安全级别降到中和中以下级别；如果不希望降低安全级别，则请在安全级别限制中，手动将“将文件上载到服务器时包含本地目录路径”的选项置为启用状态。



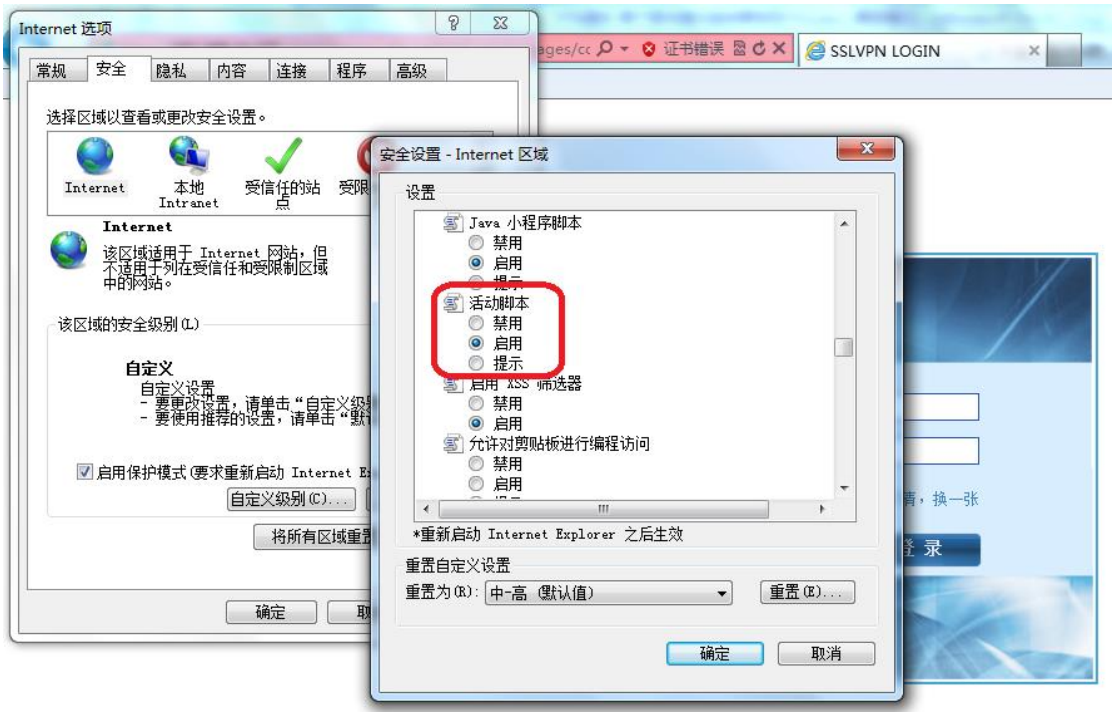
现象描述 6：通过 web 代理方式无法打开使用公司的 erp 报销系统，页面跳转不正确或跳转后无法登录进去，建立报销单时无法弹出日期选择页面。

解决方法：需要启用 html 重写，同时配置特殊改写字段为 /OA_HTML/cabo/jsps/a.jsp。（如果是其他公司特有的网页或系统无法实现页面跳转，请联系相关人员帮忙查看对应的特殊改写字段需要怎样配置）

现象描述 7：通过 ie8 或 ie9 打开 sslvpn 页面后，点击登录按钮没有反应，不提示任何信息，无法登录。

解决方法：需要将浏览器的安全级别中的自定义项目中的活动脚本设为启

用的状态：



现象描述 8：通过 ie9 连接隧道，点击连接后显示该页无法显示，无法正常连接隧道。

解决方法：这是由于 ie9 老版本存在本身的问题，解决方法有两种：1、升级 ie9 补丁到编号为 KB2586448；2、采用右键选择在新窗口中打开链接，之后就能连上隧道进行访问了：

现象描述 9：通过 ie64 位浏览器无法运行插件，无法访问 agent 资源。

解决方法：需要使用 ie32 位浏览器来进行插件的安装和使用，不支持 ie64 位浏览器使用插件功能。

33 第33章 L2TP

33.1 L2TP概述

PPP 定义了一种通过二层（L2）点对点连接传输多种协议报文的封装机制。典型情况下，一个用户通过某种接入技术（如 ISDN，ADSL 拨号等）获得一个到网络接入服务器（NAS）的二层连接，并在该连接上进行 PPP 会话。在这样的配置中，二层终节点和 PPP 会话的终节点位于同样的物理设备上（也就是说，NAS）。

L2TP（Layer Two Tunneling Protocol）是一种二层隧道协议，它扩展了 PPP 的模型，通过二层隧道将 PPP 会话的终点延伸到另一个通过分组交换网互连的不同设备上，而不是二层接入的终节点。从而将 PPP 会话从二层终结的限制中解脱出来，扩大了 PPP 的应用范围。

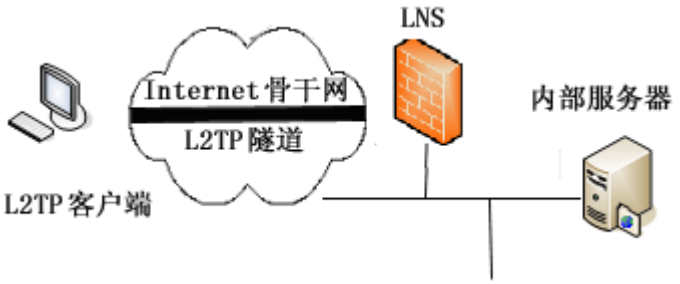
L2TP 包括 LAC 和 LNS 两种功能：

- LAC（L2TP Access Concentrator）：L2TP 访问集中器。是 L2TP 隧道的一个端点，是 L2TP 网络服务器（LNS）的对等体（PEER）。LAC 负责在一个 LNS 和一个远地系统之间转发 PPP 报文，并维护 LAC 和 LNS 之间的隧道（TUNNEL）和会话（SESSION）连接。
- LNS（L2TP Network Server）：L2TP 网络服务器。是 L2TP 隧道的一个端点，是 LAC 的对等体。负责维护与远地系统之间的 PPP 连接，为远地系统提供对内部网的访问服务。

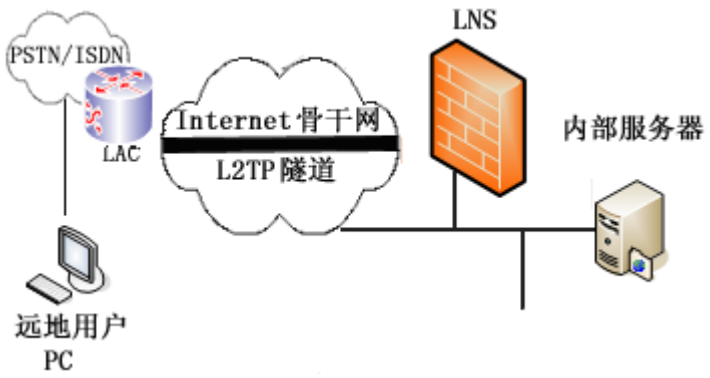
L2TP 隧道给远程拨号用户提供了连接到 VPN 网关的解决方案，拨号 VPN 又称为 VPDN(Virtual Private Dial Network)。在这种应用中，由 VPN 网关提供 LNS 功能，如果拨号用户本身支持 L2TP，则可以采用自愿隧道模式直接连接到 LNS；如果拨号用户本身不支持 L2TP，则可以通过当地 ISP 提供的 LAC 功能采用强制隧道模式连接到 LNS。

这两种连接方式的拓扑结构如下所示：

L2TP 客户端直接接入 LNS

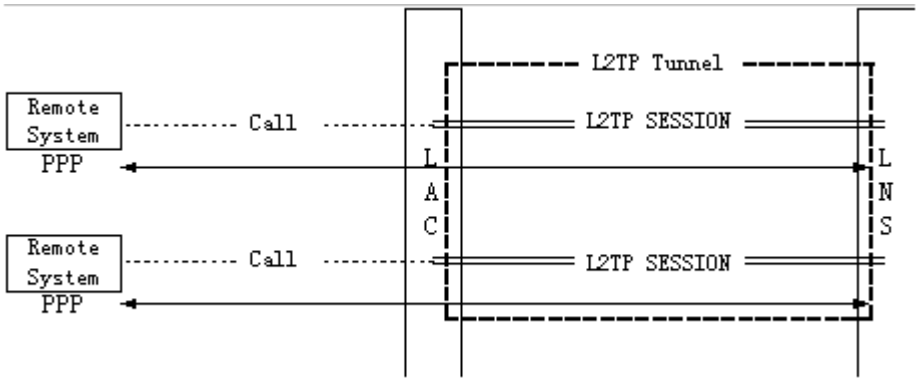


拨号用户通过 LAC 远程接入 LNS



在一个 LNS 和 LAC 对之间存在着两种类型的连接，一种是隧道（tunnel）连接，它定义了一个 LNS 和 LAC 对；另一种是会话（session）连接，它复用在隧道连接之上，用于表示承载在隧道连接中的每个 PPP 会话过程。

隧道透传 PPP 帧



L2TP 连接的维护以及 PPP 数据的传送都是通过 L2TP 报文的交换来完成的，这些报文封装在 UDP 报文里，从而在承载在 TCP/IP 上。

L2TP 报文可以分为两种类型，一种是控制报文，另一种是数据报文。控制报文用于隧道连接和会话连接的建立与维护。控制报文的传输是可靠的，使用了报文编号确认，滑动窗口，超时重传，隧道保活检测等机制保证控制报文的传输。数据报文则用于承载用户的 PPP 会话数据包。数据报文本身不保证可靠传输，应该根据上层应用由上层协议保证数据报文的可靠投递。

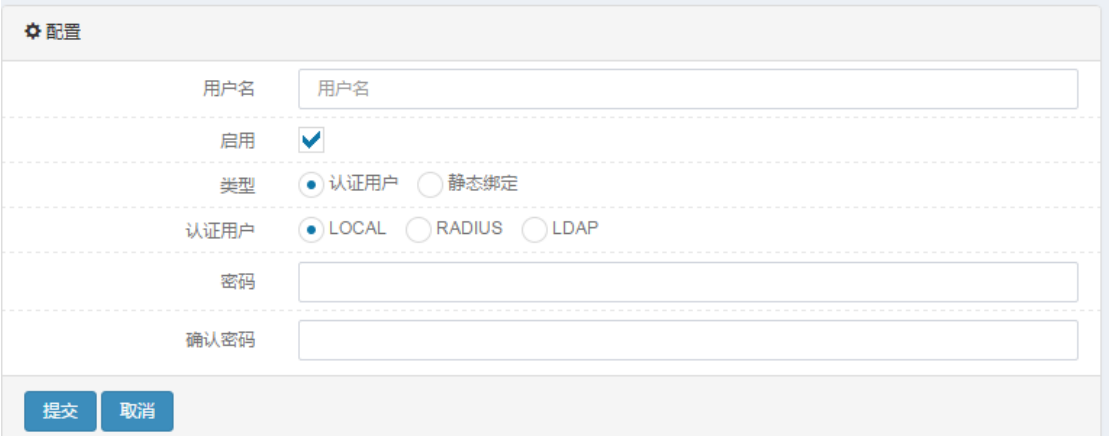
33.2 配置L2TP

T 系列防火墙设备出厂默认是没有 L2TP 配置的，配置 L2TP，需要进行地址池，认证用户组等配置。

33.2.1 配置认证用户

认证用户是在客户端进行拨号时进行认证使用的，包括用户名，密码的配置。

配置认证用户：进入**对象>用户对象>用户**，点击**新建**



参数说明：

用户名： 帐号的名称，长度限制为 63 个字符。

启用：选中表示启用此帐号。

类型：配置用户类型是否是认证用户。

认证用户：认证用户的类型。

密码： 此帐号的密码。如果使用 RADIUS 认证，则不用配置密码。

确认密码：确认账号密码。

配置步骤：

1. 在用户名一栏填写帐号的名称。
2. 点击启用。
3. 类型选择认证用户。
4. 如果不用 RADIUS 认证，则输入密码，并确认一遍。
5. 如果通过 RADIUS 认证，则选择一个配置好的 RADIUS 配置。
6. 点击**提交**。

33.2.2 配置用户组

L2TP 模版配置时必须需要一个用户组，客户端的拨号帐号必须是用户组里包含的帐号。

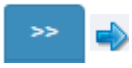
配置用户组：进入**对象>用户对象>用户组**，点击**新建**

名称： 用户组的名称。

用户成员： 要加入用户组的认证用户。

配置步骤：

10. 配置用户组名称。

11. 选取可选成员中的帐号，点击  ，加入到组中。

12. 点击**提交**。

33.2.3 配置接口接入控制

进入**网络>接口>物理接口，**点击某一接口，进入**编辑物理接口**页面

参数说明：

接口：物理接口名称。

名称：物理接口的别名。

管理状态：物理接口的启用或关闭，可选 UP/DOWN。

协商模式：物理接口协商模式，可选自协商/非自协商。

速率：物理接口协商速率，单位 Mbps。可选 1000/100/10。

双工模式：物理接口双工模式，分为全双工/半双工两种（FULL/HALF）。

MTU：MTU 值，范围为 68-1500。

管理访问：配置该接口地址上允许访问的服务类别。

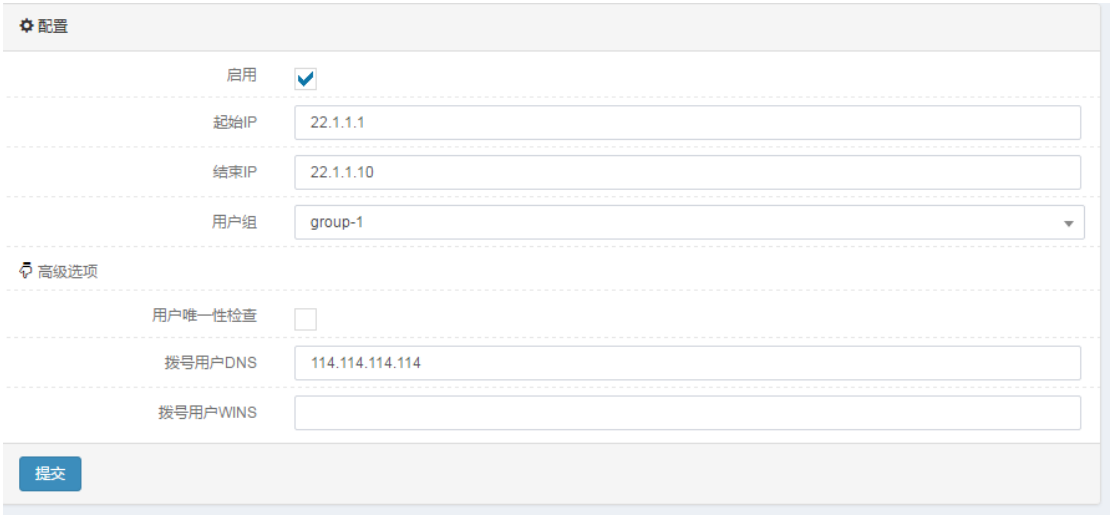
接入控制：接口在网络中的接入方式。

配置步骤：

13. 配置地址模式为静态，并配置正确的地址/掩码。
14. 配置管理访问。
15. 接入控制中选中 L2TP。
16. 点击**提交**。

33.2.4 配置L2TP

进入**网络>VPN>L2TP>配置**，进入 L2TP 的**配置**界面



参数说明：

启用 L2TP： 选中表示启用 L2TP 功能，否则停止 L2TP 功能。

起始 IP：用来进行地址分配的起始地址。

终止 IP：用来进行地址分配的终止地址。

用户组：通过选中的用户组来对拨号客户端身份进行验证。

高级选项：可选的拨号用户 DNS 和拨号用户 WINS 配置，用于在客户端拨号成功后，为用户拨号连接设置 DNS 和 WINS 地址。可选的用户唯一性检查约束同一用户是否可以同时多次登入。

配置步骤：

22. 选中启用 L2TP。
23. 配置起始 IP。
24. 配置终止 IP。
25. 选择一个用户组。
26. 点击**提交。**

33.3 配置案例

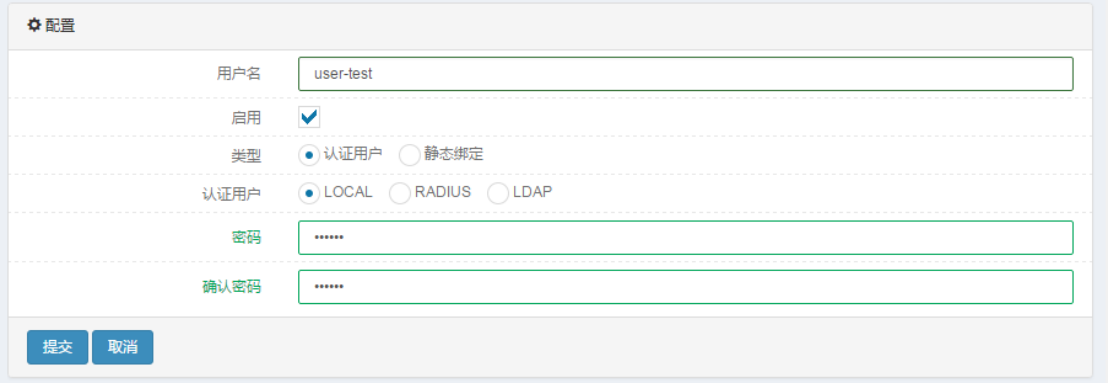
33.3.1 案例1：在接口ge0/0上启用L2TP

案例描述

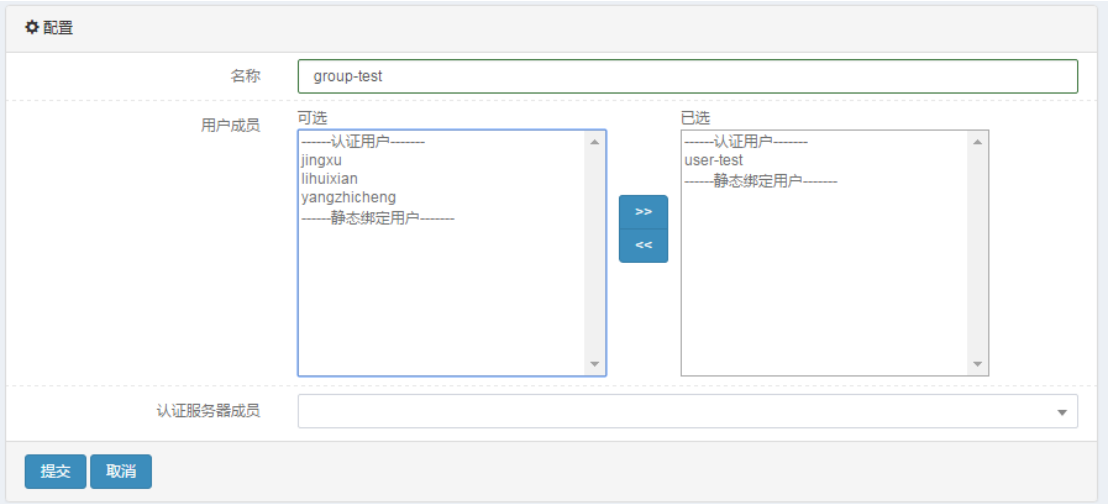
在物理口 ge0/0 上配置 L2TP，允许客户端进行 L2TP 拨号。

配置步骤：

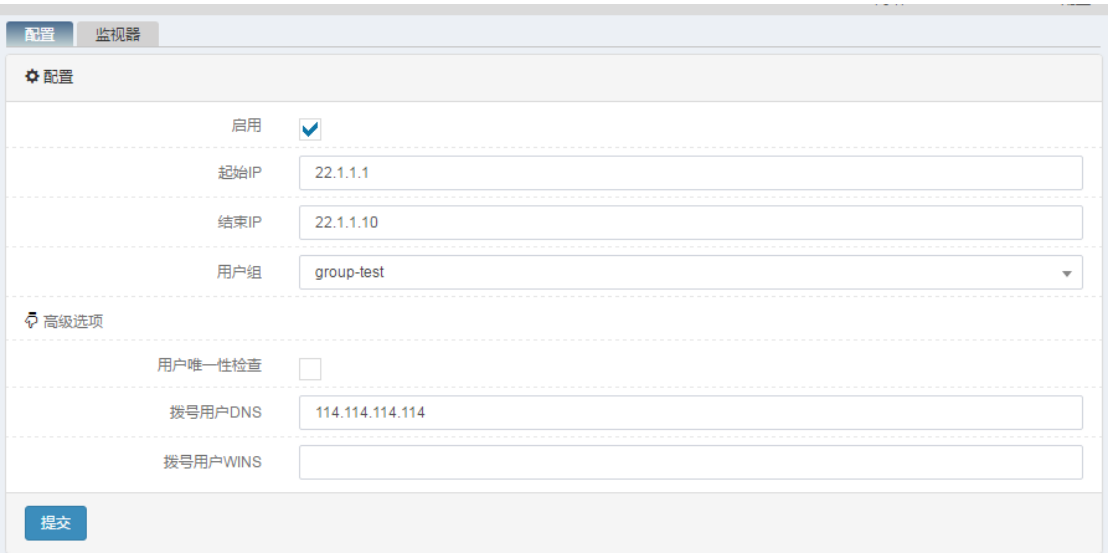
1. 进入**对象>用户对象>用户**，点击新建，如下图：



2. 输入参数。
3. 点击**提交**完成设置。
4. 进入**对象>用户对象>用户组**，点击**新建**。



5. 输入参数。
6. 点击**提交**完成设置。
7. 进入**网络>VPN>L2TP>配置**，进入 L2TP 的配置界面。



8. 输入参数。
9. 点击提交完成设置。
10. 进入**网络>接口>物理接口**，点击接口 ge0/0，进入编辑页面。

11. 配置 IP 地址，在接入控制中选取 L2TP。
12. 点击**提交**完成设置。

33.4 L2TP监控与维护

33.4.1 察看L2TP会话信息

进入**网络>VPN>L2TP>监视器**，察看 L2TP 的会话信息

在该页面可以点击 ✖ 可以使某一特定登录用户断开，点击 清空所有 可以断开所有登录用户。

33.5 故障分析

33.5.1 L2TP客户端拨号，无法建立连接

现象	L2TP客户端直接拨号到LNS，无法建立连接。

分析	有可能是以下几种情况导致客户端无法建立连接 ● 客户端的用户名密码错误，确认一下用户名和密码。 ● 客户端指定的连接地址不是LNS拨号接口配置的地址。 ● 查看服务端配置的地址池地址是否已分配完全，是否还有可用地址。 ● 接口是否勾选L2TP，允许客户端连接。

33.5.2 L2TP建立连接后，出现异常断开

现象	L2TP客户端直接连接到LNS，出现异常断开连接。
分析	有可能是以下几种情况导致客户端无法建立连接 ● 由于网络故障导致L2TP隧道的hello报文没有应答，设备断开隧道连接。请确认网络线路没有故障，而且L2TP服务器接口正常工作。

34 第34章 DNS 代理

34.1 DNS代理概述

DNS 透明代理技术，能够有效实现对多条链路带宽的合理利用，避免带宽资源浪费的情况。主要通过对内网用户访问外网资源的时候对 DNS 解析过程进行优化，内网用户所有 DNS 请求可以通过 DNS 代理设备进行转发。可以通过对多条链路发起 DNS 请求探测，根据探测结果结和预先设定的策略，将 DNS 请求转发到不同的服务器，用户就会得到比较理想的 DNS 请求结果，从而实现对链路带宽资源的合理利用。

34.2 配置DNS代理

34.2.1 配置服务器

1. 进入**网络>DNS 代理>服务器**，如下图所示：

IP 地址：DNS 服务器地址。

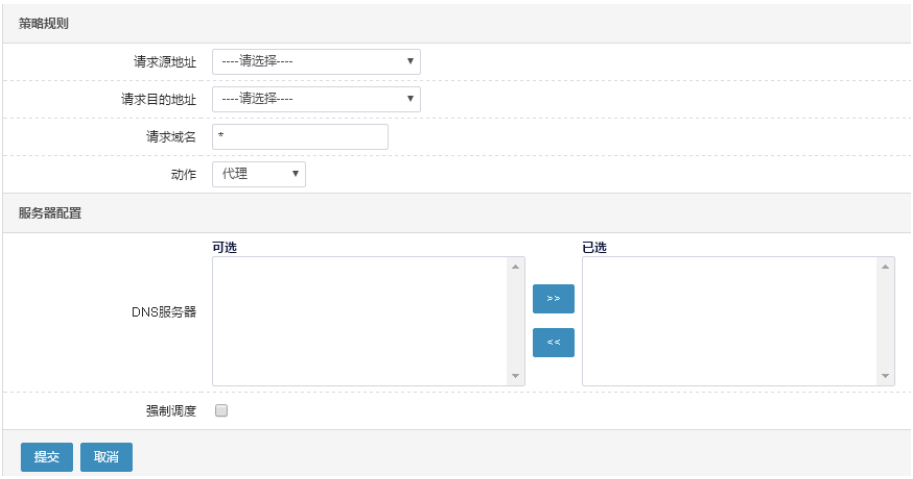
下一跳地址：到达 DNS 服务器选择的下一跳地址。

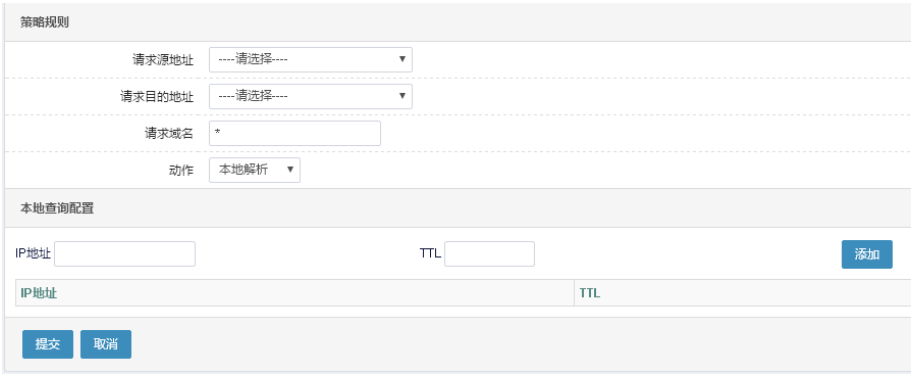
权值：当前 DNS 服务器的权值或优先级，取值范围[1,100]。

2. 根据需要修改参数。
3. 点击确定，提交配置。

34.2.2 配置代理策略

1．进入**网络>DNS 代理>代理策略**，如下图所示：





策略规则配置参数说明：

请求源地址：DNS 请求报文的源地址，配置为 any 时，所有源地址的请求报文都可以匹配。

请求目的地址：DNS 请求报文的目的地址，配置为 any 时，所有目的地址的请求报文都可以匹配。

请求域名：DNS 报文请求的域名。

动作：命中策略后是做代理、转发还是本地解析。

服务器配置参数说明：

DNS 服务器：命中策略后，如果动作是代理，可以选择服务器。

本地解析配置参数说明：

IP 地址：点分十进制，配置 DNS 的域名请求所对应的指定 IP 地址。

TTL：DNS 配置的本地解析 IP 地址缓存时间。

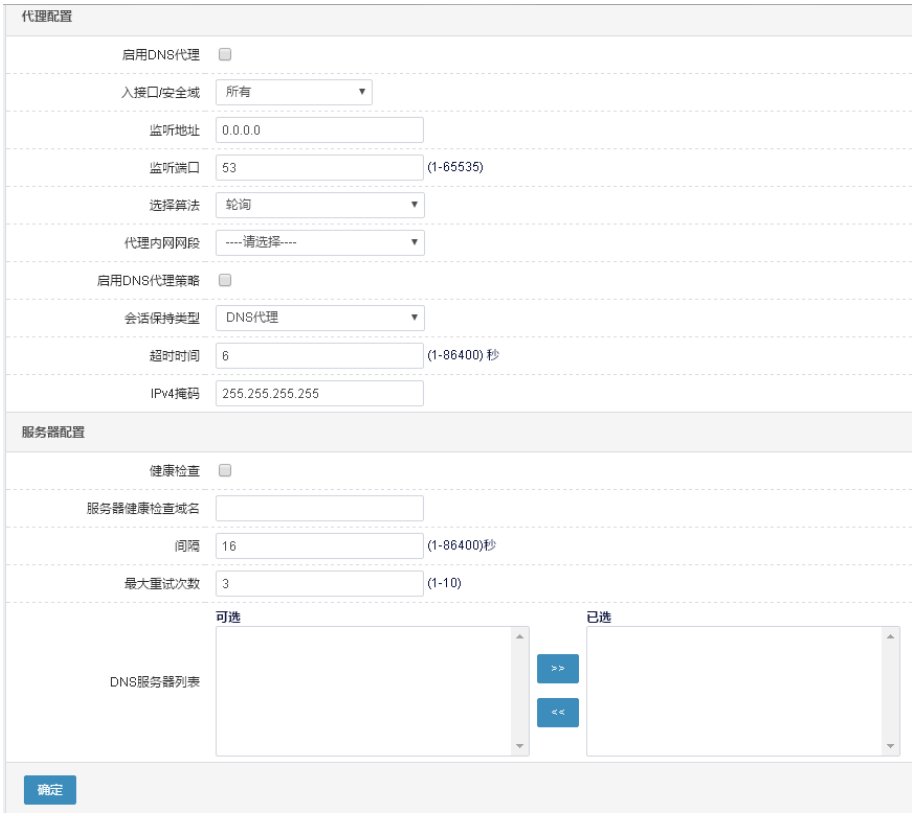
添加：添加需要配置的 DNS 本地解析条目（限制范围是 5 条）。

2. 根据需要修改参数。

3. 点击**确定**，提交配置。

34.2.3 配置全局配置

1. 进入网络>DNS 代理>全局配置，如下图所示：



代理配置参数说明：

启用 DNS 代理：用于设定是否启用 DNS 代理功能。

入接口/安全域：DNS 请求报文的入接口。

监听地址：用来设定监听的 DNS 服务器的地址，通常设置为用户网络配置中 DNS 服务器的地址，默认为所有。

监听端口：用来设定监听的 DNS 服务器的端口，默认为 53 端口。

选择算法：选择服务器的算法，包含轮询，加权轮询，加权最小流量，优先级。

代理内网网段：选择需要代理的源 IP 地址对象。

启用 DNS 代理策略：默认不勾选。勾选后，DNS 代理>代理策略页面配置

的内容生效。

会话保持类型：选择会话保持类型，可以对 DNS 请求进行基于请求域名和源地址的会话保持和请求源地址的会话保持，默认不配置。

超时时间：用于会话保持的超时时间，默认 30 秒。

Ipv4 掩码：用于会话保持源地址的掩码，默认 255.255.255.255。

服务器配置参数说明：

健康检查：是否对 DNS 服务器列表中的 DNS 服务器进行健康检查。如果启用了此项功能，则系统会向 DNS 服务器列表中的 DNS 服务器发探测报文，如果某 DNS 服务器对探测报文没有响应，则该 DNS 服务器不会参加调度。

服务器健康检查域名：要检查的 dns 域名。

间隔：DNS 服务器列表中服务器进行健康检查的间隔时间，默认为 16 秒。

最大重试次数：健康检查探测包探测失败后的重试次数。例如，默认参数 3 次，如果发送 3 个健康检查状态包都没有收到回应或者 3 次都探测失败，则健康检查返回状态为失败的最终结果。

DNS 服务器列表：选择使用的 DNS 服务器。

2. 根据需要修改参数。

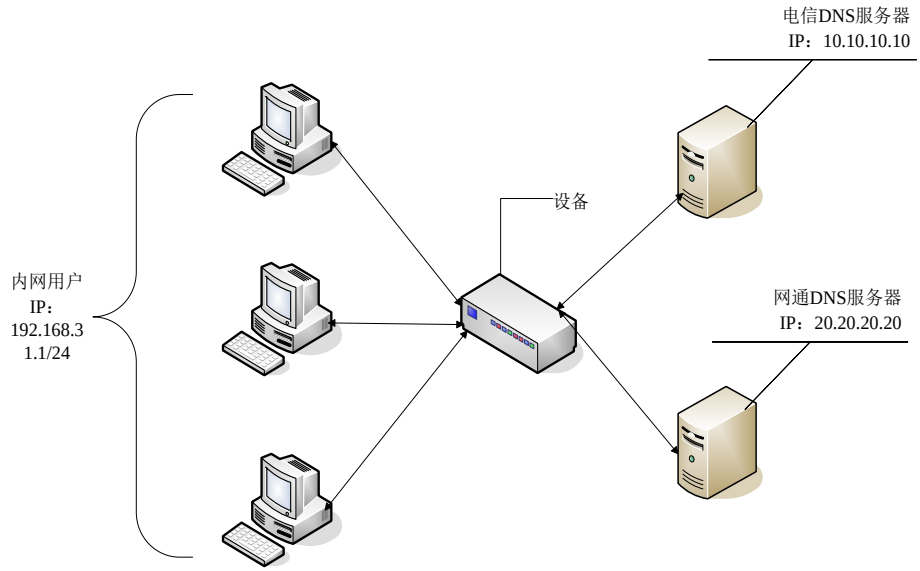
3. 点击**确定**，提交配置。

34.3 配置案例

34.3.1 DNS代理配置案例1

网络出口部署了一条电信链路，一条网通链路，这时如果内网大部分的用户电脑 DNS 地址都填写电信的 DNS 地址的话，就会大部分用户都使用电信的链路去访问相应的资源，而网通的链路只分担小部分的上网任务，这样就有可能造成电信的链路拥塞而网通的链路出现闲置的情况，通过设置 DNS 透明代理技术，不论内网用户填写哪家运营商的 DNS 服务器地址，都会通过设备进行 DNS 请求转发，设备会根据设定的调度策略选择合适的 DNS 服务器并把解析后的地址返回给内网用户，可以实现对带宽资源的合理利用。

配置步骤：



1、 配置网络环境，要保证内网用户流量可以正确访问外网。

2、 配置参数如下：

2.1 配置服务器

2.2 配置全局配置

34.3.2 DNS代理配置案例2

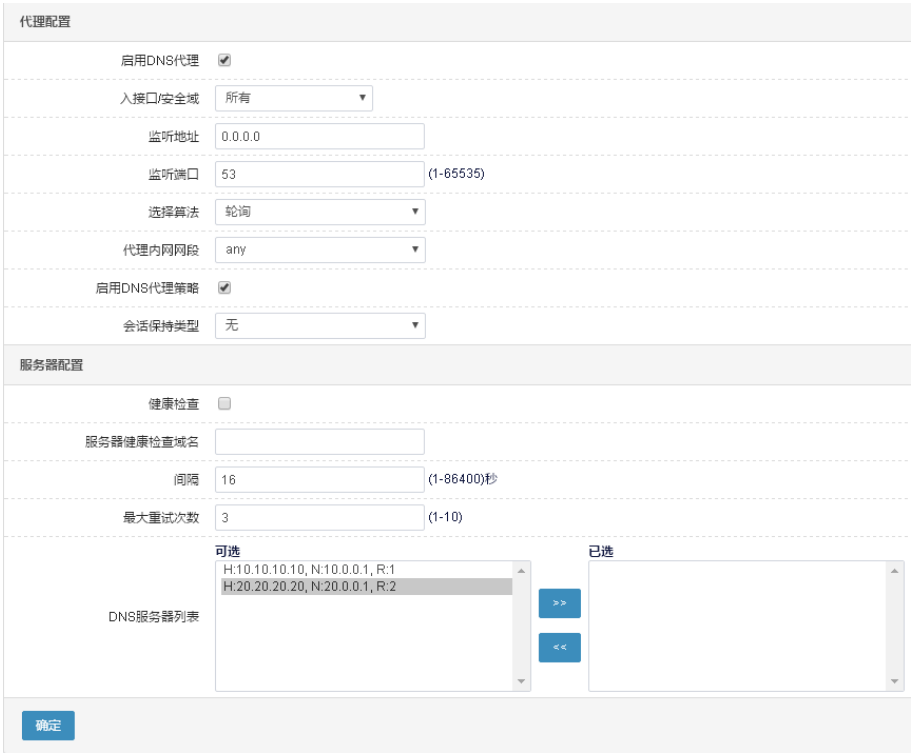
DNS 代理全局配置中勾选了 DNS 代理关联，这时如果没有配置本地解析功能的 DNS 策略，用户会根据电脑配置的 DNS 地址或通过设备匹配 DNS 代理策略和全局配置进行 DNS 请求转发，设备会根据设定的调度策略选择合适的 DNS 服务器并把解析后的地址返回给用户；而如果配置了 DNS 本地解析功能，那么用户发出的 DNS 请求就不会发往 DNS 服务器进行解析，而是根据本地的手动配置进行 DNS 的 A 记录请求的解析，并把解析后的地址返回给用户，这样就可以省去访问 DNS 服务器进行域名解析的过程。

配置步骤：

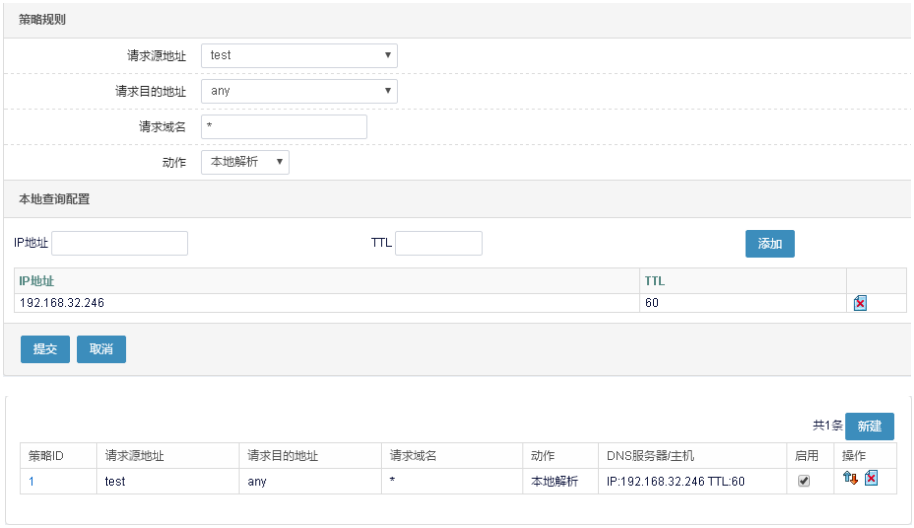
1、 配置 DNS代理功能，要保证勾选启用 DNS 代理，勾选启用 DNS 代理策略。

2、 配置参数如下：

2.1 配置全局配置：



2.2 配置本地解析代理策略并勾选启用：



用 wireshark 进行抓包测试，在没有启用本地解析功能时，可以正常访问百度网址，当引用配置地址为 192.168.32.246 的本地解析策略后，当 pc 客户端向百度发起域名请求，都会重定向到本地配置的 192.168.32.246 的 ip 地址，而不是通过 DNS 服务器去解析出百度真正对应的 ip 地址返回给用户。

35 第35章 DNS 服务

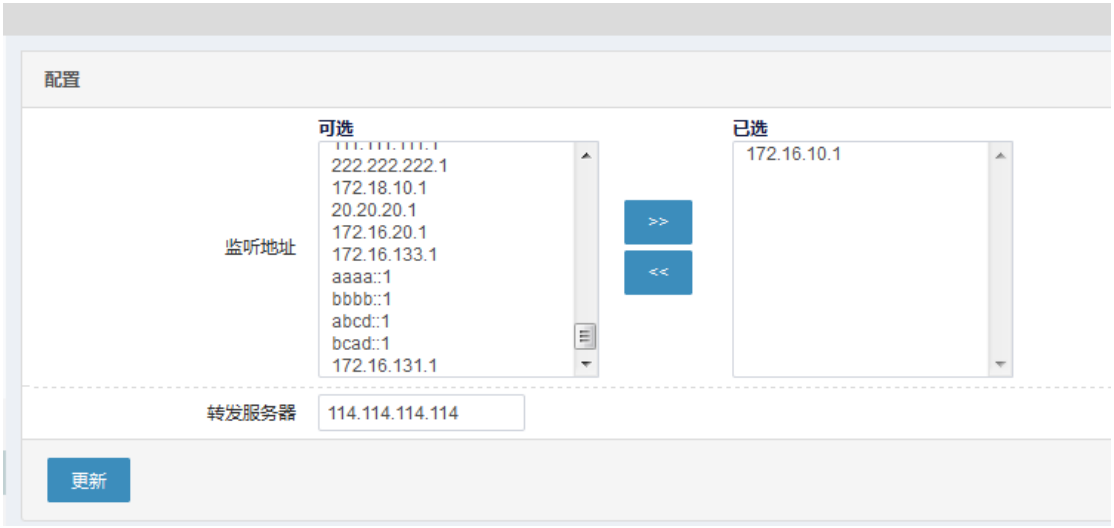
35.1 DNS服务概述

DNS（Domain Name Server，域名服务器）是进行域名(domain name)和与之相对应的 IP 地址 (IP address)转换的服务器。T 系列防火墙能够提供标准的 DNS 服务。

35.2 配置DNS服务

35.2.1 基础配置

1. 进入**网络>DNS 服务>基础配置**。



参数说明：

监听地址：监听 DNS 请求的地址。

可选：可供选择的设备 IP 地址。

已选：已被选择作为监听 DNS 请求的设备 IP 地址。

转发服务器：本地 DNS 查询失败后，会转发到此服务器进行解析。

2. 在左侧对话框选中想要监听 DNS 请求的设备 IP 地址，点击 

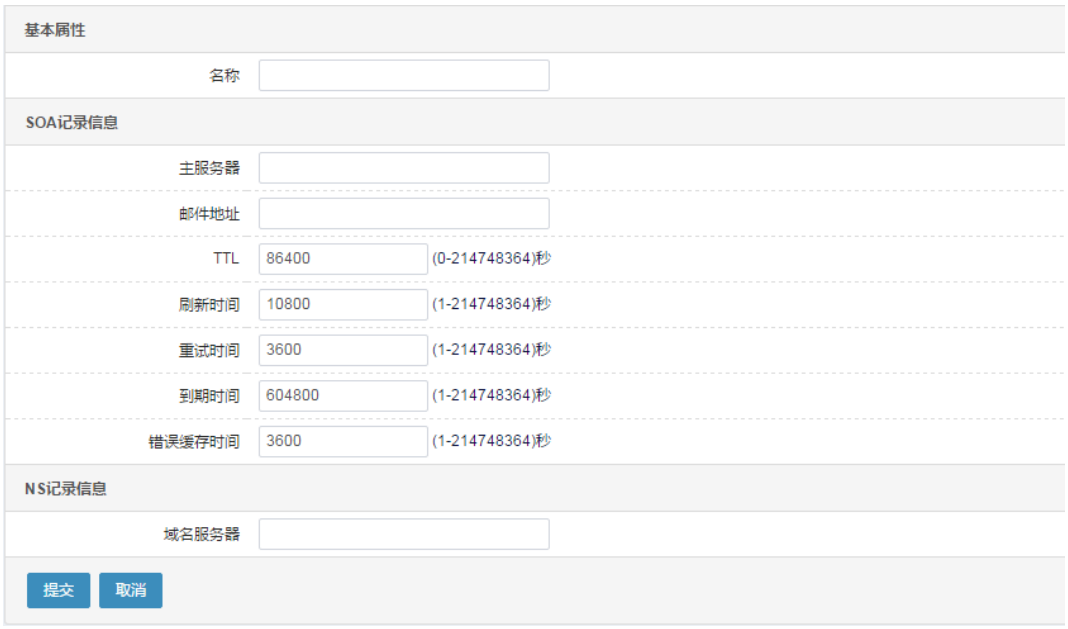
按钮选入到右侧对话框中。
3. 点击**更新**。

35.2.2 配置DNS记录

通过配置 DNS 记录，可以提供多种类型的本地权威解析，DNS 记录的管理风格与 bind 兼容，以 zone 为多记录的集合进行管理。

进入**网络>DNS 服务> DNS Zones**，

点击**新建**，进入 zone 的新建页面：



名称：zone 的域名。

主服务器：该 zone 的主域名服务器名称。

邮件地址：该 zone 的联系邮件地址。

TTL：zone 对应 soa 记录的 ttl 值，也作为该 zone 中记录的缺省 ttl 值。

刷新时间：soa 记录的 refresh 值，用于该 zone 的辅域名服务器从主域名服务器同步 zone 文件的周期时间。

重试时间：soa 记录的 retry 值，用于辅域名服务器从主域名服务器同步 zone 文件失败后，重试的间隔。

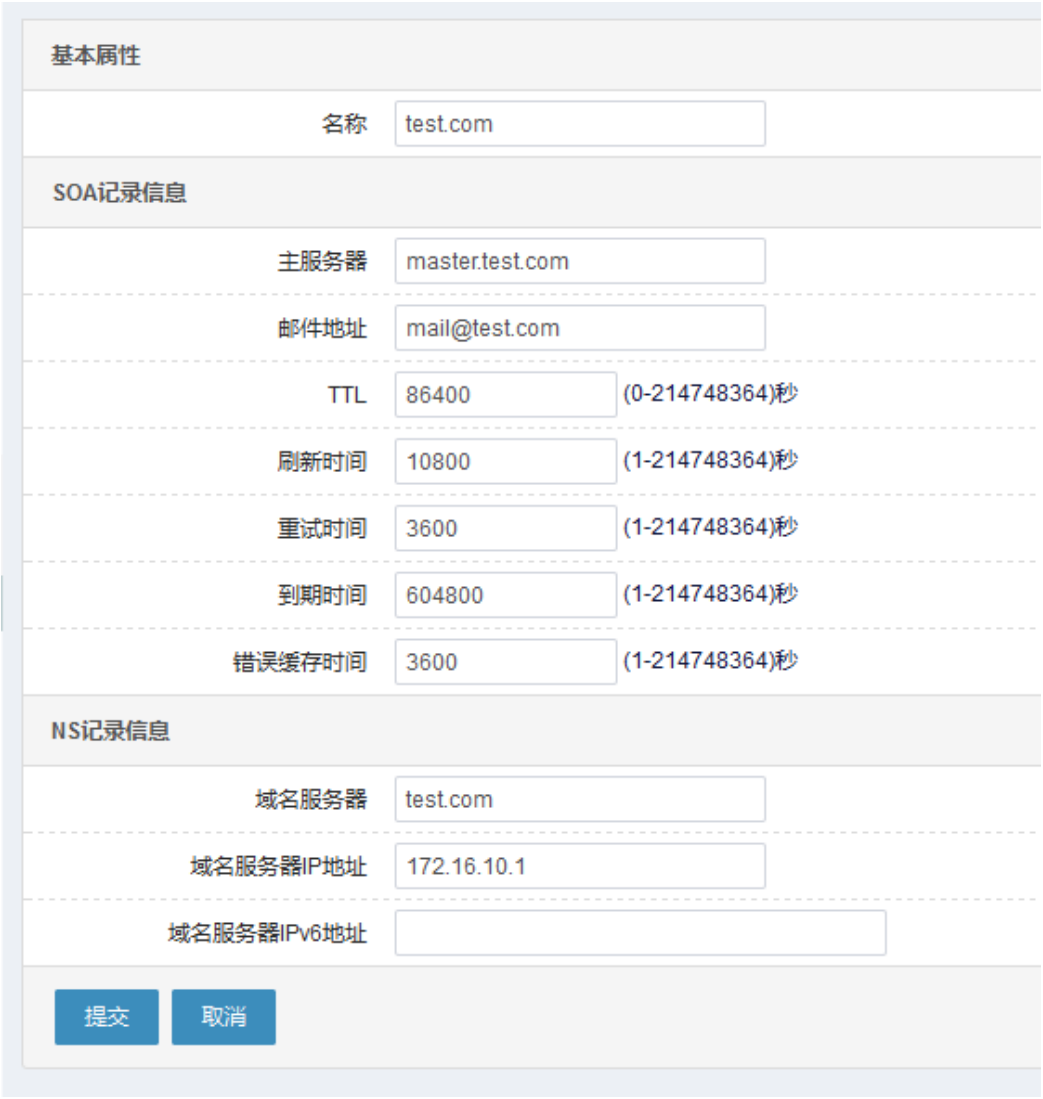
到期时间：soa 记录的 expire 值，若辅域名服务器与主域名服务器通信失败时间超过该值，则认定该 zone 失效。

错误缓存时间：soa 记录的 negative ttl，用于该 zone 的错误记录的缓存时间。

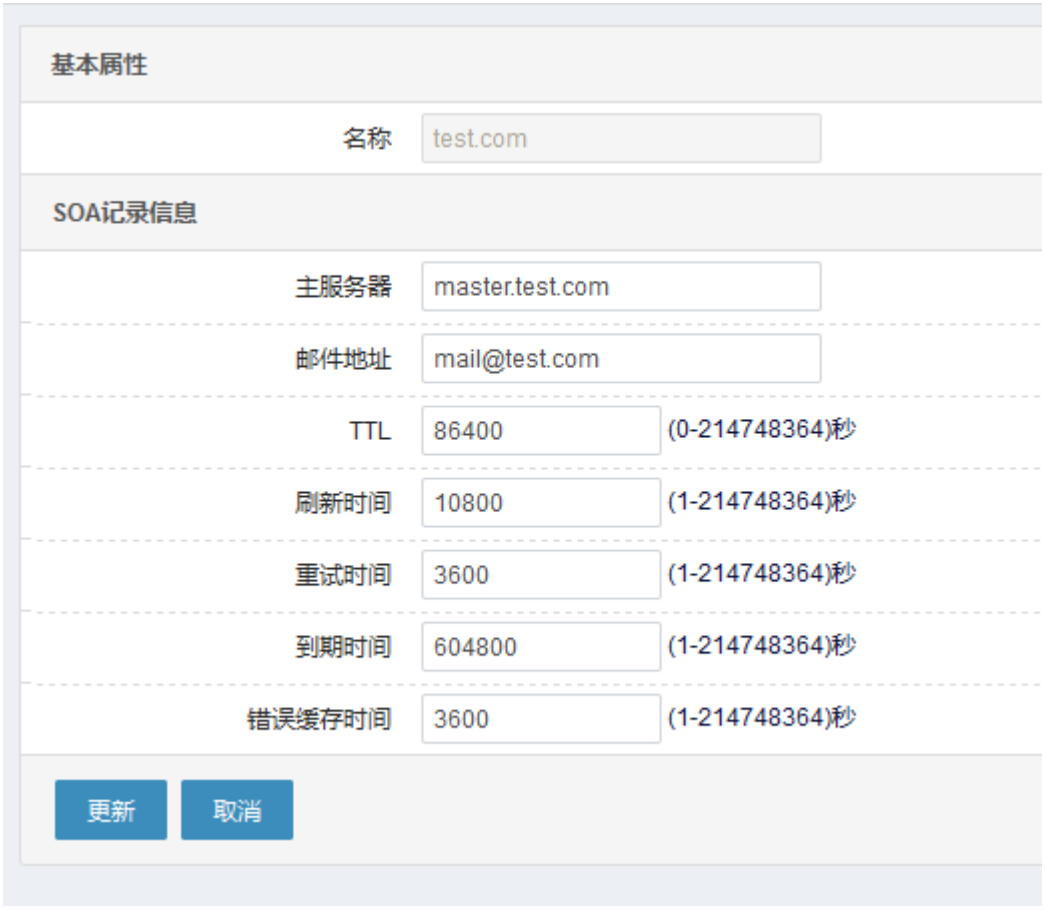
域名服务器：新建一个 zone 时，至少要有一条 ns 记录，该配置项表示以该 zone 名称为记录名称的 ns 类型记录的内容，即该 zone 的域名服务器名称。当添入的域名属于该 zone 时（即以该域名结尾），则需添入对应的 A 记录数据（IPv4 地址）或者 AAAA 记录数据（IPv6 地址）。

配置步骤：

添加时，在所有配置项添入对应内容后，点击提交。

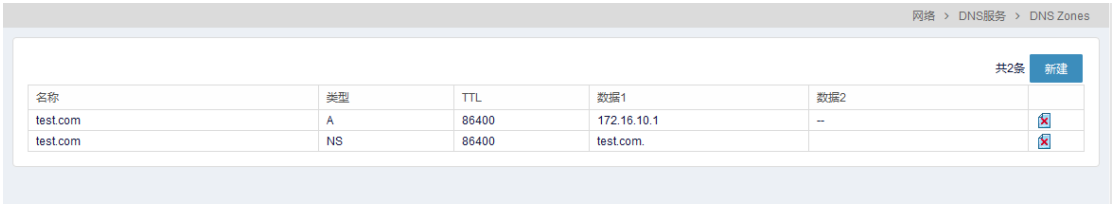


当需要修改以上某项内容（除 zone 名称）时，在 zone 列表点击对应的 zone 名称，进入到如下页面：

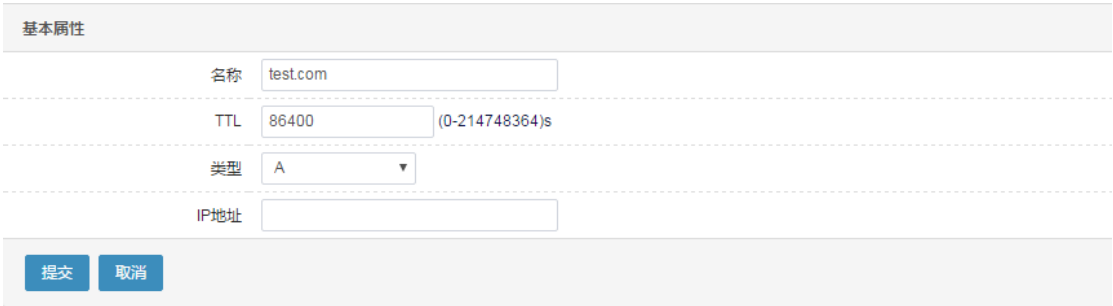


在对应位置添入修改后的信息，点击**更新**，使得修改内容生效。

在 zone 列表页面，点击 **DNS 记录**列中表示当前 zone 中存在记录个数的数字，进入到该 zone 的 DNS 记录管理页面，如下：



点击**新建**，进入新建该 zone 的 DNS 记录的页面。



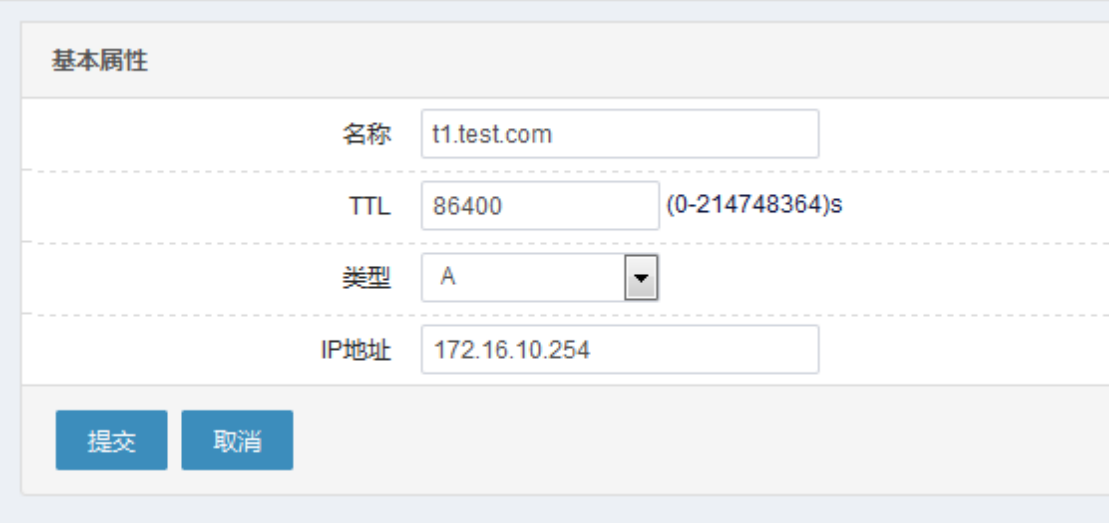
名称：记录名称。

TTL：当前记录的 ttl 值。

类型：记录类型，目前共支持 A、AAAA、NS、CNAME、MX、TXT 以及 PTR 7 种类型。

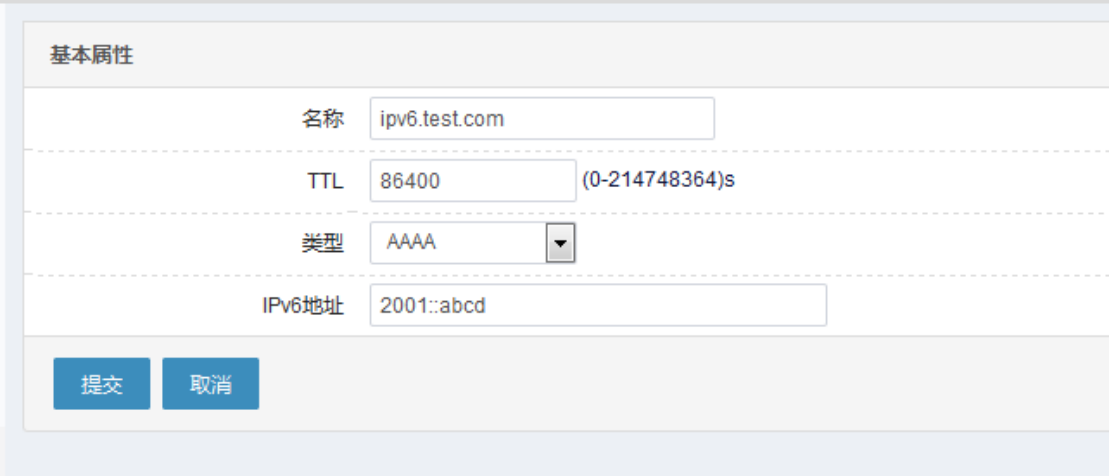
A：ipv4 地址类型记录。

IP 地址：记录名对应的 IP 地址。



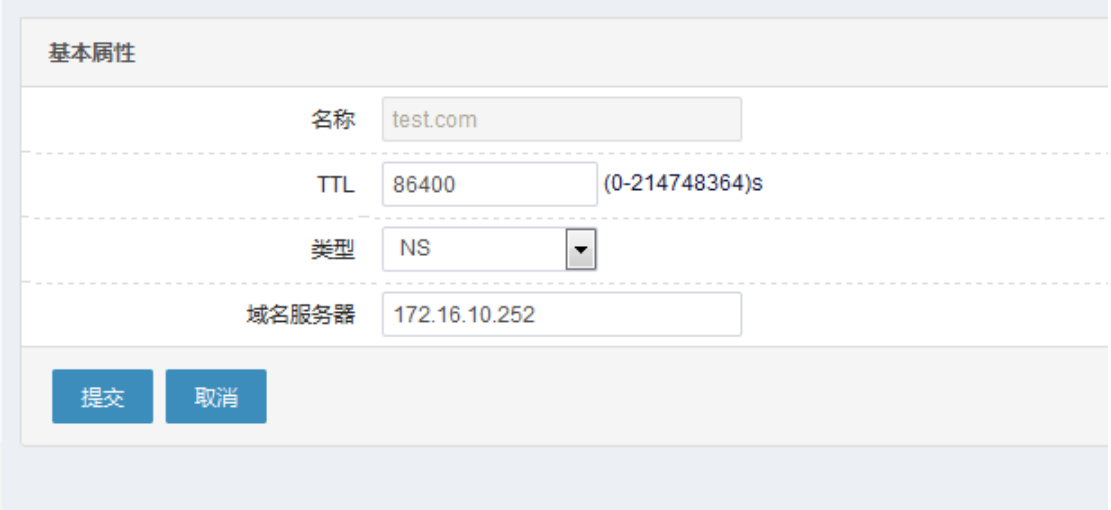
AAAA：ipv6 地址类型记录。

IPv6 地址：记录名对应的 IPv6 地址。



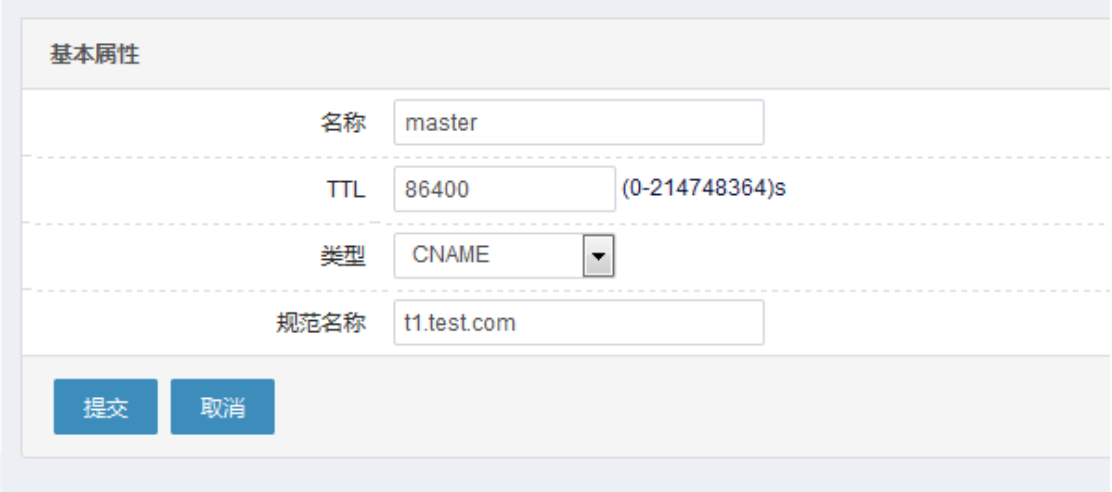
NS：域名服务器记录。

域名服务器：记录名称表示的 zone 对应的权威域名服务器名称。



CNAME：规范名记录。

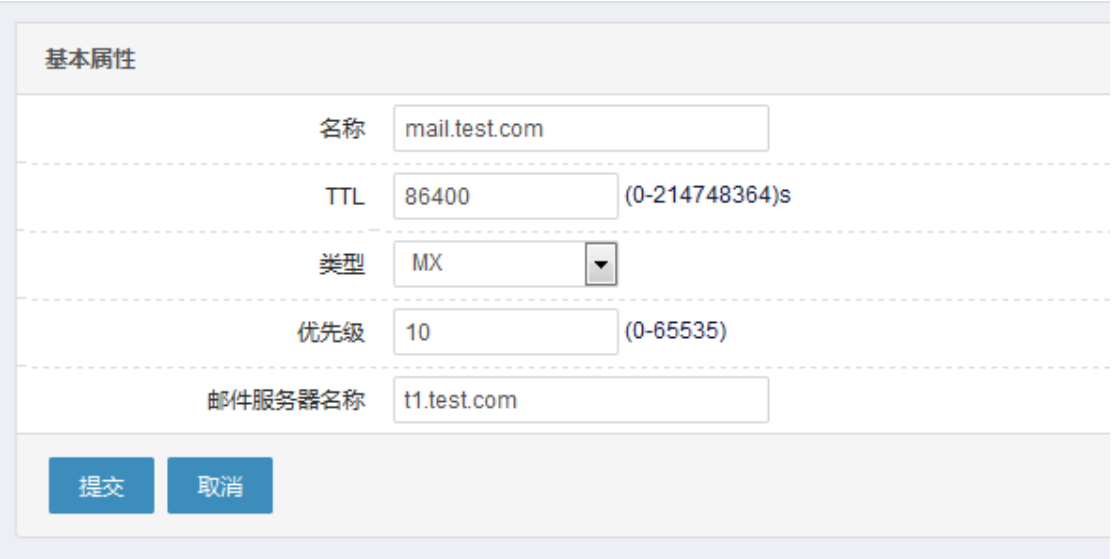
规范名称：记录名称表示的别名所对应的规范域名名称。



MX：邮件中转站记录。

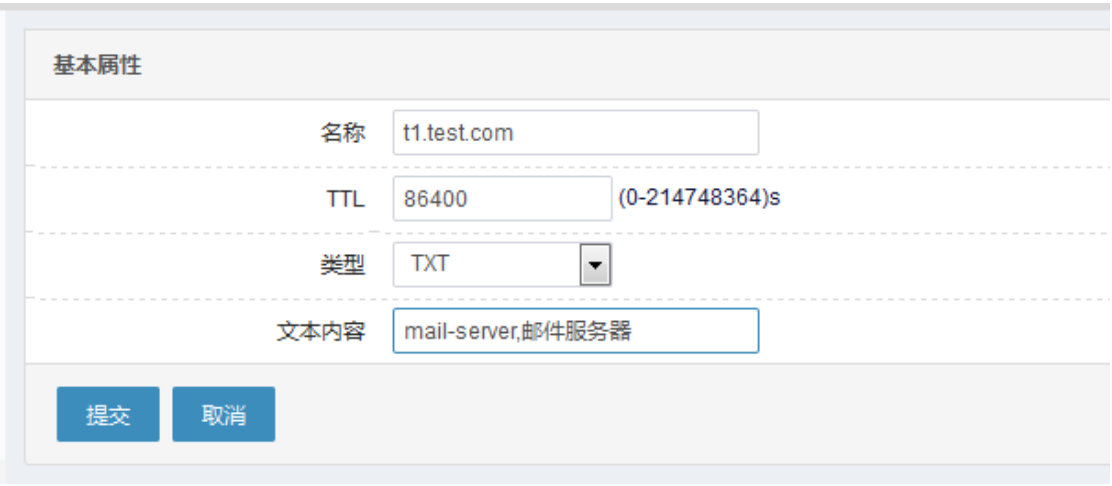
优先级：选择 mx 记录的优先级，数值越小，优先级越高。

邮件服务器名称：记录名称的域名表示的邮件域名所在的邮件服务器（或通往邮件服务器的中转邮件服务器）名称。



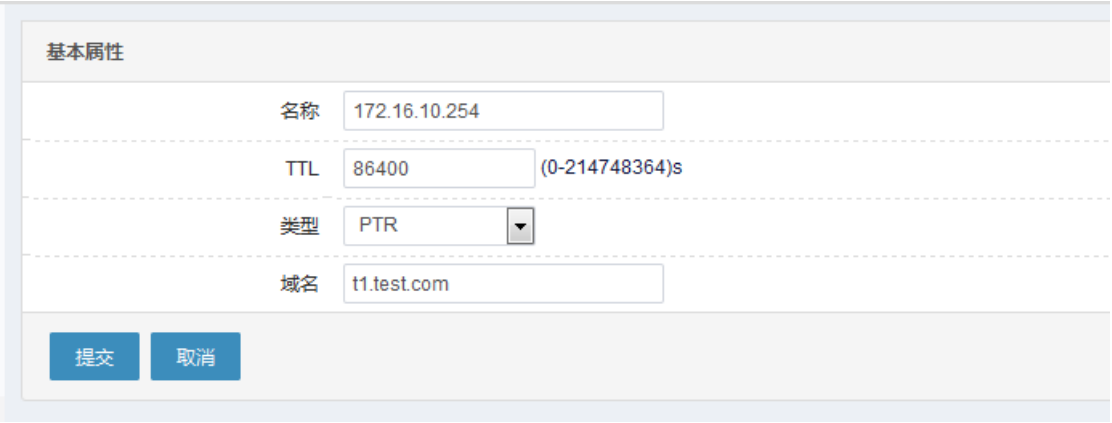
TXT：文本类记录。

文本内容：记录名称对应的一段文本信息，可由该 zone 管理员自定义，表示任意内容。可以是中文或者英文。



PTR：反向查询记录。

域名：与 A（或 AAAA）正好相反，通过 IPv4（或 IPV6）地址查找对应的域名，主要在反向 zone（in-addr.arpa.或者 ip6.arpa.）中管理。

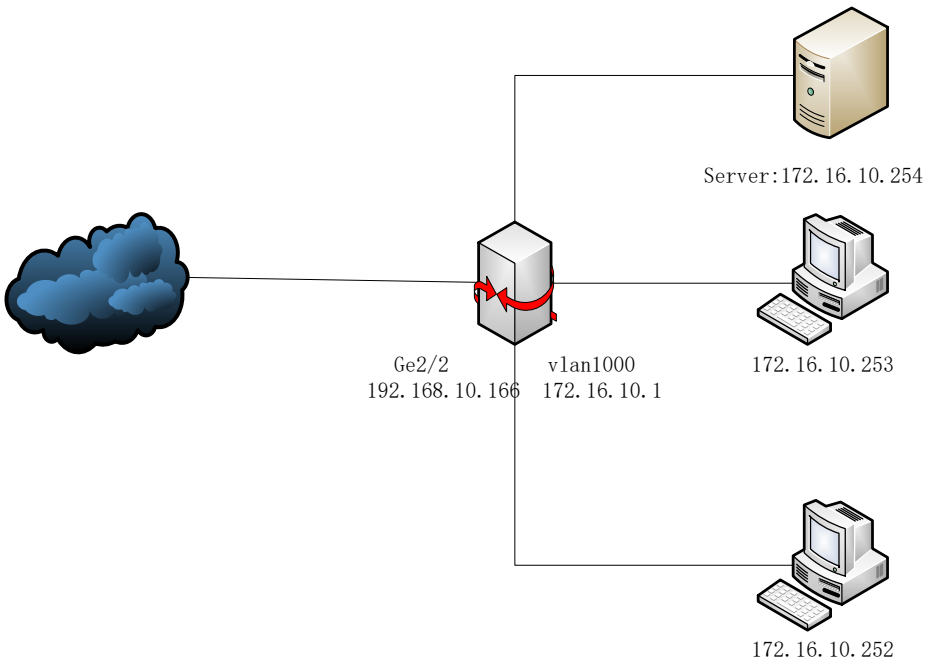


35.2.3 配置案例

案例描述：

内部网络通过域名访问内部服务，同时又能正常上网。（需要提前配置好与外网互通的路由）

案例组网图：

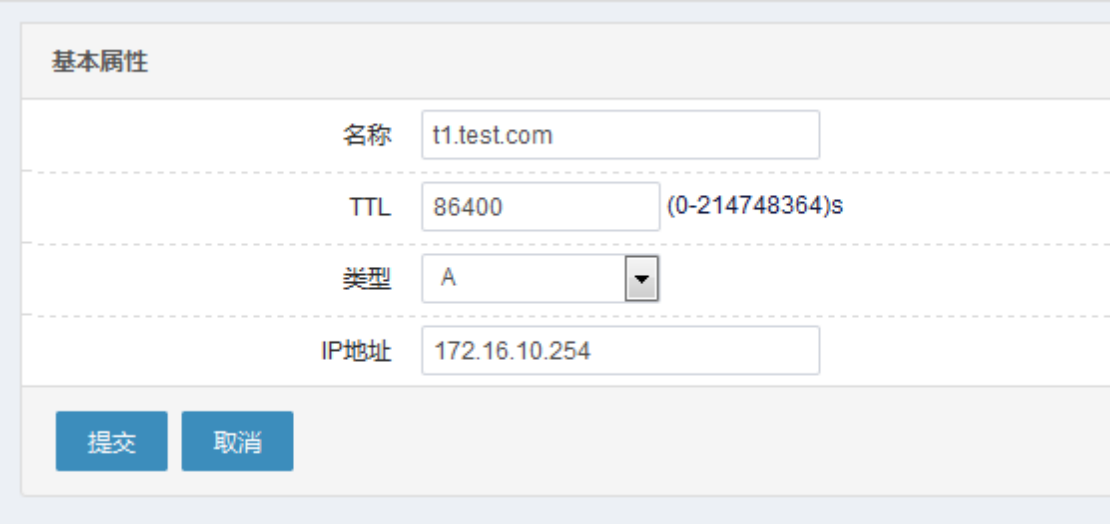


配置步骤：

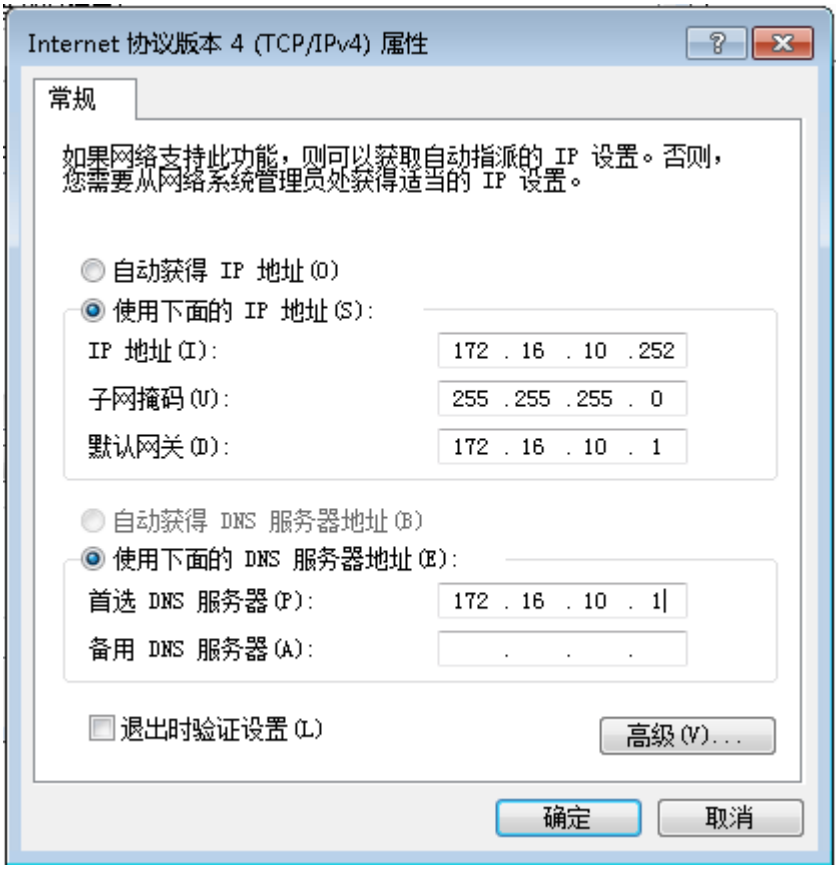
1. 配置 DNS 监听地址以及 DNS 转发服务器：

2. 配置 DNS zones：

3. **新建** dns 记录，输入 server 的域名对应 A 记录，点击**提交**。



4. 客户端配置 DNS 服务器为 172.16.10.1，此时既可以访问内部 server 又可以正常上网。



36 第36章 系统参数

36.1 系统参数概述

协议管理：网络设备对不同协议的连接都有超时删除功能，以保护设备的连接资源。在本产品中，对 TCP 协议的全连接，默认超时时间是 1 小时，UDP 协议为 30 秒。有些应用程序在全连接建立后，报文只会根据实际的数据进行交互，而没有保活机制，往往会导致连接超时删除，后续的数据无法通过设备。协议管理功能提供了设置特定服务超时时间的功能，可以解决这种需要长时间空闲连接的问题。

TCP 状态管理：链接数统计时，根据此链接的 tcp 状态，决定是否统计此链接，如果选择 ESTABLISH 链接，只统计状态为 established 链接，选择所有链接，统计所有链接。

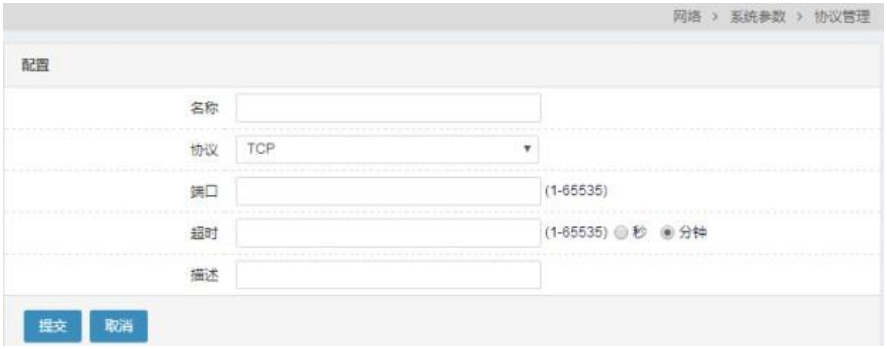
参数管理：一些模块功能的控制开关，统一置于此处，方便操作。

36.2 协议管理

配置步骤：

1. 进入**网络>系统参数>协议管理。**

2. 点击**新建**按钮。



参数说明：

名称：该协议管理的名称。

协议：选择该协议管理的协议类型，TCP 或 UDP。

端口：填写该协议对应的业务端口。

超时时间：<1-65535>，单位为分钟或者秒。

描述：对该协议管理进行注释说明。

3. 点击**提交**按钮以使配置生效。如下图为配置好的协议管理。

注意

配置协议管理后，对新建的连接才会生效。

36.3 TCP状态管理

配置步骤：

1. 进入**网络>系统参数>TCP 状态管理。**

2. TCP 全连接状态统计

勾选 **ESTABLISHED 连接**，只统计全连接；勾选 **所有连接**， 统计所有连接，包括全连接和半连接。

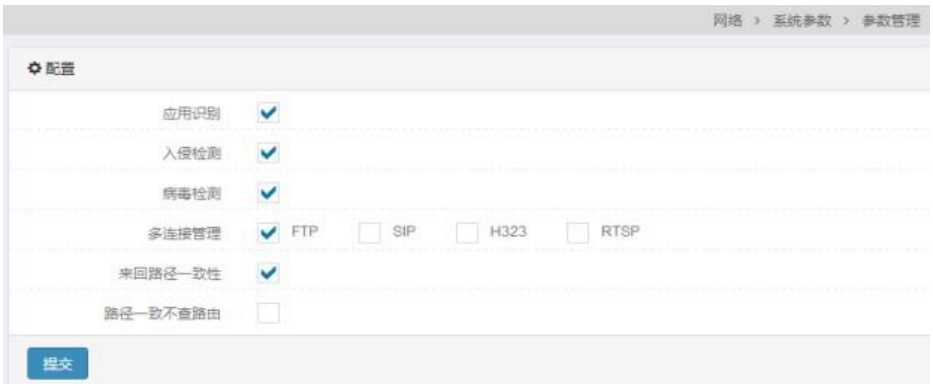
3. TCP 状态检查

勾选**开启或者关闭**按钮， 实现 tcp 宽松检查的开启和关闭。

36.4 参数管理

配置步骤：

1．进入**网络>系统参数>参数管理。**



应用识别：是否开启应用识别。

入侵检测：是否开启入侵检测。

病毒检测：是否开启病毒检测。

多连接管理：是否将协议识别为多链接。

来回路径一致性：是否开启来回路径一致性。

路径一致不查路由：是否开启路径一致不查路由。

37 第37章 WEB 调试

37.1 WEB调试概述

为了方便用户进行配置排错，防火墙设备中提供了 WEB 调试功能。用户可通过该功能，直观的看到匹配指定条件的转发数据包在设备中的关键处理流程。

目前可观察的关键流程包含：数据包的流相关处理、NAT 处理、防火墙策略处理、包信息。

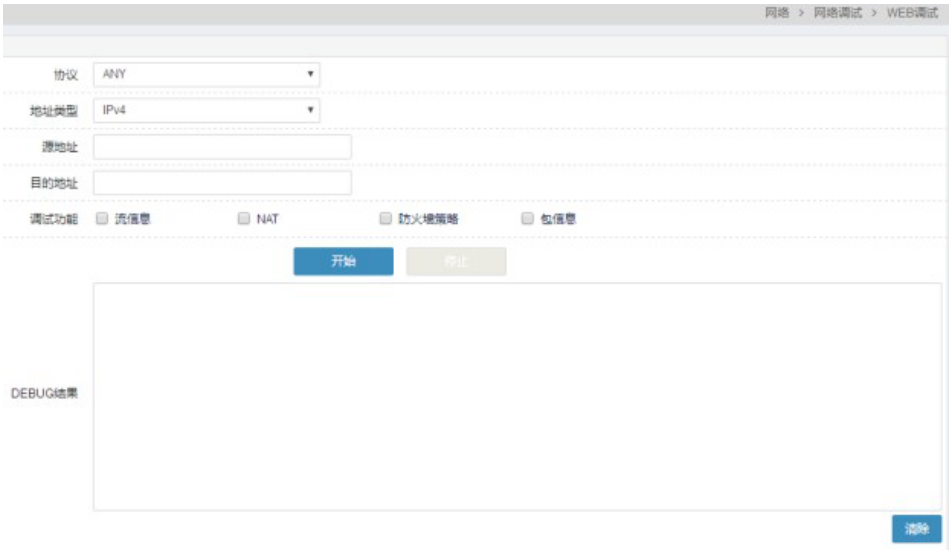
37.2 配置WEB调试

37.2.1 配置WEB调试的基本要素

WEB 调试的基本要素包括数据包的协议、地址类型、源地址、目的地址、调试功能。用户通过配置，可看到满足这些要素的转发数据包，在调试功能所指定的功能模块中是如何被处理的。

配置步骤：

1. 进入**网络>网络调试>WEB 调试**，如下图：



参数说明：

协议：数据包的协议类型，下拉框中可以选择 ANY、TCP、UDP、ICMP、OTHER。选择为 ANY 为所有协议，不同的协议类型还有各自对应的参数。

地址类型：数据包的 IP 类型，下拉框中可以选择 IPv4、IPv6。

源地址：数据包的源地址。

目的地址：数据包的目的地址。

调试功能：指定查看的功能模块处理结果，可选择流信息、NAT、防火墙策略。

流信息：数据包相关的流的新建、以及匹配信息。

NAT：数据包进行地址转换的信息。

防火墙策略：数据包进行防火墙策略匹配的信息。

包信息：数据包的信息。

2. 配置完毕后，点击**开始**，调试开始。
3. 点击**清除**，可以清空 DEBUG 结果框中显示的信息。
4. 在调试时，点击**停止**，调试停止。

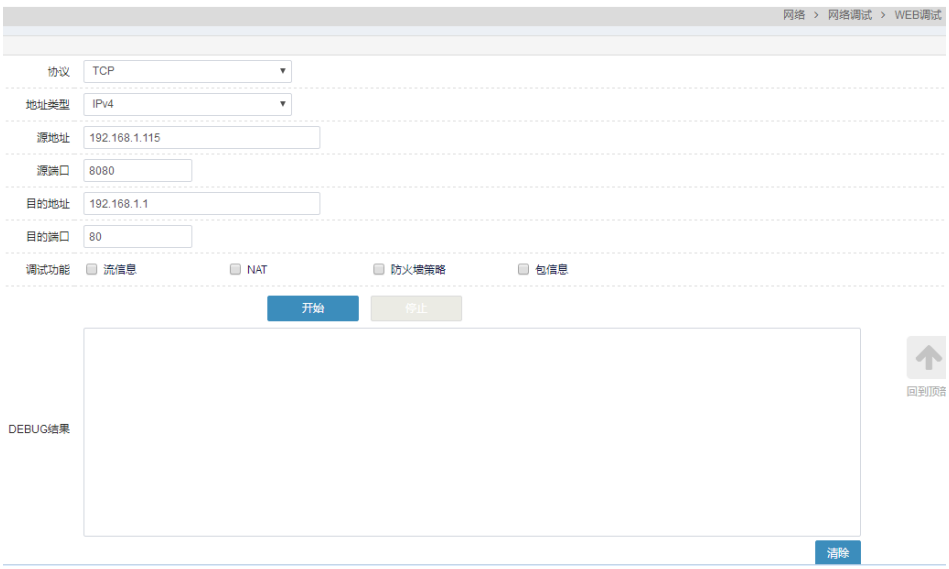
在调试过程中不能更改参数，需停止后方可更改。

37.2.2 配置协议为TCP(UDP)的WEB调试

协议为 TCP(UDP)的 WEB 调试需要填写源端口、目的端口参数。

配置步骤：

1. 进入**网络>网络调试>WEB 调试**，在**协议**下拉框中选择 **TCP**，填写参数，如下图：



源端口：数据包的源端口。

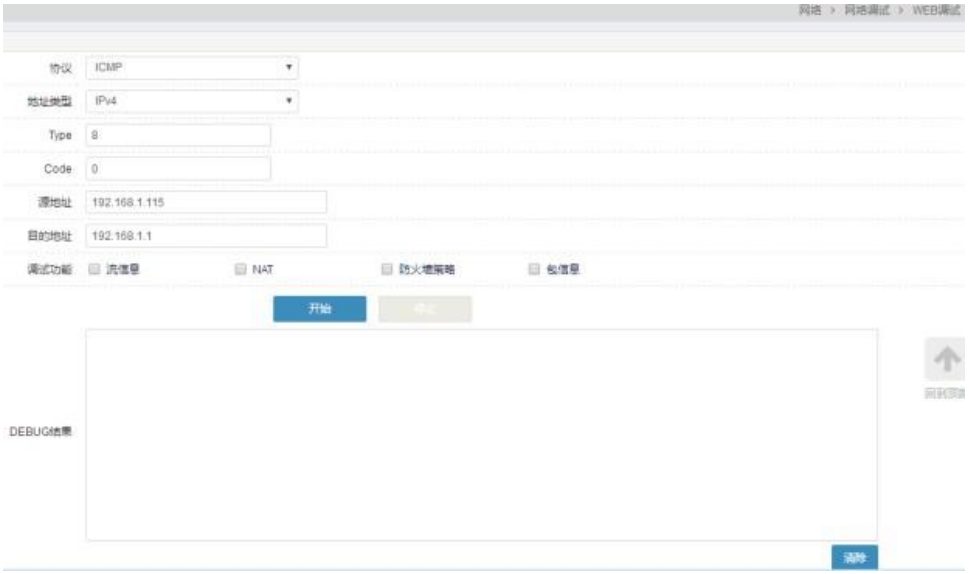
目的端口：数据包的目的端口。

37.2.3 配置协议为ICMP的WEB调试

协议为 ICMP 的 WEB 调试需要填写 Code、Type 参数。

配置步骤：

1. 进入**网络>网络调试>WEB 调试**，在**协议**下拉框中选择 **ICMP**，填写参数，如下图：



Type：ICMP 报文的类型，取值区间 0~255。

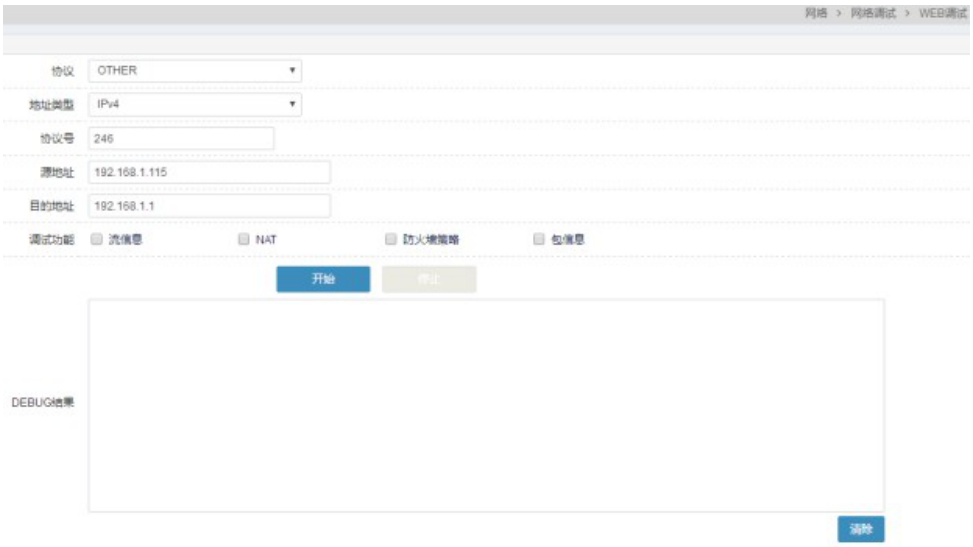
Code：ICMP 报文携带的的代码字段，取值区间 0~255。

37.2.4 配置协议为OTHER的WEB调试

协议为 OTHER 的 WEB 调试需要填写四层协议号参数。

配置步骤：

1. 进入**网络>网络调试>WEB 调试**，在**协议**下拉框中选择 OTHER，填写参数，如下图：



协议号：数据包的四层协议号，取值范围为 1~255。

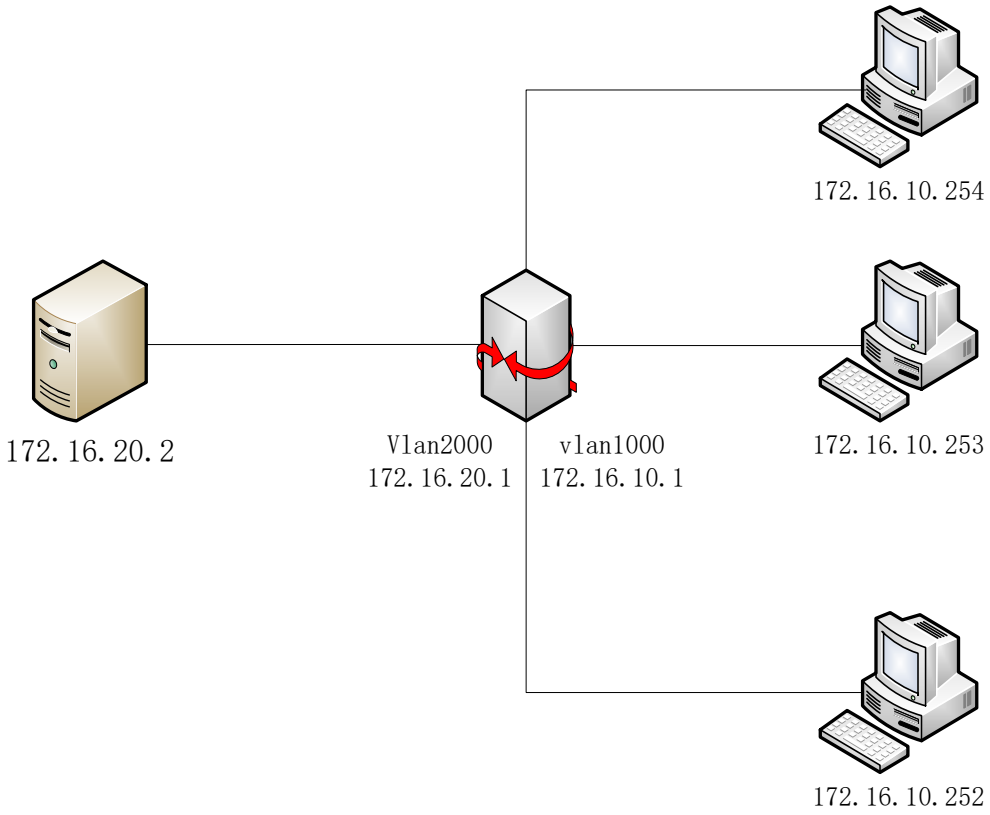
37.3 配置案例

37.3.1 案例1：使用IPv4的Web调试功能

案例描述：

观察内部地址做源 nat 后，访问 http server 的数据包交互信息。

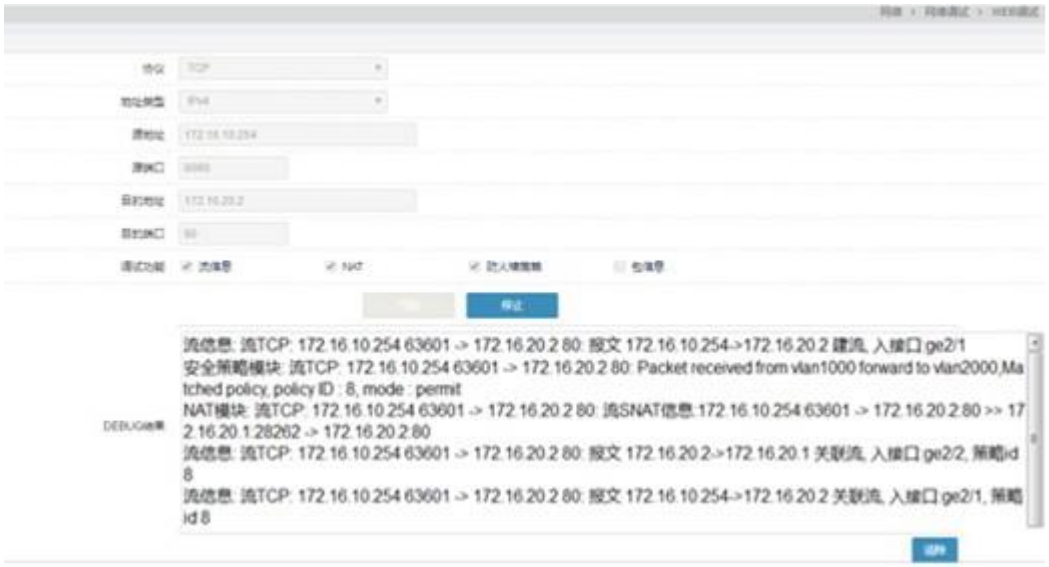
案例组网图：



配置步骤：

1．进入**网络>网络调试>WEB 调试**，**协议**下拉框中选择 TCP，**IP 类型**下拉框中选择 IPv4，源地址选填写客户端地址，目的地址为 http server 地址，目的端口为 80，**调试功能**复选框中选择**流信息、NAT 和防火墙策略**，如下图：

2． 点击**开始**，如下图：


流信息: 流TCP: 172.16.10.254 63601 -> 172.16.20.2 80: 报文 172.16.10.254->172.16.20.2 建流, 入接口 ge2/1
安全策略模块: 流TCP: 172.16.10.254 63601 -> 172.16.20.2 80: Packet received from vlan1000 forward to vlan2000,Matched policy, policy ID : 8, mode : permit
NAT模块: 流TCP: 172.16.10.254 63601 -> 172.16.20.2 80: 流SNAT信息:172.16.10.254 63601 -> 172.16.20.2 80 >> 172.16.20.1 28262 -> 172.16.20.2 80
流信息: 流TCP: 172.16.10.254 63601 -> 172.16.20.2 80: 报文 172.16.20.2->172.16.20.1 关联流, 入接口 ge2/2, 策略id 8
流信息: 流TCP: 172.16.10.254 63601 -> 172.16.20.2 80: 报文 172.16.10.254->172.16.20.2 关联流, 入接口 ge2/1, 策略id 8

38 第38章 路由跟踪

38.1 路由跟踪概述

为了了解数据包在设备中的详细流程，方便用户配置和管理，设备中提供了路由跟踪功能。通过配置路由跟踪，用户能模拟一个数据包在设备中进行全流程处理，并根据相应的结果定位问题，方便用户调整配置，了解设备处理概况。

路由跟踪的输出结果主要包含：模拟的数据包经过的功能模块及处理结果。

目前支持的功能模块主要包括：安全策略的匹配，地址池的调用，会话控制策略的匹配，防护策略的匹配，用户认证策略的匹配，流量或连接数限制检查结果，NAT 地址转换，路由查询结果。

路由跟踪只显示数据包经过的功能模块。

38.2 配置路由跟踪

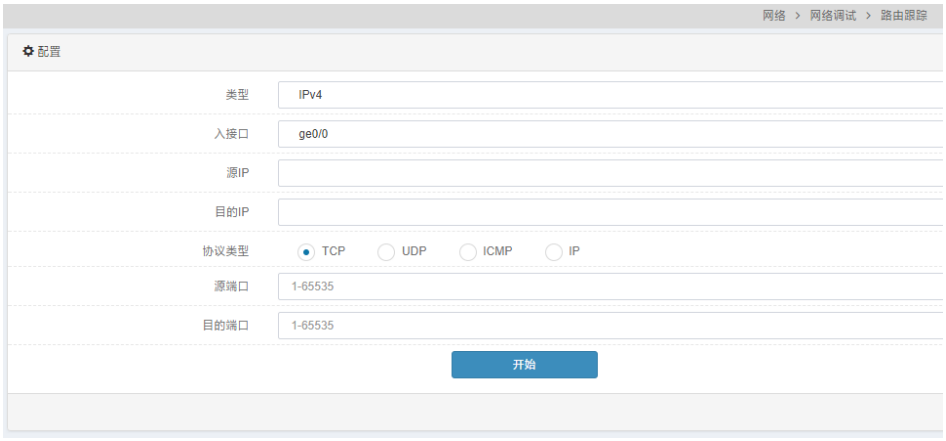
38.2.1 配置路由跟踪的基本要素

路由跟踪的基本要素包括数据流的地址类型、入接口、源地址、目的地址、协议类型。不同的协议类型的配置略有差异。

用户必须指定所有的基本要素，以模拟一个数据包。

配置步骤：

1. 进入**网络>网络调试>路由跟踪**，如下图：



参数说明：

类型：数据包的的协议类型，可以组建 IPv4 或 IPv6 协议类型的数据包。

入接口：数据包的流入方向，可以指定某个物理口、vlan 或者 trunk。

源地址：数据包的源地址。

目的地址：数据包的目的地址。

协议类型：数据包的四层协议类型，包括 TCP、UDP、ICMP、IP。

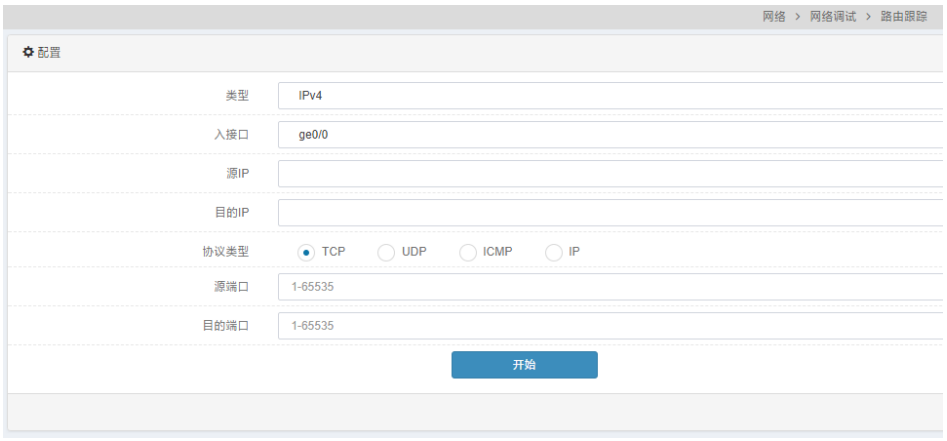
2. 配置完毕后，点击**开始**。

38.2.2 配置TCP(或UDP)协议类型的路由跟踪

协议类型为 TCP(或 UDP)的路由跟踪，需要填写源端口和目的端口参数。

配置步骤：

1. 进入**网络>网络调试>路由跟踪**，在协议类型中选择 TCP(或 UDP)，如下图：



源端口：数据包的源端口。

目的端口：数据包的目的端口。

2. 点击**开始**。

38.2.3 配置ICMP协议类型的路由跟踪

协议类型为 ICMP 的路由跟踪，需要填写类型、代码。

配置步骤：

1. 进入**网络>网络调试>路由跟踪**，在协议类型中选择 ICMP，如下图：

类型：ICMP 报文的类型。

代码：ICMP 报文的代码字段。

2. 点击**开始**。

38.2.4 配置IP协议类型的路由跟踪

协议类型为 IP 的路由跟踪，需要填写协议参数。

配置步骤：

1. 进入**网络>网络调试>路由跟踪**，在协议类型中选择 IP，如下图：

协议：数据流的四层协议号，取值范围为 1~255。

2. 点击**开始**。

38.3 配置案例

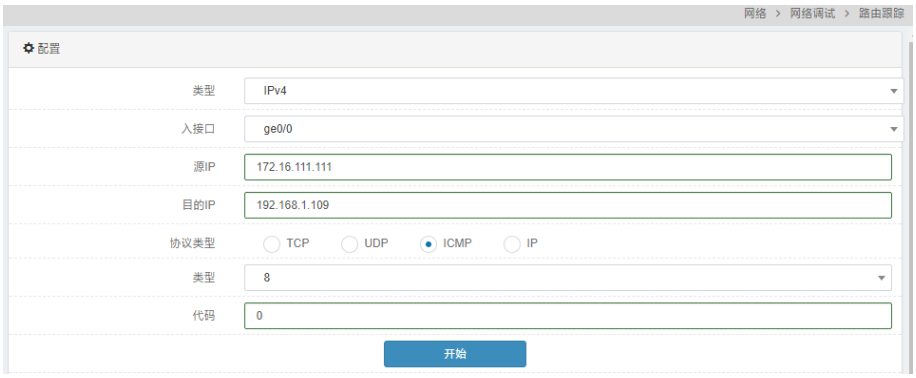
38.3.1 案例1：配置IPv4路由跟踪

案例描述

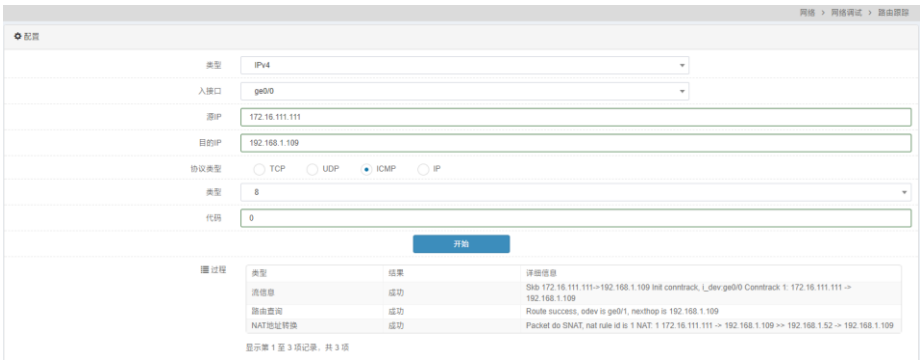
配置 IPv4 的路由跟踪，模拟 172.16.111.111 ping 192.168.1.109 的数据包。

配置步骤：

1. 进入**网络>网络调试>路由跟踪**，在协议类型中选择 ICMP，填写参数，如下图：



2. 点击**开始**，完成配置，如下图：



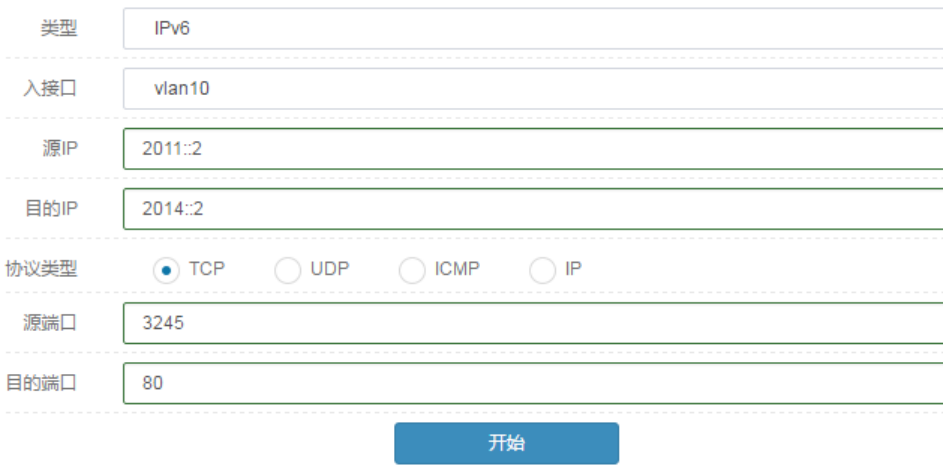
38.3.2 案例2：配置IPv6路由跟踪

案例描述：

配置 IPv6 的路由跟踪，模拟 2011::4 访问 2014::2 的 80 端口的数据包。

配置步骤：

1. 进入**网络>网络调试>路由跟踪**，在协议类型中选择 TCP，填写参数，如下图：



2. 点击开始，完成配置如下图：

39 第39章 诊断

39.1 诊断功能概述

诊断功能为网络调试中的一个子功能。主要功能有 3 种：ping 诊断、traceroute 诊断、TCP 诊断、ping6。

- Ping 诊断：向一个目的地址发送 ping 报文。
- TCP 诊断：向一个目的地址发送 SYN 报文。
- Traceroute 诊断：定位设备和目标计算机之间的所有路由器。支持选定 UDP 端口。
- Ping6 诊断：向一个 IPv6 目的地址发送 ping 报文。

39.2 配置

39.2.1 配置traceroute诊断

配置步骤：

1. 进入**网络>网络调试>诊断**，如下图：

参数说明：

诊断配置：选择诊断类型。

目标地址：需要探测的目标地址。

启用 UDP 端口探测：UDP 端口探测开关。

端口：配置报文发送的端口号。

2. 配置完毕后，点击**诊断**。

39.2.2 配置ping诊断

配置步骤：

1. 进入**网络>网络调试>诊断**，如下图：

参数说明：

诊断配置：选择诊断类型。

目标地址：需要探测的目标地址。

数据长度：发送报文携带的数据长度。

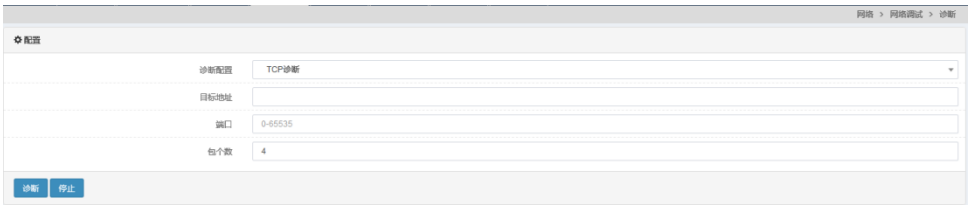
包个数：发送的报文个数。

2. 配置完毕后，点击**诊断**。

39.2.3 配置TCP诊断

配置步骤：

1. 进入**网络>网络调试>诊断**，如下图：



参数说明：

诊断配置：选择诊断类型。

目标地址：需要探测的目标地址。

端口：配置报文发送的目的端口号。

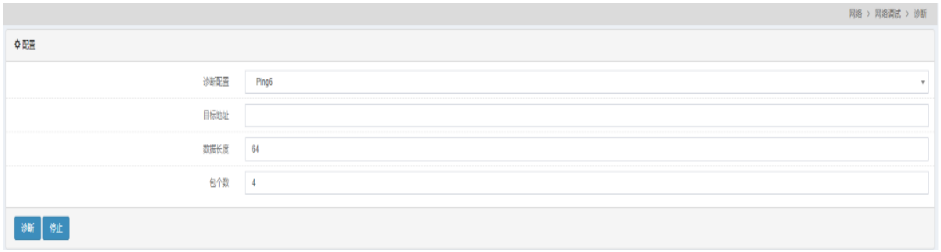
包个数：发送的报文个数。

2. 配置完毕后，点击**诊断**。

39.2.4 配置ping6诊断

配置步骤：

1. 进入**网络>网络调试>诊断**，如下图：



参数说明：

诊断配置：选择诊断类型为 Ping6。

目标地址：输入需要探测的 IPv6 目标地址。

数据长度：发送报文携带的数据长度。

包个数：发送的报文个数。

配置完毕后，点击**诊断**。

39.3 配置案例

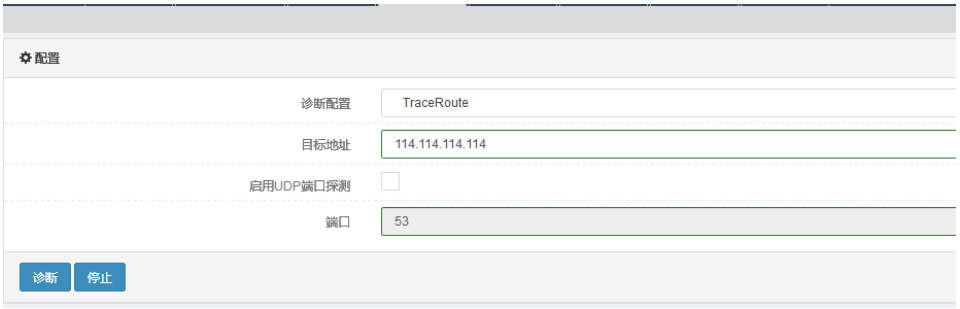
39.3.1 配置案例1：对网络进行traceroute诊断

案例描述

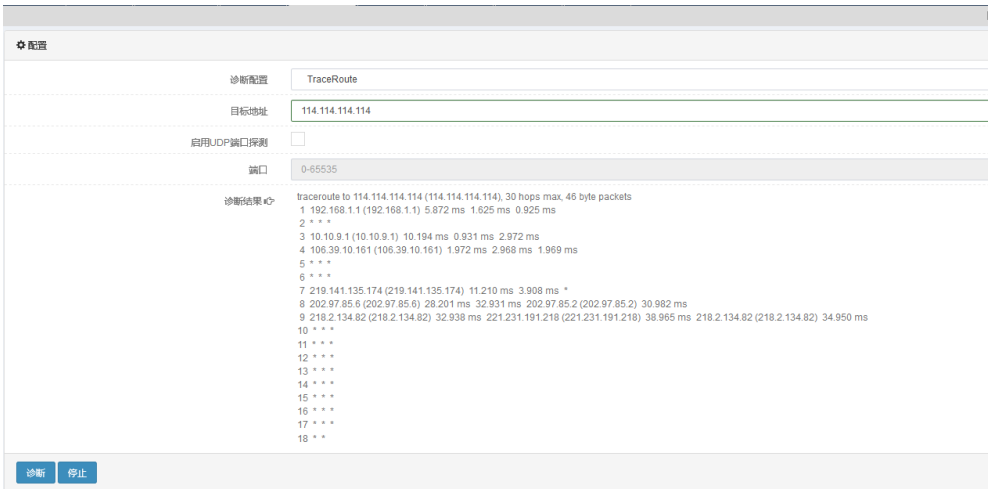
对 114.114.114.114 进行 traceroute 探测。

配置步骤：

4. 进入**网络>网络调试>诊断**，如下图所示：



5. 点击**诊断**



若不想等待完整结果，可以点击停止。将返回现已探测出的结果。

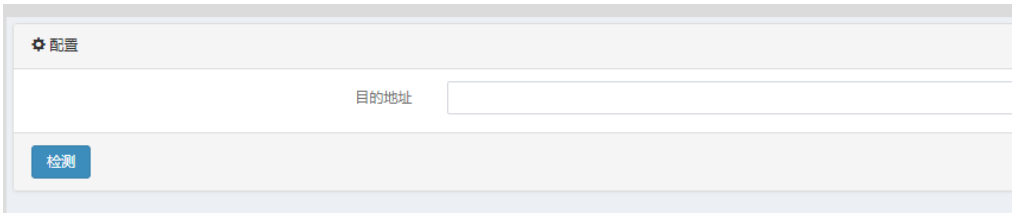
40 第40章 PMTU

40.1 PMTU概述

使用 pmtu 功能，用户可以通过配置目的 IP 地址去探测到达这个 IP 地址的路径上最大传输单元。

40.2 PMTU配置

进入**网络>网络调试>pmtu**，可看到如下界面。



目的地址：可根据选择的地址类型，指定探测的目的地址。

检测：点击检测后开始探测。

40.3 配置案例

案例描述

探测到 192.168.1.1 路径上最大传输单元。

配置步骤：

1.进入**网络>网络调试>pmtu**，填写目的地址：

2.点击**检测**，进行探测，探测结果：


配置
目的地址
192.168.1.1
检测结果
1: 192.168.1.246 0.357ms pmtu 1500
1: 192.168.1.1 9.669ms reached
1: 192.168.1.1 3.182ms reached
Resume: pmtu 1500 hops 1 back 64
检测

41 第41章 自定义抓包

41.1 自定义抓包概述

使用自定义抓包功能，用户可以通过指定过滤条件，抓取实际网络中的数据包，便于分析网络状态，追踪网络问题。

41.2 自定义抓包配置

进入**网络>网络状态>自定义抓包**，可看到如下界面。可通过配置过滤条件，抓取指定的数据包。

协议：指定抓包的传输层协议。默认为所有。

如果指定为 TCP 或者 UDP，可以指定源端口和目的端口号（如果不填，默认为所有端口号）；

如果指定为 ICMP，可以指定 TYPE 和 CODE（如果不填，默认为所有 ICMP 协议的报文）；

如果指定为 OTHER，可指定传输层协议号（如果不填，默认为除去 TCP, UDP, ICMP 其他的所有传输层协议报文）。

抓包方式：可以指定抓某端的报文。

发送端：抓取发送端发出和接收到的报文；

接收端：抓取接收端发出和接收的报文；

所有：不分方向，全部抓取。

地址类型：可选择抓取报文的网络层协议类型，可为 IPv4，或者 IPv6，或

者为所有。（指定为所有时，不允许指定地址）

源地址：可根据选择的地址类型，指定抓取发起端报文的源地址。（支持主机地址格式 A.B.C.D，地址范围格式 A.B.C.D-E.F.G.H，网络地址格式 A.B.C.D/M，如果不填，默认为该类型的所有地址。）

目的地址：可根据选择的地址类型，指定抓取发起端报文的目的地址。（支持主机地址格式 A.B.C.D，网段地址格式 A.B.C.D-E.F.G.H，网络地址格式 A.B.C.D/M，如果不填，默认为该类型的所有地址。）

开始：点击开始后开始抓取报文

停止：点击停止后停止抓包（当报文抓满 10 个后会自动停止抓取）。

注意

3. 抓包文件每个最大为 10M，超过 10M 后会自动保存为下一个文件。
4. 最多保存 10 个抓包文件，抓满 10 个文件后会自动停止抓取。
5. 如果已有 10 个抓包文件，想要再次开始抓包之前，必须删除或者清空，才能正常开始抓取。
6. 如果是多连接协议，比如 FTP 协议，指定控制连接的过滤条件，也会抓取对应的数据连接的报文。
7. 源地址和目的地址始终为连接的初始源地址和目的地址。

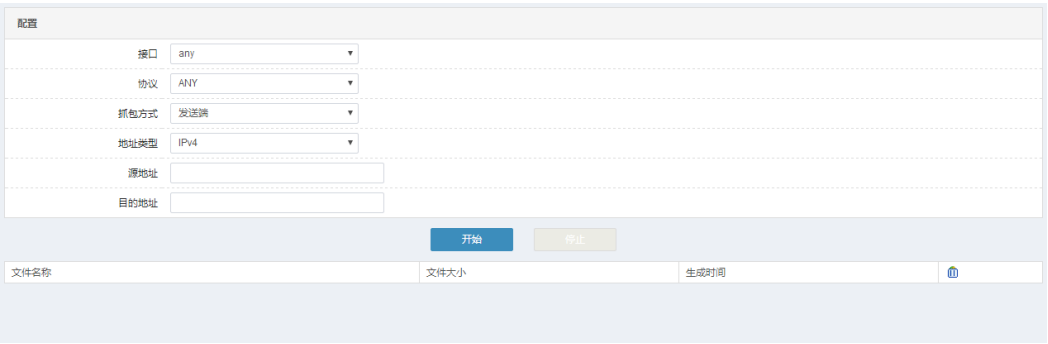
41.3 配置案例

案例描述

抓取本机 6.6.6.6 发出的数据包。

配置步骤：

1.进入**网络>网络调试>自定义抓包**，进行过滤条件的设置：



注：地址和端口输入框，如果不设置任何值的话，就相当于指定了所有该类型的地址和端口。

2.点击**开始**，进行抓包，当抓取一段时间后，点击**停止**，可看到已抓取的报文**:**

文件名称	文件大小	生成时间	
capture_file_0.cap	4.27 KB	Thu Feb 5 01:18:04 2009	

3.点击报文后的  ，可下载报文进行分析。下载后可使用 wireshark 软件打开查看。

42 第42章 SDWAN 策略

42.1 SDWAN策略概述

SDWAN 策略，是指在 SDWAN 组网环境下，符合指定条件的报文，在多出口链路的情况下，根据链路的实时质量选择出口下一跳。根据 SDWAN 策略选路的优先级和策略路由相同，高于路由选路。

链路质量检查用来探测 SDWAN 策略的下一跳的链路质量。

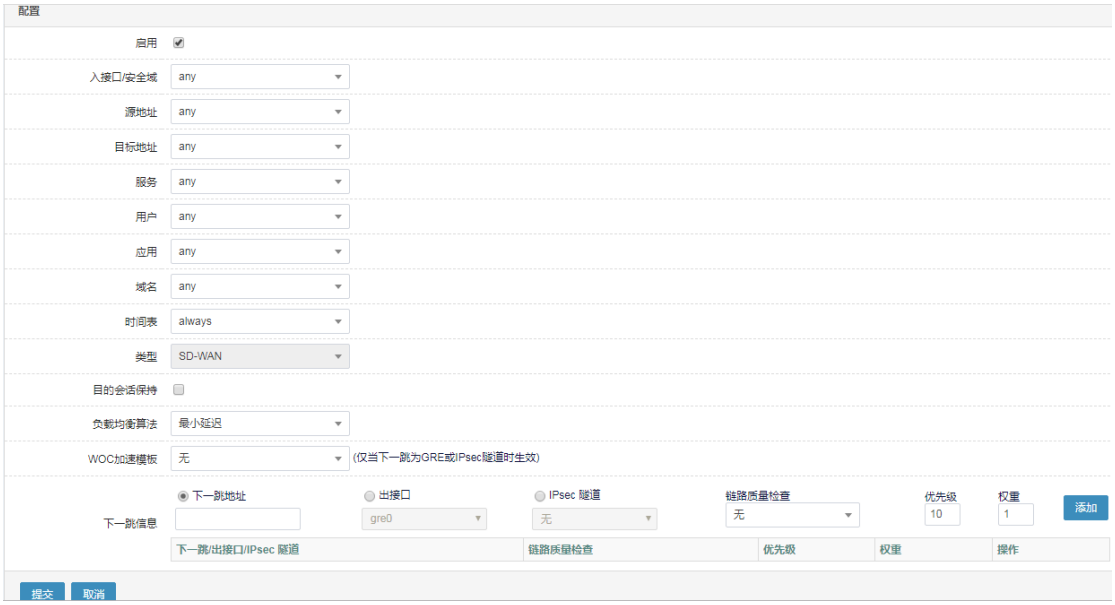
链路质量检查通过周期性主动发送 ICMP 探测报文的方式获得 SDWAN 策略各下一跳的延迟、抖动、丢包率等信息，以便 SDWAN 策略能够选择出更优质可靠的链路发送数据。

配置链路质量检查前，请确保被探测的目的 IP 能够正常回复 ICMP 报文。

42.2 配置SDWAN策略

42.2.1 创建SDWAN策略

1. 配置 SDWAN 策略之前，需要配置相应的地址对象、服务对象应用对象、时间对象和链路质量检查模板。
2. 进入 **SDWAN>SDWAN 策略>SDWAN 策略**，点击**新建**。



参数说明：

启用：是否启用本条 SDWAN 策略，只有启用的情况下，该 SDWAN 策略才会参与匹配。

入接口：指定 SDWAN 策略匹配的入接口，只有从该接口进入的报文才会进入到 SDWAN 策略选路流程中，Any 表示所有接口。

源地址：指定 SDWAN 策略匹配的源地址或网段，any 表示所有源地址。

目的地址：指定 SDWAN 策略匹配的目的地址或网段，any 表示所有目的地址。

服务：指定 SDWAN 策略匹配的服务对象, any 表示所有目的服务。

用户：指定 SDWAN 策略匹配的用户对象，any 表示所有用户。

应用：指定 SDWAN 策略匹配的应用对象，any 表示所有应用。

域名：指定 SDWAN 策略匹配的域名对象，any 表示所有域名。

时间表：指定 SDWAN 策略匹配的时间对象，always 表示全部时间。

类型：指定选路策略的类型为 SDWAN 策略。

目的会话保持：是否启用基于目的地址的会话保持功能。

负载均衡算法：选择下一跳的算法，支持最小延迟、最小抖动、最小丢包率、轮询、加权轮询、源 IP 哈希、源 IP 和端口哈希、链路复制等。

WOC 加速模板：指定符合匹配条件的流量要引用的 WOC 加速模板。

下一跳地址：指定出口链路的下一跳 IP 地址。

出接口：指定路由的出接口。

IPSEC 隧道：指定出口链路是 IPSEC 隧道。

链路质量检查：引用链路质量检查模板，用于检查出口链路的质量。

优先级：下一跳的优先级，范围 1 到 100。

权重：下一跳的权重，范围 1 到 255。

3. 点击**提交**。

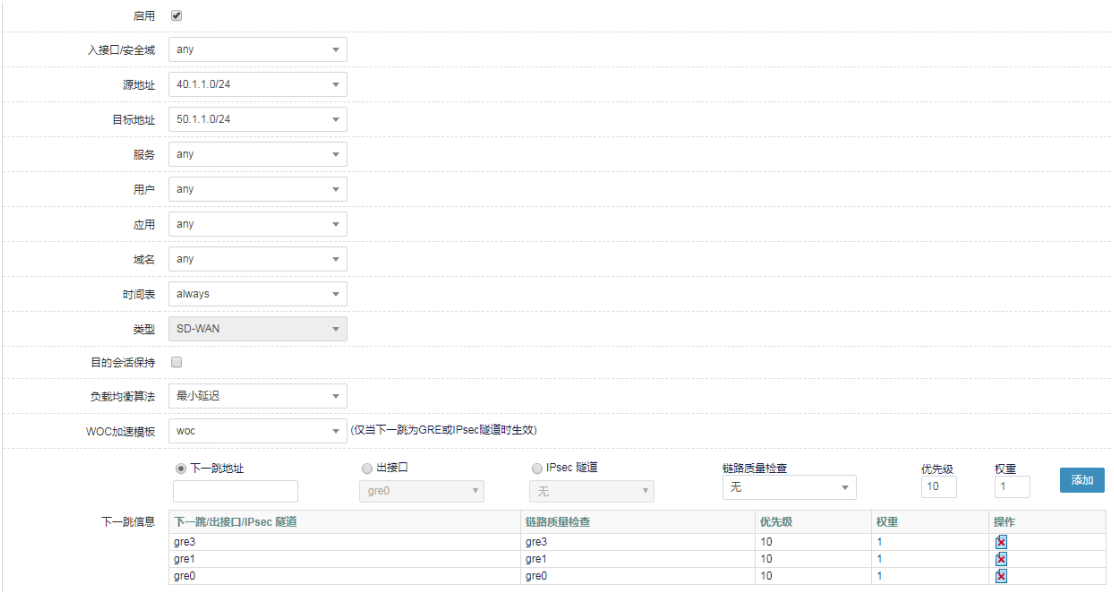
1. SDWAN 策略选路的优先级和策略路由相同，高于普通路由选路。
2. SDWAN 策略依据接口、源地址、目标地址等作为冲突检查。如果配置重叠或者出现冲突，则会提示配置错误。
3. 优先级越高下一跳越优，高优先级链路的链路状态都不可用后，会自动切换到低优先级下一跳转发。当高优先级故障恢复后，则再次切换到高优先级下一跳转发。
4. 链路质量检查对象若为非下一跳地址，注意设备要有到该地址的路由。

5. 对于设备直连的路由网段不匹配 SDWAN 策略转发而是查直连路由转发。
6. WOC 加速模板、链路复制算法，都是只有当下一跳为 GRE 接口或 IPSEC 隧道的情况下，才会生效。
7. 当使用最小延迟、最小抖动和最小丢包率算法时，下一跳必须引用链路质量检查模板才能获取到链路质量值并依据算法调度。

42.2.2 编辑SDWAN策略

1．进入 **SDWAN>SDWAN 策略>SDWAN 策略**，点击 **ID** 字段可编辑对应策略路由。

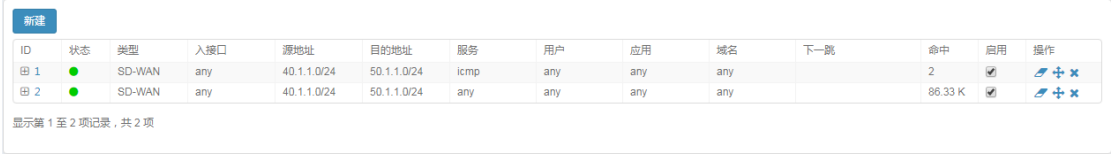
2．进入 SDWAN 策略编辑界面，如下图：



3．编辑完成后点击**更新**按钮。

42.2.3 删除SDWAN策略

1．进入 **SDWAN>SDWAN 策略>SDWAN 策略**，如下图：

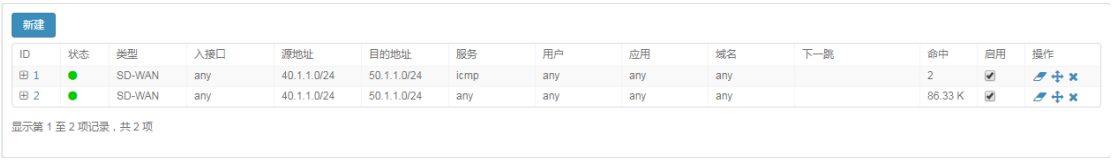


2．点击 删除对应 SDWAN 策略

3．点击**确定**删除 SDWAN 策略。

42.2.4 SDWAN策略顺序调整

1. 进入 **SDWAN>SDWAN 策略>SDWAN 策略**，如下图：



2. 点击 调整对应 SDWAN 策略的匹配优先级。

规则 ID：需要被移动的策略 ID 号。

移动到：参考策略 ID 号。

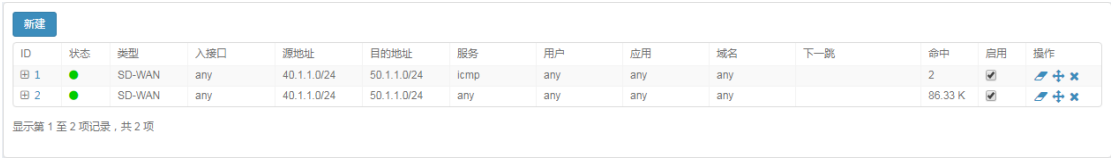
之前：移动到参考策略 ID 之前。

之后：移动到参考策略 ID 之后。

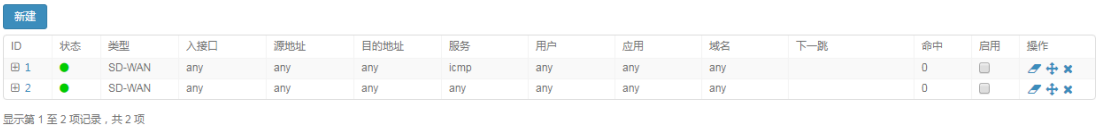
流量匹配 SDWAN 策略时，按照页面顺序向下匹配，命中后不再进行后续策略匹配。当所有的 SDWAN 策略都无法匹配时，则匹配路由转发。

42.2.5 SDWAN策略启用禁用

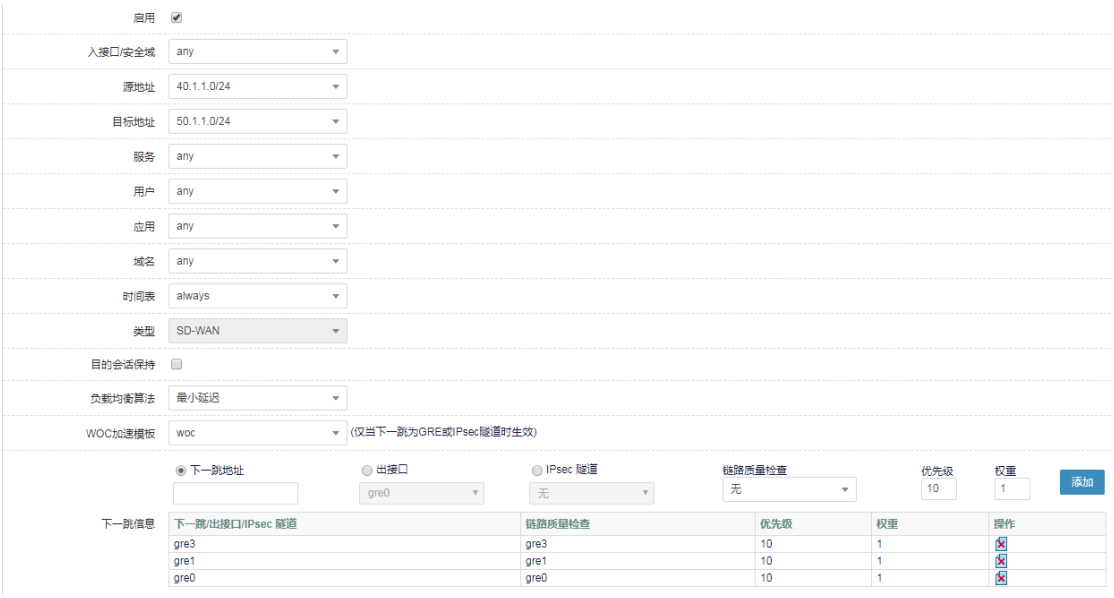
1．进入 **SDWAN>SDWAN 策略>SDWAN 策略**，勾选启用按钮，如下图，策略启用。



2．进入 **SDWAN>SDWAN 策略>SDWAN 策略**，不勾选启用按钮，策略禁用。



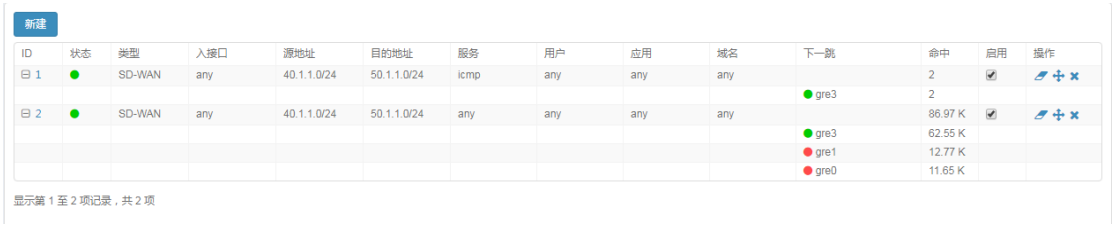
3．进入 **SDWAN>SDWAN 策略>SDWAN 策略**，点击 **ID** 字段编辑对应 SDWAN 策略，勾选启用按钮，点击更新提交。如下图，策略启用。



4．进入 **SDWAN>SDWAN 策略>SDWAN 策略**，点击 **ID** 字段编辑对应策略路由，不勾选启用按钮，点击更新提交。如下图，策略禁用。

42.2.6 查看SDWAN策略列表

1．进入 **SDWAN>SDWAN 策略>SDWAN 策略**，如下图：



2．策略状态：-策略可用，-没有可用下一跳，策略不可用。

3．下一跳状态：-链路状态可调度，下一跳可用-链路状态不可调度，下一跳不可用。

4．点击即可对下一跳进行展开和收缩操作。

5．点击即可重置对应 SDWAN 策略的命中统计。

42.3 配置链路质量检查

进入 **SDWAN 策略>链路质量检查**，点击**新建**。

名称：链路质量检查模板的名称。

探测周期：每周期发送探测报文的个数。

间隔：链路质量检查发送探测包的间隔时间，单位为 100 毫秒。

最大重试次数：当报文连续超时次数达到最大重试次数时，认为当前链路质量探测失败。

超时时间：发送的链路质量探测包在此时间内如果没收到回应包，则判定此报文未收到回复，单位为秒。

目的 IP 地址类型：选择目的 IP 的地址类型，IPv4 或域名。

目的 IP：链路质量检查报文的目的 IP。

覆盖域名：链路质量检查会解析此域名并将其解析结果作为链路质量检查的目的 IP。**源 IP：**指定发送链路质量探测包的源 IP 地址，当链路质量源 IP 地址需要指定时填写此项。

抖动阈值：链路质量检查结果中的链路抖动值超过抖动阈值时认为此链路不可用。单位毫秒。

丢包阈值：链路质量检查结果中的链路丢包值超过丢包阈值时认为此链路不可用。

延时阈值：链路质量检查结果中的链路延时值超过延时阈值时认为此链路不可用。单位毫秒。

配置步骤：

1. 输入**名称**。
2. 输入**目的 IP**。
3. 输入**源 IP**。
4. 输入**抖动阈值**

5. 输入**丢包阈值**
6. 输入**延时阈值**
7. 点击**提交**。

注意

1. 当下一跳类型为接口或者 IPSecVPN 隧道时，必须配置源 IP、目的 IP 或覆盖域名，否则会导致链路质量检查失败。
2. 链路质量检查配置源 IP 时，源 IP 地址必须在接口上存在，否则会导致链路质量检查失败。

42.4 配置案例

42.4.1 SDWAN策略案例

案例描述：

某企业，上海分公司内网地址段 40.1.1.0/24，出口部署 FW1，北京总部内网地址段 50.1.1.0/24，出口部署 FW2，分公司员工需要直接通过内网地址访问总部的 HTTP 服务器。

上海分公司有两条出口链路，分别属于电信、网通，电信的出口公网地址为 10.10.10.10；网通出口的公网地址为 11.11.11.11。

北京总部也有两条出口链路，分别属于电信、网通，电信的出口公网地址为 20.10.10.20；网通出口的公网地址为 21.11.11.12。

上海和北京的两条出口分别使用 gre 和 ipsec 隧道打通，分部和总部之间访问时，选择延时最小的隧道进行通信。

配置步骤：

1. 进入**对象>地址对象>地址节点**，分别创建地址对象**上海分公司、北京总部**。

上海分公司	40.1.1.0/24
北京总部	50.1.1.0/24

2. 进入 **SDWAN>SDWAN 策略>链路质量检查**，创建链路质量检查模板。

   在上海分公司，创建检查模板 **GRE-sh、ipsec-sh**，源和目的 IP 分别配置为隧道两个端点的 IP 地址。


配置
名称
GRE-sh
探测周期
60
(10-1024)
间隔
1
(1-60)百毫秒
最大重试次数
3
(1-10)
超时时间
1
(1-10)秒
目的IP地址类型
IPv4
域名
目的IP
20.10.10.20
源IP
10.10.10.10
抖动阈值
20
(0-1000) ms
丢包阈值
5
(0-100) %
延时阈值
100
(0-1000) ms
更新
取消

使用相同的方法在北京总部，创建链路质量检查模板 **GREbj**、**ipsec-bj**。

grebj 配置的检查模板，源 IP 为：20.10.10.20 目的 IP 为：10.10.10.10

ipsec-bj 配置的检查模板，源 IP 为：21.11.11.12 目的 IP 为：11.11.11.11

3. 进入 **SDWAN>SDWAN 策略>SDWAN 策略**，创建 **SDWAN 策略**。

上海分公司：

目标地址选择北京总部，源地址选择上海分公司，服务选择 http，并引用链路质量检查模板。

北京总部：

目标地址选择上海分公司，源地址选择北京总部，服务选择 http，并引用链路质量检查模板。

42.4.2 链路质量检查案例

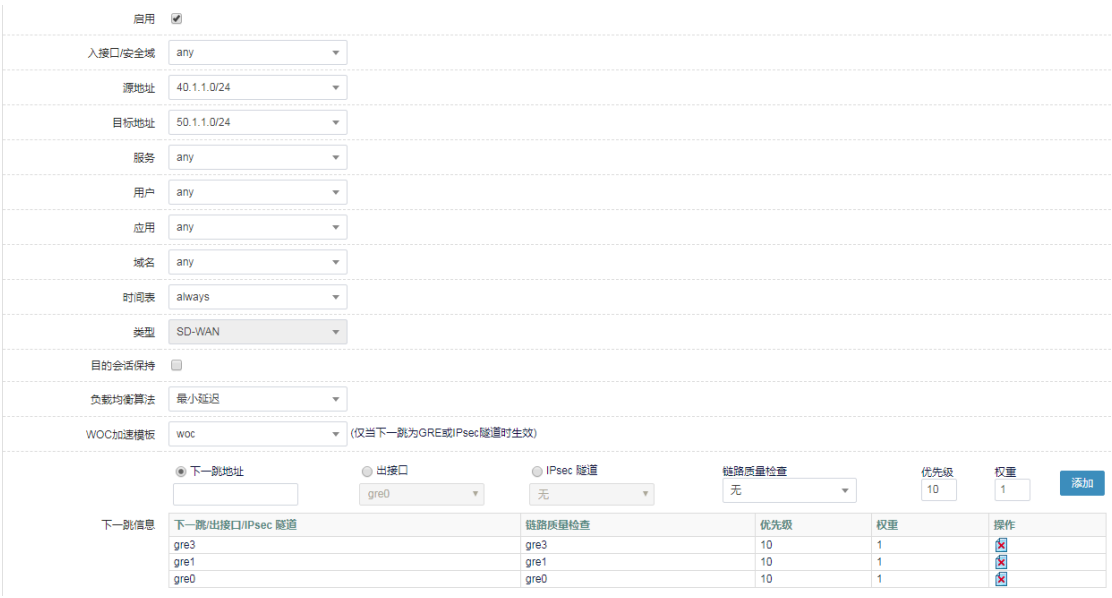
案例描述：

新建一个链路质量检查模板，然后在 SDWAN 策略中引用此模板，对下一跳进行探测，返回探测结果显示。

配置步骤：

1. 新建链路质量检查的模板：

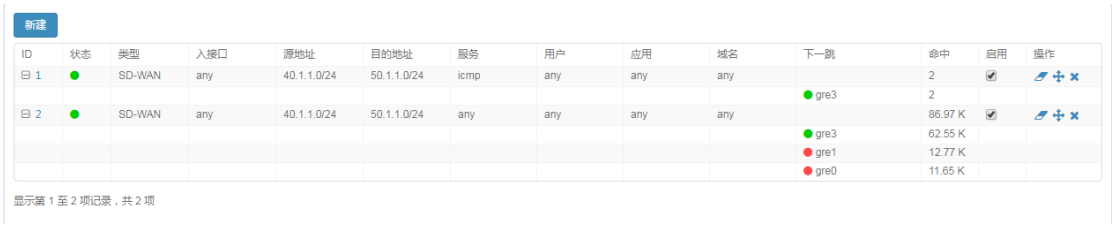
2. 在 SDWAN 策略中引用该模板：



3. 查看链路质量检查结果

如下图所示，下一跳 gre1 不能 ping 通，或抖动、丢包、延时的实时值大于

对应的阈值，状态不可用。



42.5 常见故障分析

42.5.1 SDWAN策略不生效

现象	配置SDWAN策略后没有按照SDWAN策略配置转发到对应下一跳
分析	分析可能为以下几种情况： 1. SDWAN策略没有启用。 2. 匹配上了比本条SDWAN策略优先级更高的SDWAN策略。 3. 检查SDWAN策略下一跳是否配置正确，该下一跳是否有直连路由。 4. 检查SDWAN策略下一跳链路状态检查结果是否为可用。 5. 检查源IP或者目的IP地址是否在地址对象中添加了排除。 6. 检查访问的目的网段是否在设备上有直连路由。 7. 反向报文匹配SDWAN策略，该策略中下一跳对应的出接口是否包含正向报文的入接口。 8. 依据会话信息，检查连接是否为配置开启SDWAN策略之前的连接。 9. 查看命中SDWAN策略的报文是否通过设备进行二层转发。
解决	1. 将SDWAN策略启用。 2. 可以根据需求修改SDWAN策略或者改变SDWAN策略的顺序。 3. 若依据下一跳地址查不到直连路由，则不会从该下一跳出，顺序向下匹配其他SDWAN策略。 4. 检查链路状态不可用的原因，是否下一跳地址不可达，或者链路的延迟、抖动、丢包率大于阈值，或者链路出现故障。 5. 将IP地址从排除地址中删除。 6. 有直连路由情况下，会匹配直连路由转发，不再匹配SDWAN策略，故对设备上有直连路由的网段配置SDWAN策略无效。 7. SDWAN策略的正反向报文分别匹配策略路由选路，但反向报文选路时遵循路径一致性的原则。 8. 为了避免连接断开，SDWAN策略不会影响已建流的流量转发。可以通过重新发起一个连接来确认SDWAN策略是否正确匹配。 9. 只有三层转发的报文才会进SDWAN策略的匹配流程。

42.5.2 SDWAN策略部分下一跳没有命中计数

现象	SDWAN策略添加多个下一跳，流量情况下查看部分下一跳没有命中计数
分析	分析可能为以下几种情况： 1. 检查下一跳地址的优先级，是否有更高优先级的可用下一跳。 2. 检查是否开启了会话保持，查看会话保持设置的掩码是否和访问的目的地址网段相同。 3. 检查是否开启了会话保持，但访问的目的网段通过该下一跳地址出去不可达。为了保证会话保持表项的可靠性，会话保持表项有反向报文后才建立。当存在链路故障导致走该故障链路没有反向报文回应时，则会话保持表项不会建立。
解决	1. 当有可用的高优先级的下一跳时，低优先级下一跳不会参与调度，若希望参与调度，则将优先级调高。 2. 开启会话保持后，相同目的掩码网段的地址都会走相同的下一跳转发，可以依据需要对子网掩码的位数进行适当调整。 3. 检查下一跳出接口链路是否发生故障。

43 第43章 WOC 加速模板

43.1 WOC加速模板概述

WOC 有两个主要功能：双边加速和压缩，采用双边部署的方式，对 VPN 隧道的传输进行加速。在网络状况不佳的情况下，通信双方因为丢包、延迟等问题，会存在极差的网络体验。双边加速功能，使用传输协议优化技术，基于快速重传确认、选择重传等报文级别的控制，发送冗余数据缓解丢包造成的降速，使数据快速可靠的传输。压缩功能，将 IP 报文的数据部分进行压缩，节约了带宽和流量，缩短下载时间。WOC 功能的应用于网络质量不佳的链路上，能加速和优化数据传输，提升用户体验。

43.2 配置WOC加速模板

43.2.1 新建WOC加速模板

配置步骤：

1.进入 **SDWAN>WOC 加速模板**，点击**新建**。

参数说明：

名称：模板名称。

压缩：是否启用压缩功能。

双边加速：是否启用双边加速功能。

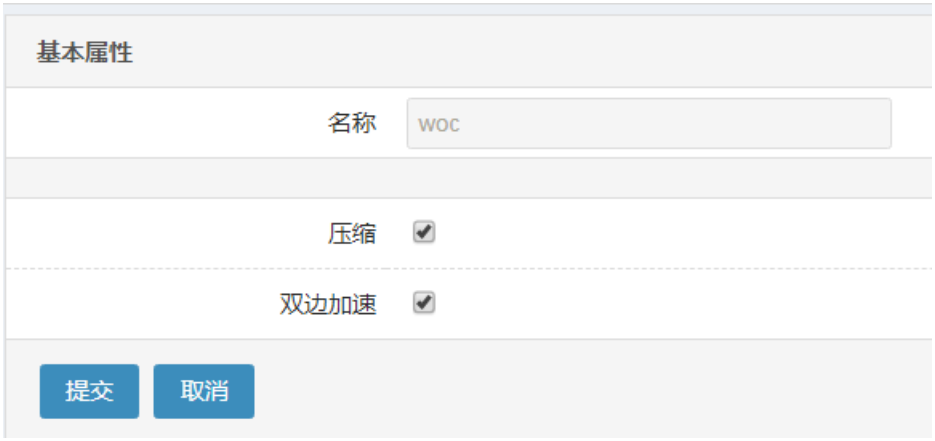
2.配置完毕后，点击**提交**。

43.2.2 编辑WOC加速模板

配置步骤：

1.进入 **SDWAN>WOC 加速模板**，对某条存在的模板点击名称进入编辑界面

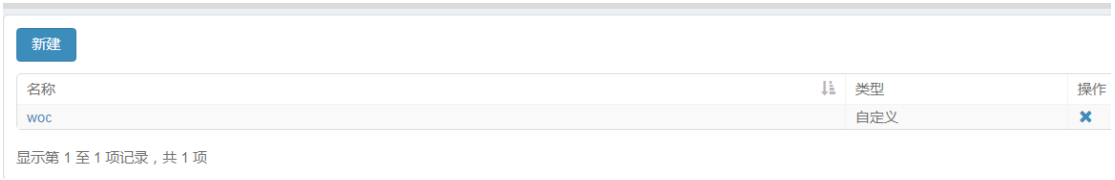
2.可以对模板里面的压缩和双边加速进行编辑修改，修改完毕后点击**提交**。



43.2.3 删除WOC加速模板

配置步骤：

1.进入 **SDWAN>WOC 加速模板**，如下图：



2.点击 删除模板。

注意 被 SDWAN 策略引用的模板不能被删除。

43.2.4 防护策略引用WOC加速模板

配置步骤：

1. 进入 **SDWAN>SDWAN 策略>SDWAN 策略**，点击**新建**，配置匹配条件，选择要引用的 WOC 加速模板

2.点击**提交**。

注意

WOC 功能只对 IPsec 或 GRE 的流量生效。

43.3 WOC加速监控

进入 **SDWAN>监控>SDWAN 策略>WOC 加速统计**，查看相关的统计数据。

43.4 配置案例

参考”SDWAN 策略”的配置案例。

44 第44章 防火墙策略

44.1 防火墙策略概述

为了对数据流进行统一控制，方便用户配置和管理，防火墙设备引入了防火墙策略的概念。

通过配置防火墙策略能够对经过设备的数据流进行有效的控制和管理。当设备收到数据报文时，把该报文的入接口、源地址、目的地址、协议、服务、用户、应用等信息和用户配置的策略匹配，决定是否建立这条数据流，并且把这条流和匹配的策略关联起来，从而确定如何处理该流的后续报文，实现允许、丢弃，决定哪些用户和数据能进出，以及它们进出的时间和地点。

防火墙策略可以进行分组管理，不同组之间的前后顺序和组内规则的排列顺序，共同决定策略的匹配顺序。只对通过设备的数据包进行处理，对于设备本身发出的数据包不进行限制。

对于策略是否生效，可以通过查看策略的命中次数来观察，如果流量匹配了策略，对应策略的命中次数会加 1。

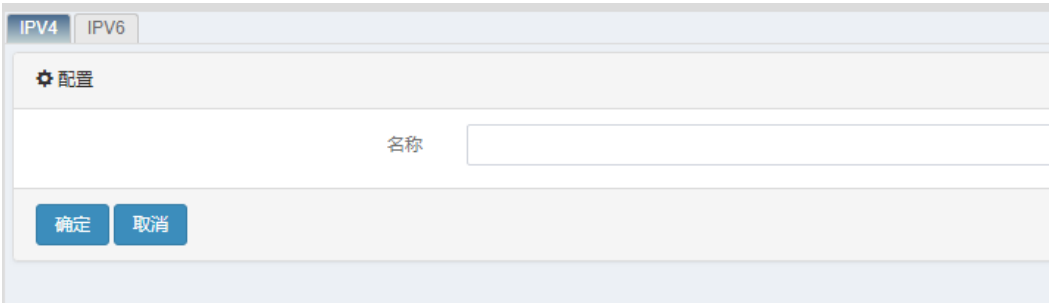
44.2 配置策略组

44.2.1 配置策略组

配置策略组，对防火墙策略进行分组管理，在添加防火墙策略时可以设置策略所属的组，防火墙系统内置的策略组为“default”，可以添加新的策略组。

配置步骤：

1. 进入**策略>防火墙>策略**，选择 IPV4 或 IPV6，点击**新建策略组**， 如下图：



参数说明：

名称：策略组的名称，名称不能重复。

2. 配置完毕后，点击**确定**。

44.2.2 启用策略组

策略组的启用，对应的策略组下所有策略的启用。

配置步骤：

1. 进入**策略>防火墙>策略**，如下图：

2. 勾选**启用**，可以启用一个策略组下的所有策略，取消勾选，策略组下所有策略都将不启用。

当策略组下的策略既有启用，又有不启用配置时，策略组启用按钮显示为不勾选状态。

44.2.3 删除策略组

删除策略组时，对于策略组下的策略，有 2 种操作方法。

配置步骤：

1. 进入**策略>防火墙>策略**，如下图：

2. 点击 ，选择删除方式，删除策略组。

选项说明：

同步删除组内策略：策略组和组内所有策略都删除。

组内策略移到默认组：策略组被删除，组内策略不被删除，移动到默认组。

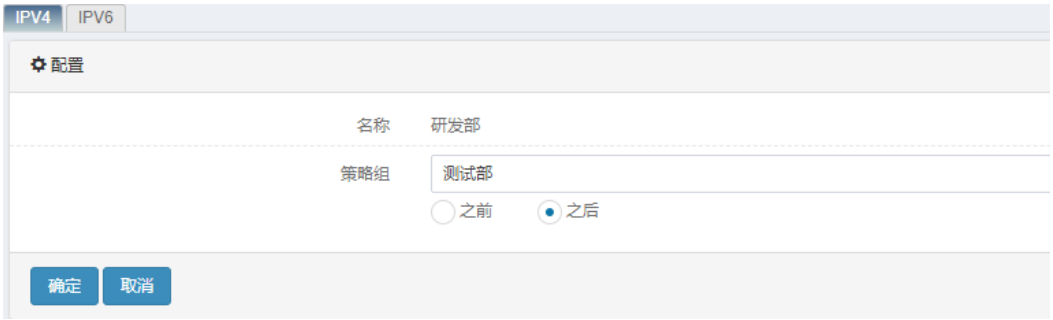
44.2.4 移动策略组

可以通过移动策略组的顺序，改变策略的匹配顺序，default 策略组不能被移动。

配置步骤：

1. 进入**策略>防火墙>策略**，如下图：

2. 点击  ，移动策略组。



参数说明：

名称：需要被移动的策略组。

策略组：参考的策略组。

之前：移动策略组到参考策略组之前。

之后：移动策略组到参考策略组之后。

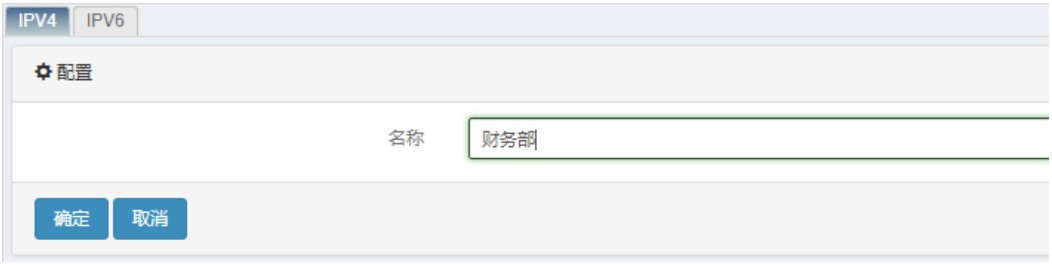
3. 配置完毕后，点击**确定**。

44.2.5 插入策略组

配置步骤：

1. 进入**策略>防火墙>策略**，如下图：

2. 点击  ，插入新的策略组，新插入的策略组将放置于被插入策略组之前。



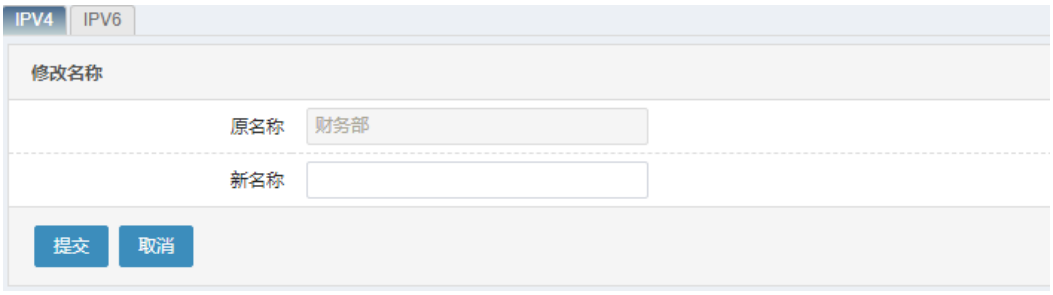
3. 配置完毕后，点击**确定**。

44.2.6 重命名策略组

配置步骤：

1. 进入**策略>防火墙>策略**，如下图：

2. 点击  ，将策略组重新命名。



3. 配置完毕后，点击**提交**。

44.2.7 策略组内策略迁移

配置步骤：

1. 进入**策略>防火墙>策略**，如下图：

2. 点击  ，将策略组内所有的策略移动到另一个策略组内。

参数说明：

名称：将被移动策略的策略组名称。

策略组：策略将移动进入的策略组的名称。

3. 配置完毕后，点击**确定**。

44.3 配置防火墙策略

44.3.1 配置策略的基本要素

防火墙策略的基本要素是匹配条件和动作。匹配条件包括数据流的方向、源地址、目的地址、服务、用户、应用和策略生效的时间范围。其中，数据流的方向通过指定入接口、出接口、源地址、目的地址来确定，服务、用户、应用和时间范围都可以直接引用已定义的对象。

策略的动作有 PERMIT，DENY，不同的动作下又有不同的可选配置，从而决定对符合匹配条件的数据流实现哪些业务。

配置步骤：

1. 进入**策略>防火墙>策略**，选择 IPV4 或 IPV6，点击**新建策略**，如下图：

参数说明：

启用：启用防火墙策略。

名称：防火墙策略的名称，名称可不配置，若指定了名称，则不同策略的名称不能重复。

入接口/安全域：数据流的流入方向，可以指定某个特定接口，也可以指定多个接口，any 表示所有接口。

出接口/安全域：数据流的流出方向，可以指定某个特定接口，也可以指定多个接口，any 表示所有接口。

源地址：数据流的源地址，可以引用已定义的某个或者多个地址对象或地址对象组，any 表示可以源地址可以匹配所有对象。。

目的地址：数据流的目的地址，可以引用已定义的某个或者多个地址对象或地址对象组，any 表示目的地址可以匹配所有对象。

服务：数据流的服务属性，包括协议、源端口和目的端口，可以引用某个或者多个系统预定义服务、自定义的服务对象或服务对象组，any 表示服务可以匹配所有对象。

用户：数据流的用户属性，可以引用某个或者多个已定义的认证用户或用户组，any 表示可以匹配所有用户对象。

应用：数据流的应用属性，可以引用某个或者多个系统预定义应用、自定义的应用对象或应用对象组，any 表示可以匹配所有应用。

时间：策略生效的时间，可以引用某个或者多个已配置的时间对象，always 表示所有时间。

动作：对符合匹配条件的数据流执行的动作，PERMIT 为允许，DENY 为拒绝。

流量统计：只有当策略动作为允许时才可配置，用于统计匹配该策略的流量，可在监控->会话->流量统计->基于防火墙策略中进行查看。

日志：启用日志功能，当策略动作为允许时，可以选择记录会话开始和会话结束的日志，当策略动作为拒绝时，可以记录匹配该拒绝动作的日志。

会话超时时间：匹配该策略的会话的超时时间，单位为秒或者分钟。不配置时，会话保持系统默认的协议的超时时间。

策略组：策略所属的策略组。

描述：防火墙策略的描述，长度限制为 127 个字符，可不配置。

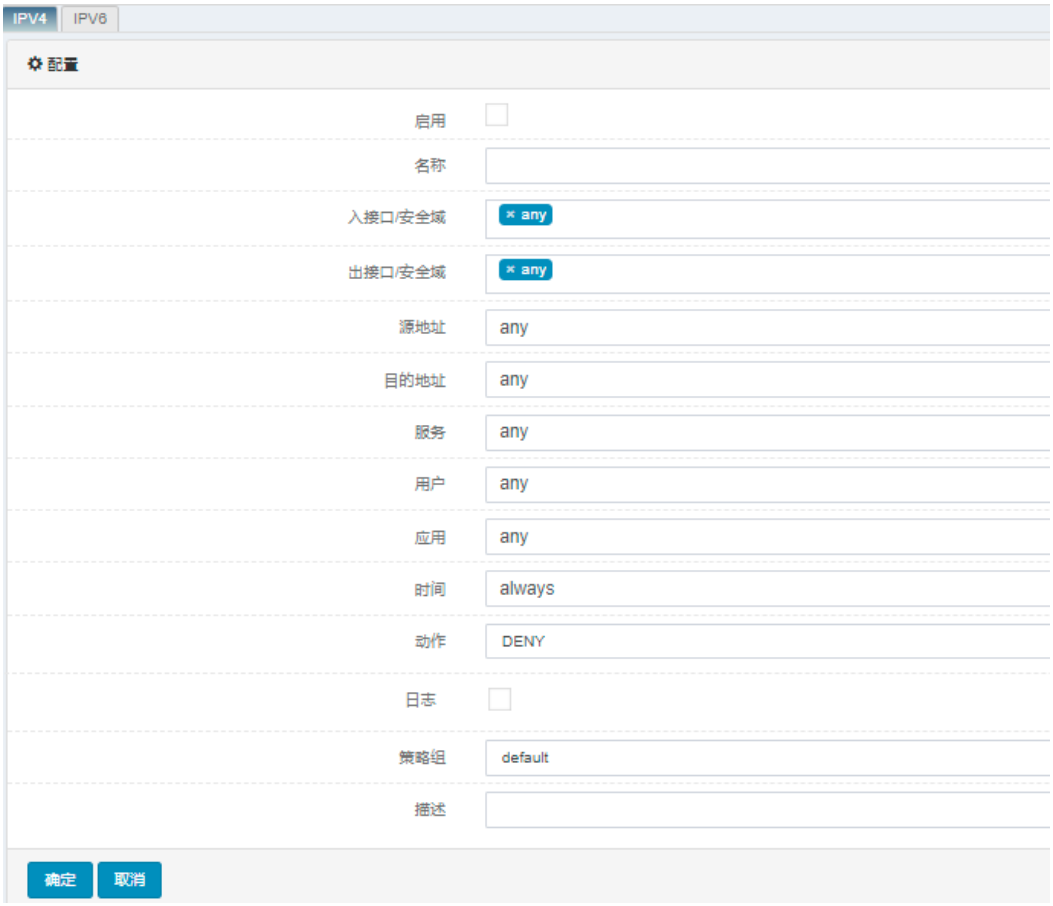
2. 配置完毕后，点击**提交**。

1. 创建一条新的防火墙策略时，引用的地址对象类型必须和当前策略协议类型匹配。
2. 防火墙策略的每个匹配都可以引用多个对象，上限为 16 个。
3. 系统会自动生成防火墙策略的 ID 号，策略 ID 是防火墙策略的唯一标识。不同协议类型的防火墙策略的 ID 是相互独立的。

44.3.2 配置DENY策略

配置步骤：

1. 进入**策略>防火墙>策略**，点击**新建策略**，在**动作**下拉框中选择 **DENY**
   如下图：



参数说明：

日志：启用日志功能，匹配该策略的数据流被阻断的信息会被发往 syslog 服务器或者产生设备本地日志，日志的优先级为通知级别。

2. 配置完毕后，点击**确定**。

44.3.3 配置PERMIT策略

配置步骤：

1. 进入**策略>防火墙>策略**，点击**新建策略**，在**动作**下拉框中选择 **PERMIT**，如下图：

参数说明：

流量统计：统计匹配该策略的流量，可在监控->会话->流量统计->基于防火墙策略中进行查看。

日志：启用日志功能，匹配该策略的数据流创建和拆除的信息会被发往 syslog 服务器或者产生设备本地日志，日志的优先级为信息级别。

会话超时时间：匹配该策略的会话的超时时间，单位为秒或者分钟。不配置时，会话保持系统默认的协议的超时时间。

2. 配置完毕后，点击**确定**。

44.3.4 启用防火墙策略

配置好的防火墙策略必须启用才能使其生效。

配置步骤：

1. 可以在列表页面开启，进入**策略>防火墙>策略**，如下图：

2. 勾选**启用**，可以启用一条策略。

3. 也可以在配置页面直接启用。

注意

策略缺省为不启用，配置后必须手工启用才能使其生效。

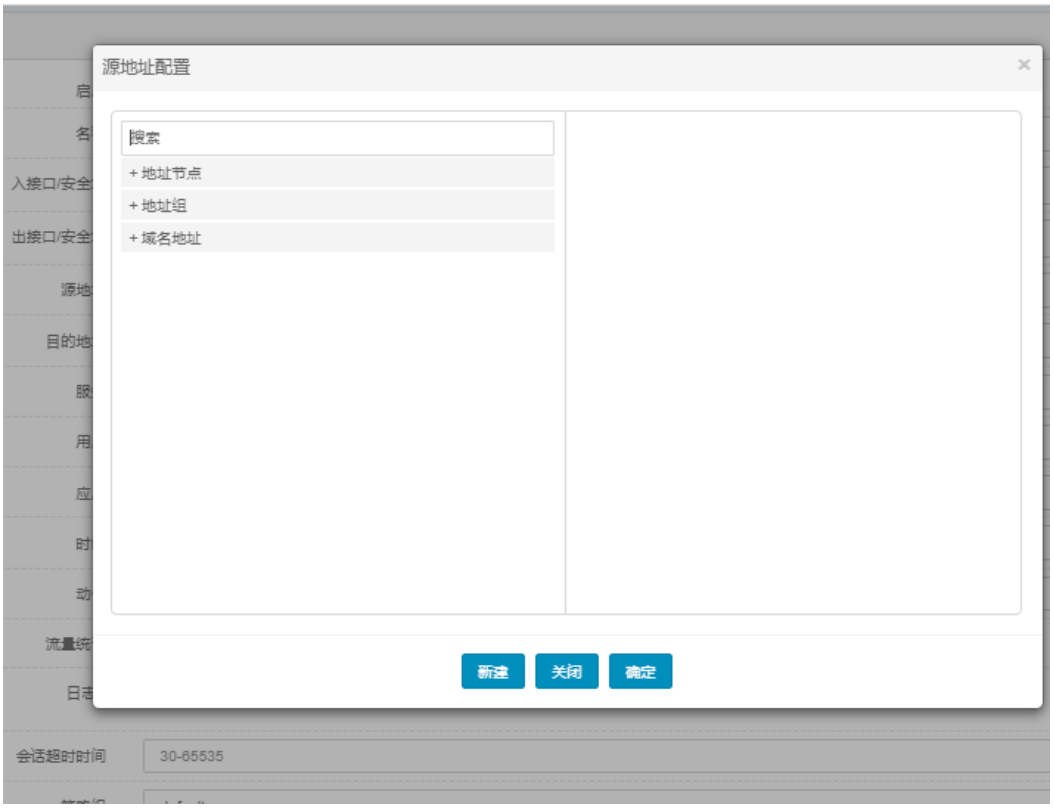
44.3.5 编辑防火墙策略

配置步骤：

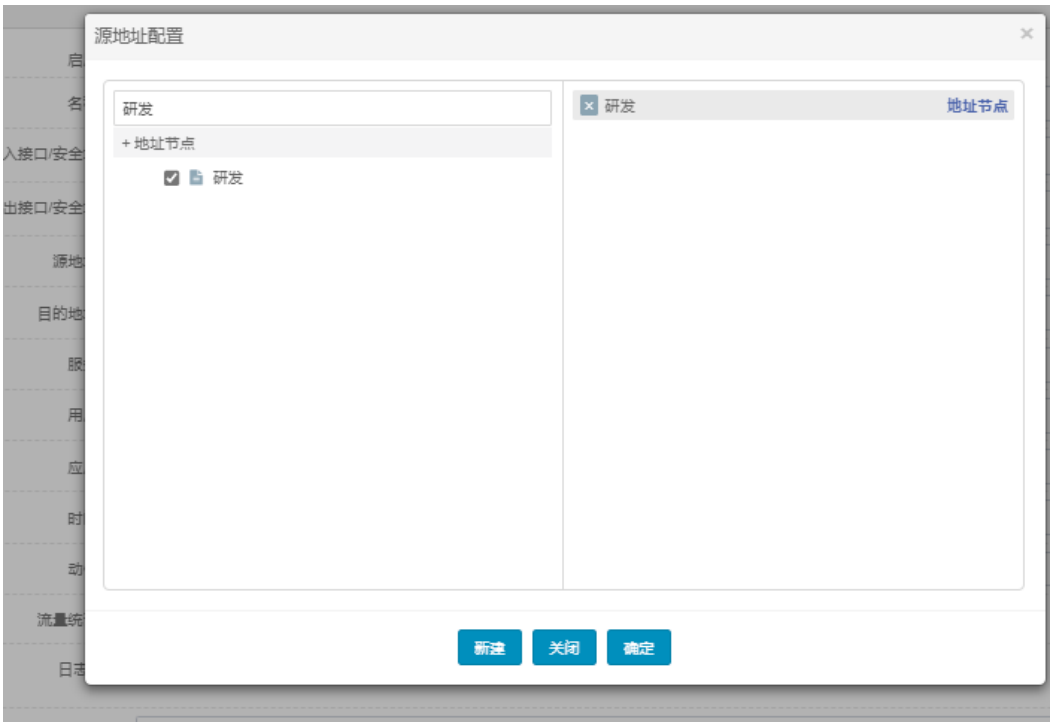
1. 进入**策略>防火墙>策略**，对某条存在的防火墙策略点击策略 ID 号进入

编辑界面，如下图：

2. 点击源地址，修改源地址。

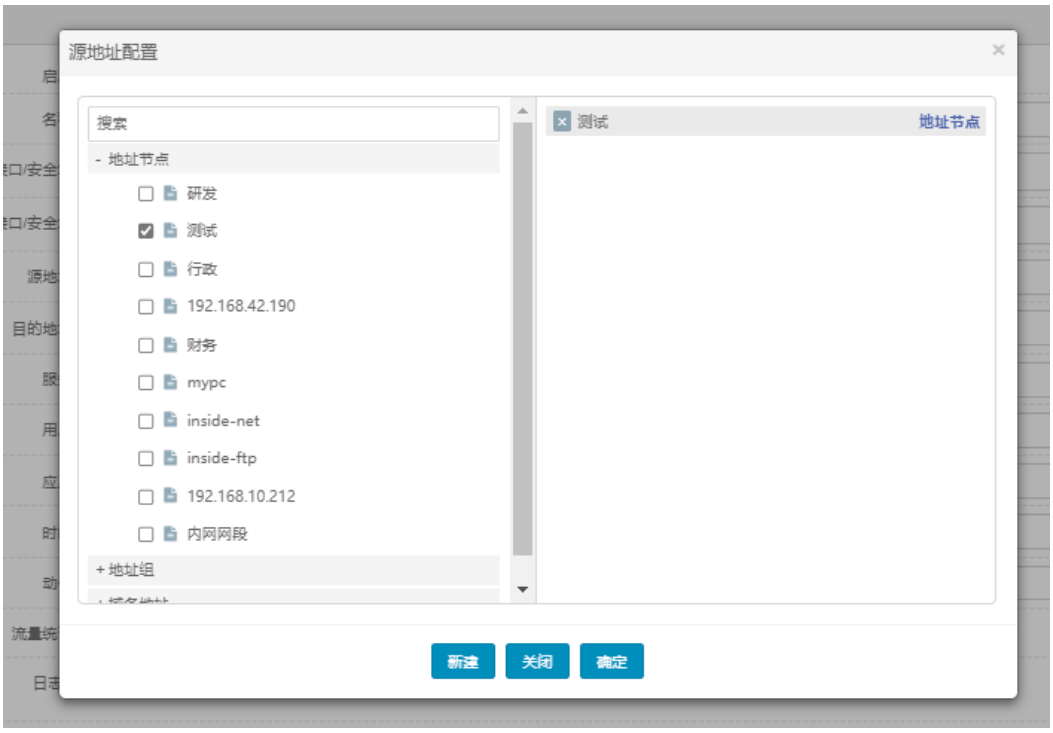


3. 在搜索框中输入地址对象名称，搜索出指定的地址对象，选定即可加入到右侧框中。

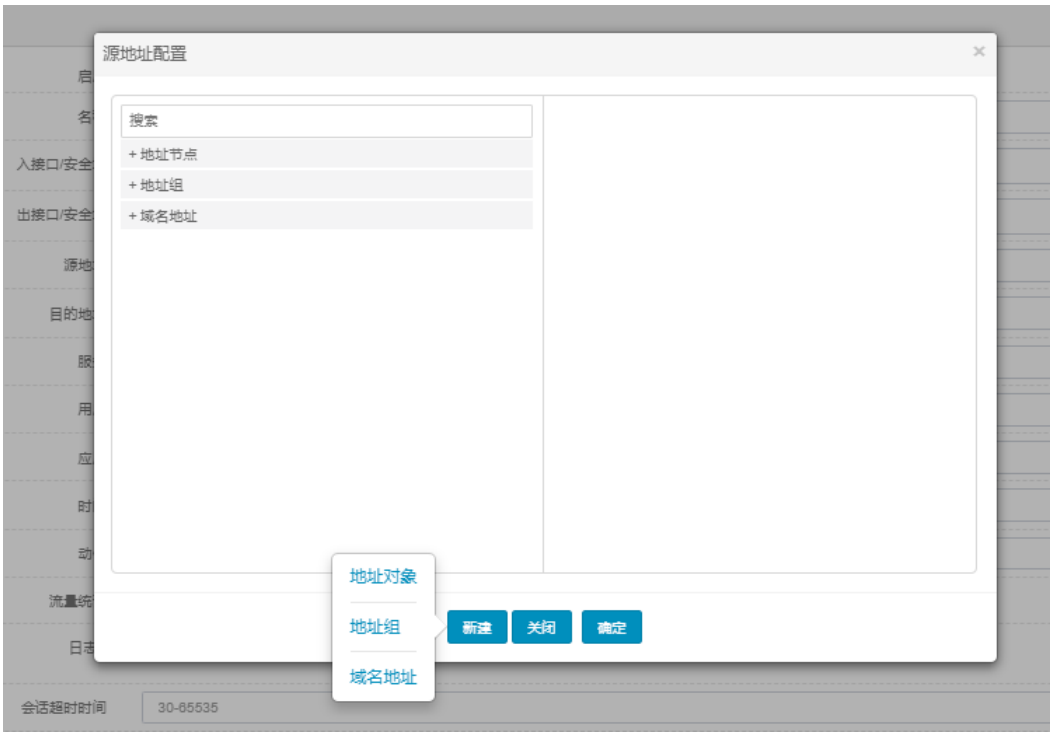


4. 点击地址节点前面的 + 按钮，展开地址对象列表，点击要选择的地址

对象，加入到右侧框中。



5. 点击下面的新建按钮，创建新的地址对象，创建完成后，点击选择新创建的地址对象，加入到右侧框中。



6. 点击**确定**。

44.3.6 删除防火墙策略

配置步骤：

1. 进入**策略>防火墙>策略**，如下图：

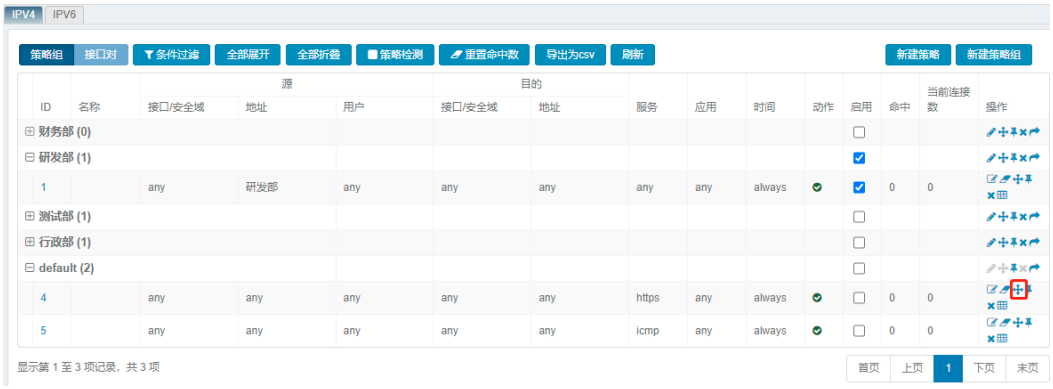
2. 点击✖，删除策略。

44.3.7 移动防火墙策略

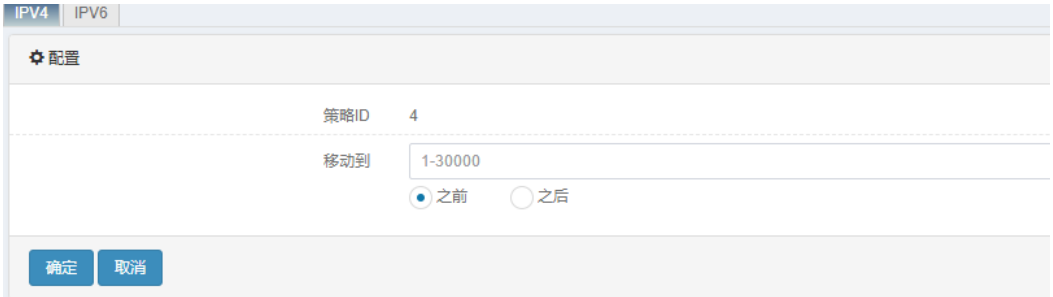
通过移动策略可以调整防火墙策略的顺序，从而使位置在前的策略优先匹配。

配置步骤：

1. 进入**策略>防火墙>策略**，如下图：



2. 点击✣，移动策略。



参数说明：

策略 ID：需要被移动的策略的 ID 号。

移动到（策略 ID）：参考策略的 ID 号。

之前：移动策略到参考策略之前。

之后：移动策略到参考策略之后。

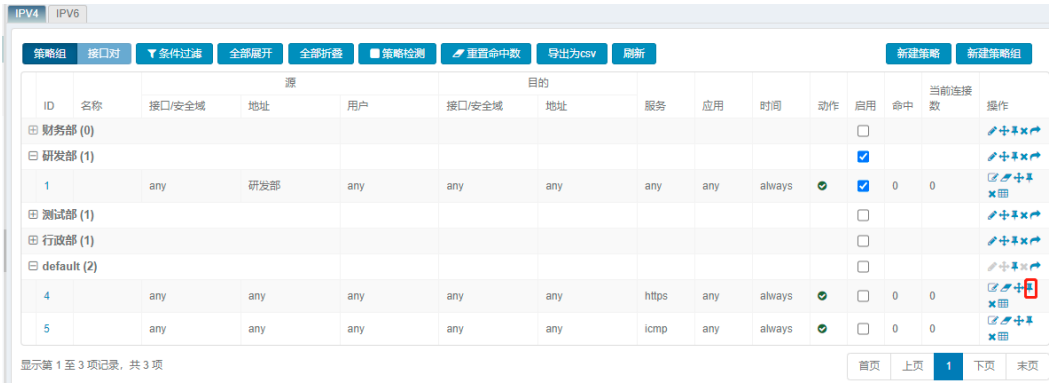
3. 配置完毕后，点击**确定**。

策略不能跨组移动，只能移动同一个组的策略。

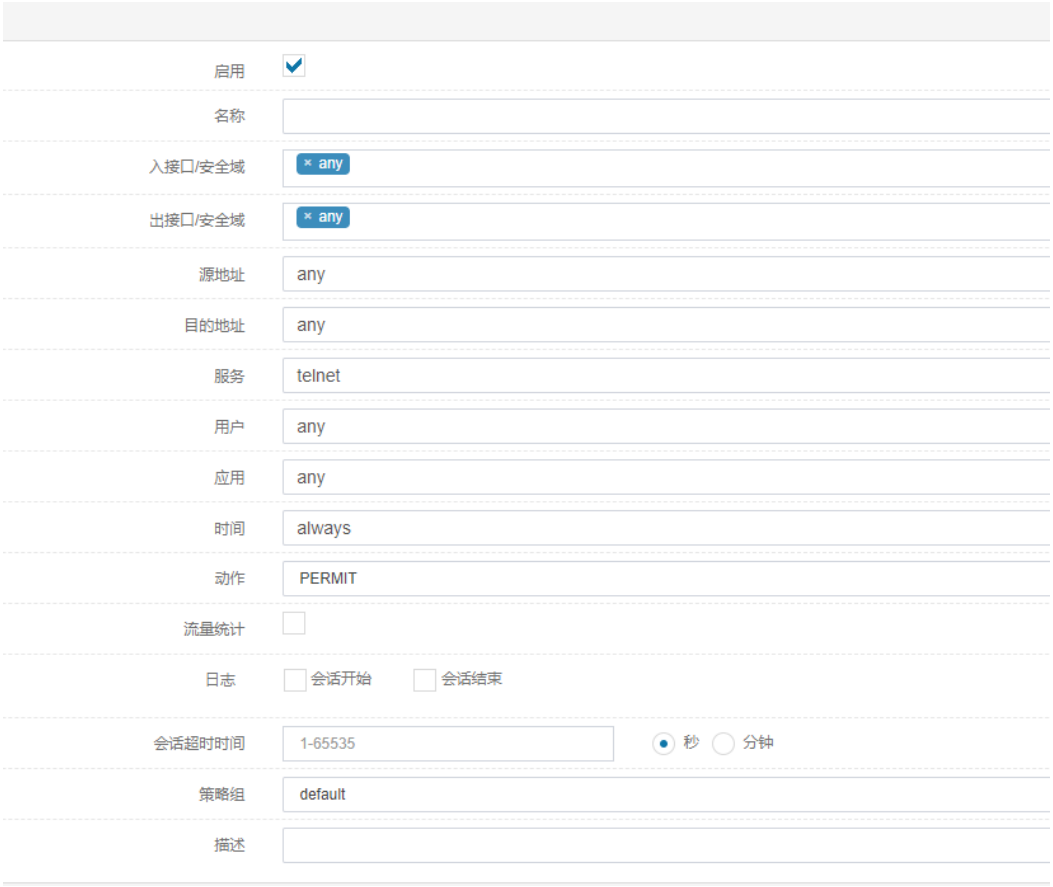
44.3.8 插入防火墙策略

配置步骤：

1. 进入**策略>防火墙>策略**，如下图：



2. 点击，插入一条新的策略到参考策略之前。



3. 配置完毕后，点击**确定**。

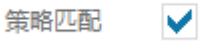
44.3.9 策略配置模块

在策略配置模块可以开启或者关闭整个策略匹配模块，也可以设置策略全部不匹配时执行的默认动作。

配置步骤：

1. 进入**策略>防火墙>策略配置**，如下图：

2. 勾选或者取消**策略匹配**的复选框，实现整个策略匹配模块的开启和关闭。



若勾选则开启策略匹配模块，经过系统的数据包都要经过防火墙策略的匹配；否则为关闭策略匹配模块，经过系统的数据包都不进行防火墙策略的匹配。

3. 选择**策略默认动作**，可选择 permit 或者 deny，此动作为匹配不到防火墙策略时的默认动作。

注意

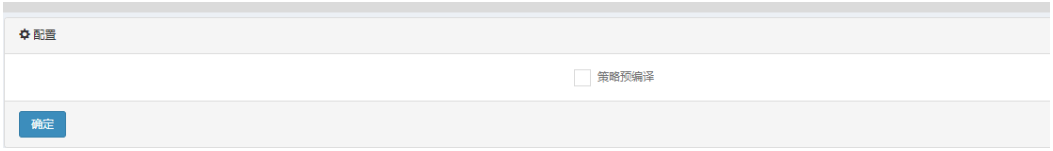
防火墙默认策略匹配开启且动作为 deny

44.3.10 策略预编译模块

在策略预编译模块可以开启或者关闭防火墙策略预编译匹配功能，默认关闭。在大量防火墙策略配置情况下，开启策略预编译可以提高策略的匹配性能。

配置步骤：

1. 进入**策略>防火墙>策略预编译**，如下图：



2. **勾选**策略预编译的复选框，点击**确定**，对当前防火墙策略配置进行预编译。

注意

1. 预编译开启后，设备会定期检查（默认 30s）策略相关配置是否改变，改变则重新进行预编译。
2. 配置改变包括：防火墙策略配置改变，被引用的地址对象和服务对象配置改变，被防火墙策略引用的接口和安全域配置改变。
3. 配置改变后，不能立即生效，直到重新编译后才能生效。

44.4 防火墙策略监控与维护

44.4.1 按协议类型查看防火墙策略

进入**策略>防火墙>策略**，可以根据 ipv4 或者 ipv6 协议类型查看已经配置的防火墙策略。

44.4.2 按分类方式（策略组）查看防火墙策略

有 2 种分类方式，策略组和接口对，默认按策略组显示。

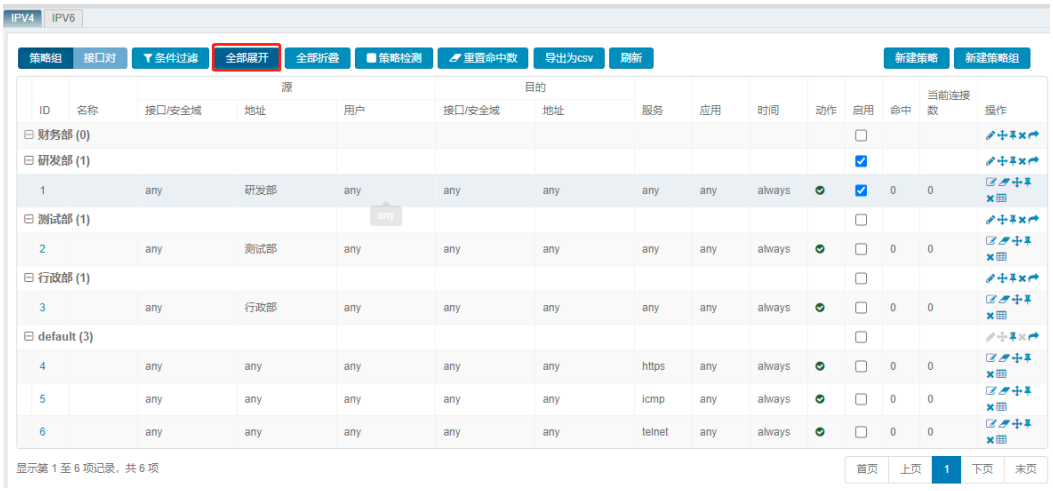
1. 进入**策略>防火墙>策略**，如下图：

策略组默认是关闭的状态，此状态下，策略组前的状态显示为⊞，此时只能看到策略组；

2. 点击策略组前的⊞，展开策略组下策略，策略组前显示⊟，如下图：

3. 点击，收起策略组下策略，如下图：

4. 点击 全部展开，展开所有策略组，如下图：



5. 点击 全部折叠，收起所有策略组，如下图：

44.4.3 按分类方式（接口对）查看防火墙策略

在防火墙策略配置满足一定条件的提前下，才能按照接口对方式显示，条件为：

1）所有的策略都在“default” 默认策略组里；

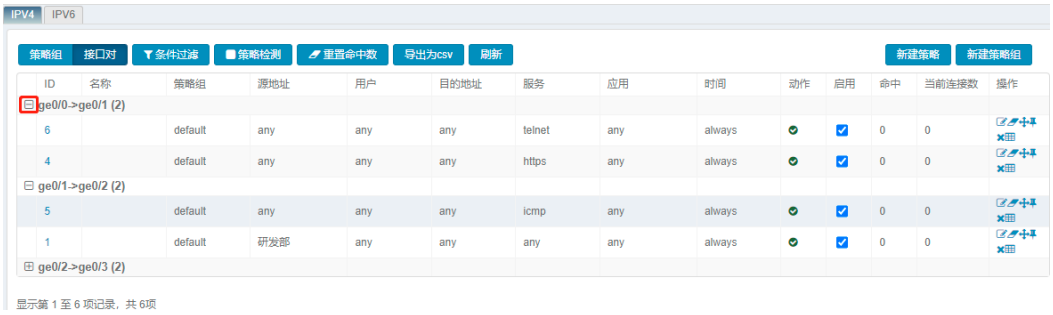
2）“default”默认策略组中的策略数量不能超过 1000；

3）策略的接口配置不能包含多接口配置；

1. 在满足条件时，按接口对方式显示，如下图：

接口对默认是关闭的状态，此状态下，接口对前的状态显示为⊞，此时只能看到接口对；

2. 点击接口对前的⊞，展开接口对下策略，接口对前显示⊟，如下图：



3. 点击⊟，收起接口对下策略，如下图：

44.4.4 导出csv文件查看防火墙策略

查询步骤：

1. 进入**策略>防火墙>策略**，如下图：

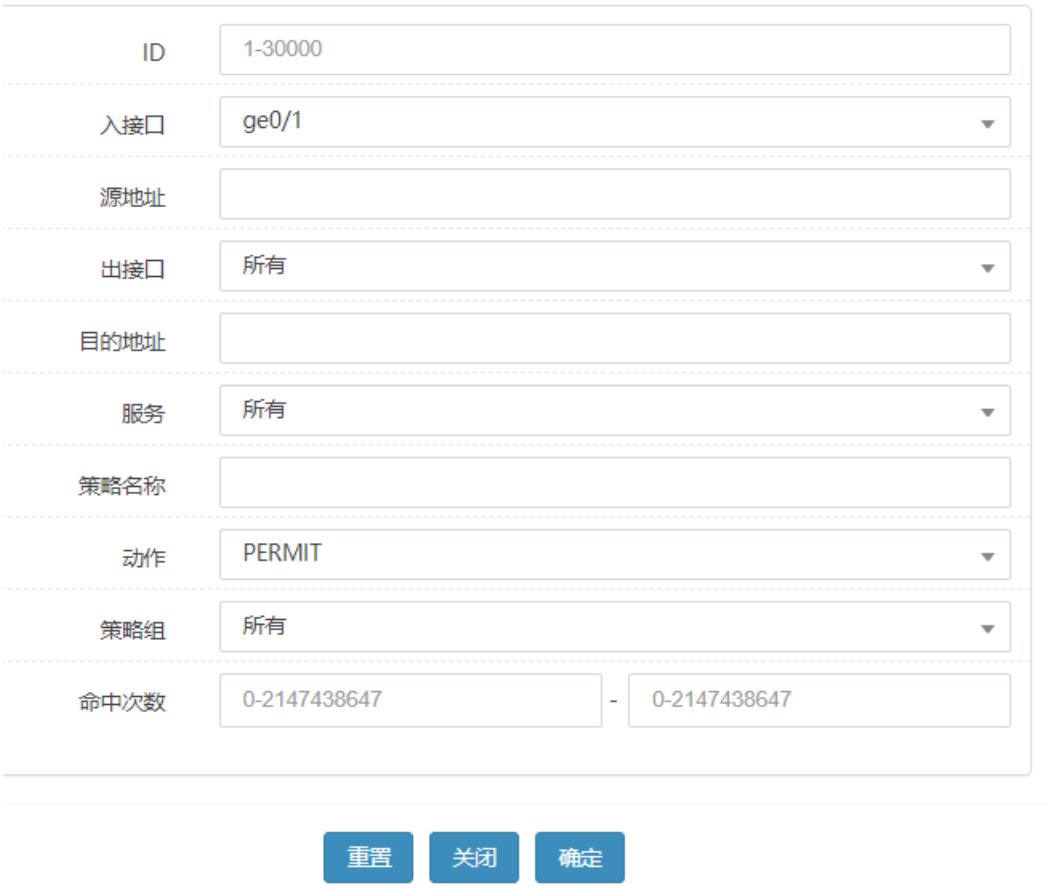
2. 点击 **导出为 csv**，导出 fw_policy_ipv4.csv 文件进行查看。

44.4.5 按过滤条件查询防火墙策略

查询步骤：

1. 进入**策略>防火墙>策略**，如下图：

2. 点击 **条件过滤**，如下图：



3. 在打开的页面中分别选择**源地址**、**目的地址**、**服务**和**动作**等过滤条件，点击**确定**，查询配置中与关键字相符的所有防火墙策略，如下图：

提示

1. 查询条件，策略名称，源地址和目的地址，是模糊搜索匹配查找。
2. 地址对象支持基于 IP 地址和地址对象名称搜索，当输入对象为 IP 地址则首先按照 IP 地址进行查找匹配，找不到再按照对象名称查找。当输入对象为对象名称时则按照对象名称进行查找匹配。

44.4.6 防火墙策略冗余检测

防火墙策略按照页面顺序从上至下匹配，若部分策略被前面的策略覆盖而不会被命中，这一类策略被定义为冗余策略，可以通过开启冗余检测自动检查出冗余策略。

检测步骤：

1. 进入**策略>防火墙>策略**，如下图：

2. 勾选**策略检测**开关，冗余的策略被高亮显示，如下图：

注意

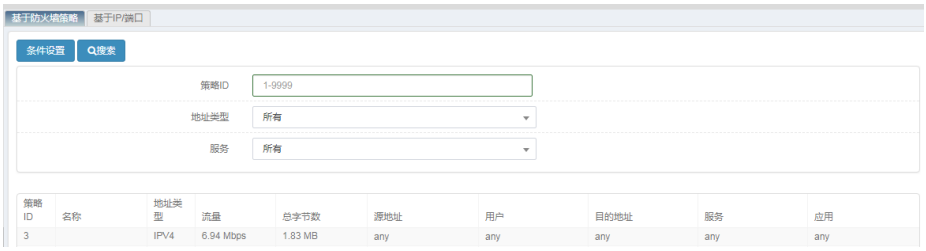
1. 开启策略检测后，冗余策略会黄色高亮显示，向右拖动水平滚动条可查看到新增一列名称为被覆盖，并显示覆盖策略的 ID。
2. 只有策略启用的情况下，该策略才会参与冗余检测的检查。
3. 冗余检测当前不支持并集覆盖检测，仅支持单个对象内容的冗余检测查找，当策略选择多个对象时，不会将多个对象进行组合，而是单个对象逐个进行匹配查找是否冗余。

44.4.7 查看防火墙策略流量统计

防火墙策略动作为 permit 的情况下且开启流量统计后可在流量统计页面下查看策略的流量统计信息。

查看步骤：

进入**监控>会话>流量统计>基于防火墙策略**，该页面可以查看到所有当前动作为 permit 的防火墙策略，若策略开启了流量统计，且有流量命中，则可以查看到命中该条策略的当前流量大小和总字节数等信息，如下图：



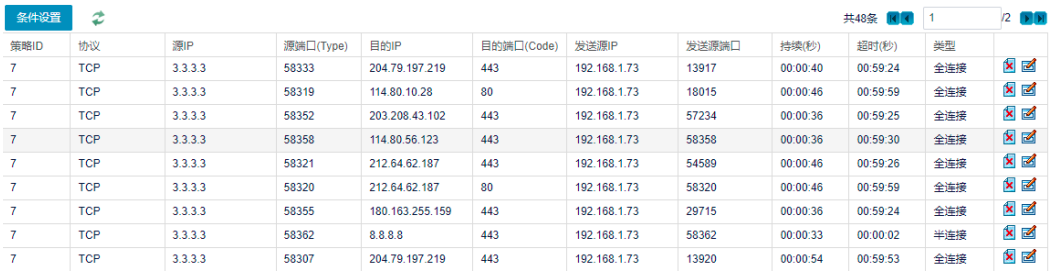
44.4.8 查看防火墙策略会话监控信息

会话上会记录跟策略相关的信息，点击策略的会话信息按钮，可以查看跟当前策略相关的会话。

查看步骤：

1. 点击策略的会话信息按钮 ，如下图：

3. 页面跳转到 **监控->会话->标准会话**，显示跟当前策略相关的会话，如下图：



提示

1、 策略 ID 为--：表示该条会话不命中任何防火墙策略。

2、 策略 ID 为 40000：表示该条会话匹配的是安全域的域内互访策略。

3、 策略 ID 为 40001：表示该条会话匹配的是防火墙策略的默认策略。

44.4.9 查看防火墙策略当前连接数

点击策略页面，查看对应策略行对应的**命中数**列和**当前连接数**列。

44.5 配置案例

44.5.1 配置案例1：创建IPV4防火墙策略

案例描述:

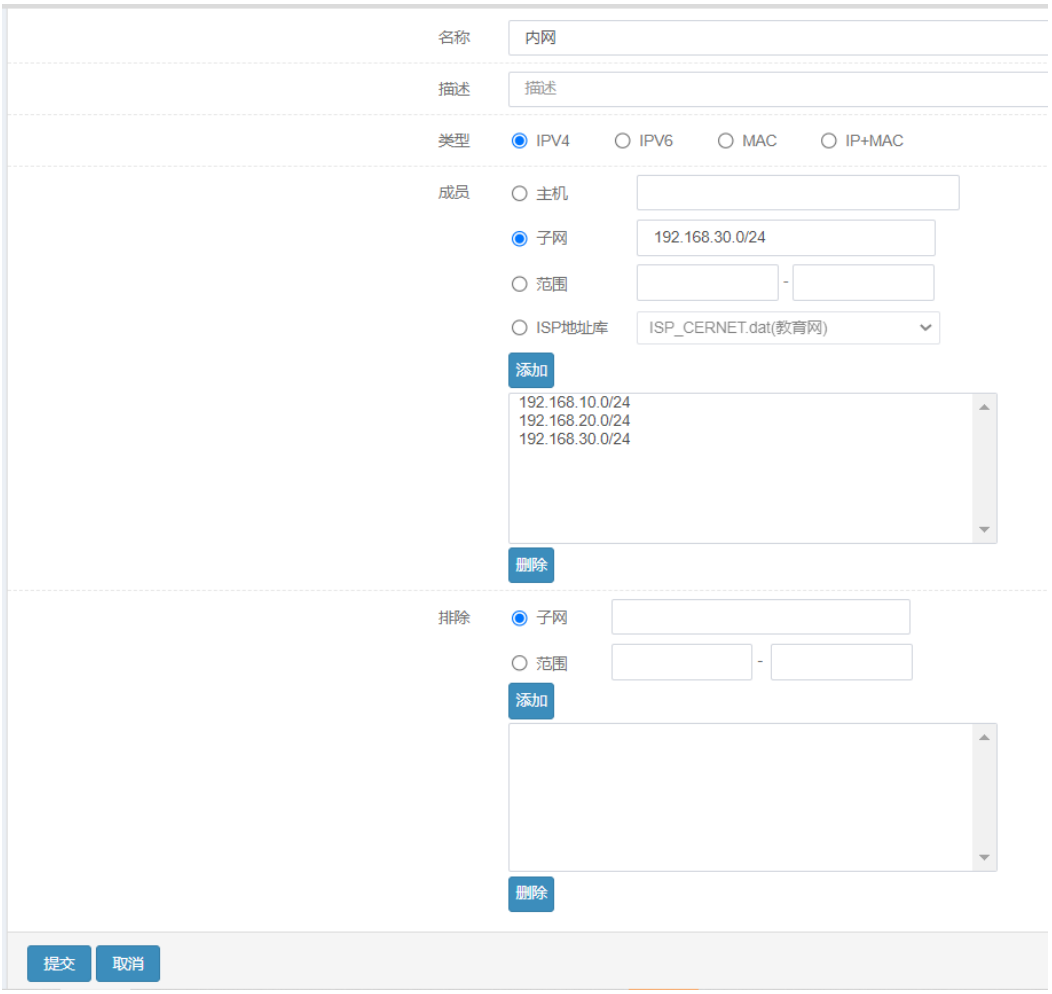
1、 设备的内网接口有 vlan10，vlan20，vlan30，加入到一个安全域内，允许域内接口之间互访。

2、 配置策略允许内网在非工作时间访问外网 ftp 和 http 服务。

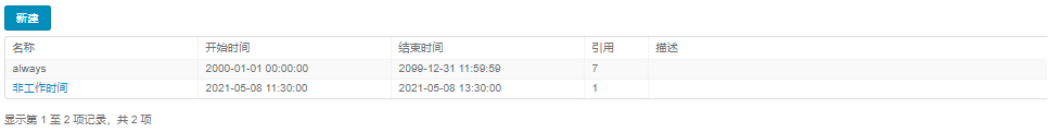
配置步骤:

1. 进入**网络>安全域**，配置添加内网接口到安全域“trust”内，勾选**允许接口间互相访问**。

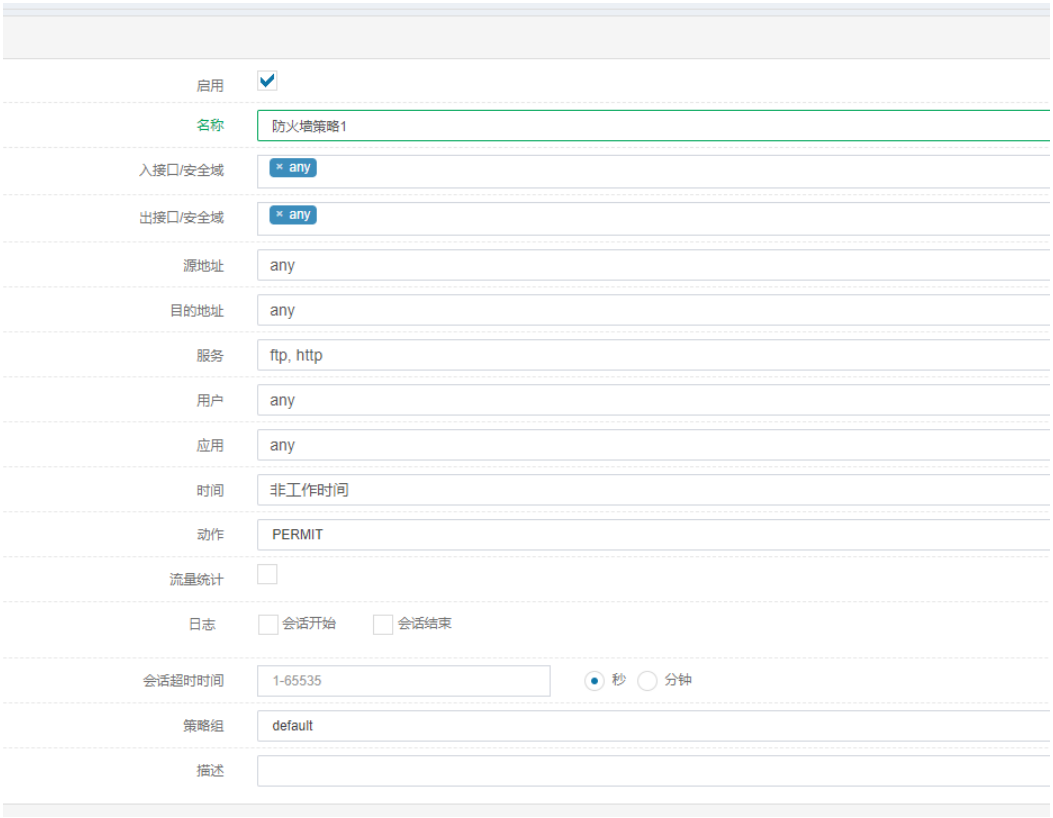
2. 进入**对象>地址对象>地址节点**，配置地址对象“内网”，如下图：



3. 进入**对象 >时间对象>周期时间**，配置时间对象“非工作时间”，如下图：



4. 进入**策略>防火墙>策略>IPV4**，点击**新建**，输入参数，如下图：



5. 点击**确定**。

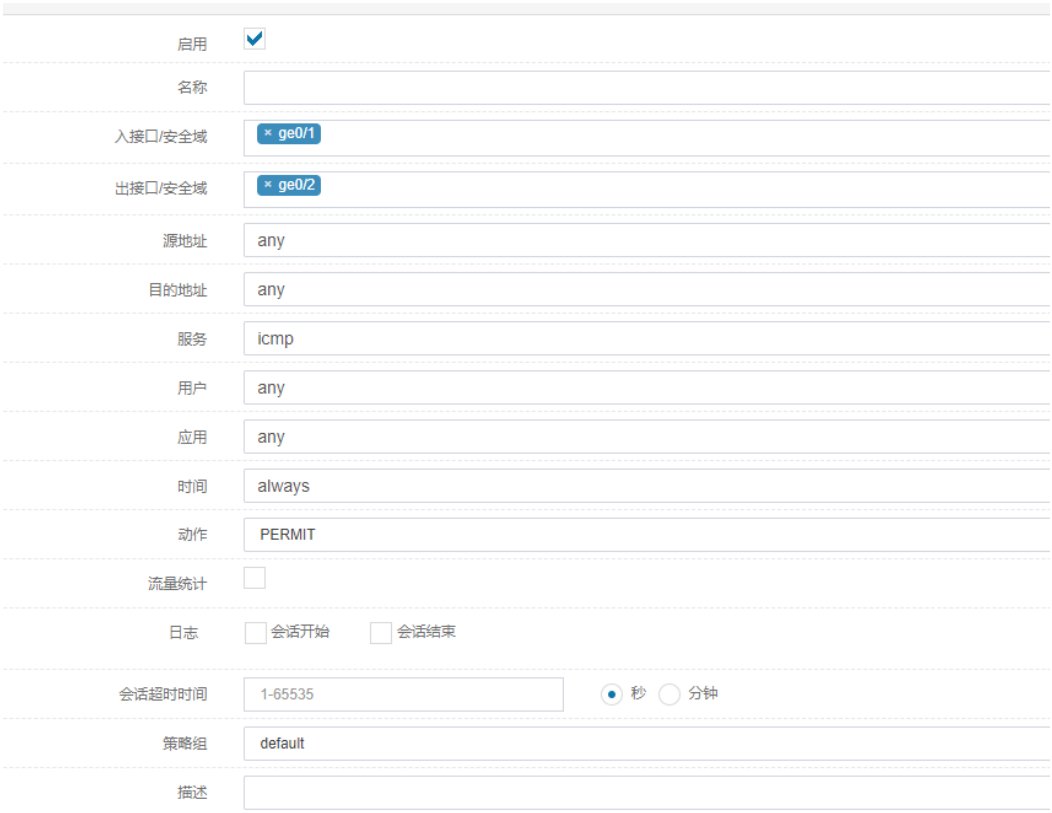
44.5.2 配置案例2 ：二层转发控制

案例描述：

设备 ge0/1 和 ge0/2 加入到 vlan100，需要控制只允许 ge0/1 到 ge0/2 的访问。

配置步骤：

1. 进入**策略>防火墙>策略>IPV4**，点击**新建策略**，如下图：



2. 点击**确定**。

44.5.3 配置案例3：web认证用户防火墙策略控制

案例描述：

1、 user1 和 user2 用户 web 认证通过后，需要控制用户只允许访问内网服务器地址。

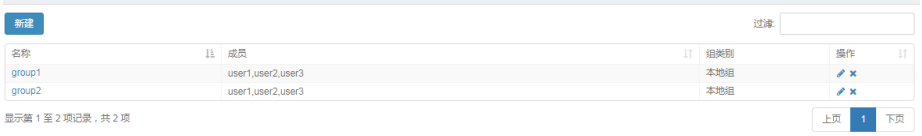
2、 属于认证用户组“group1”的用户认证通过后，不受访问控制。

配置步骤：

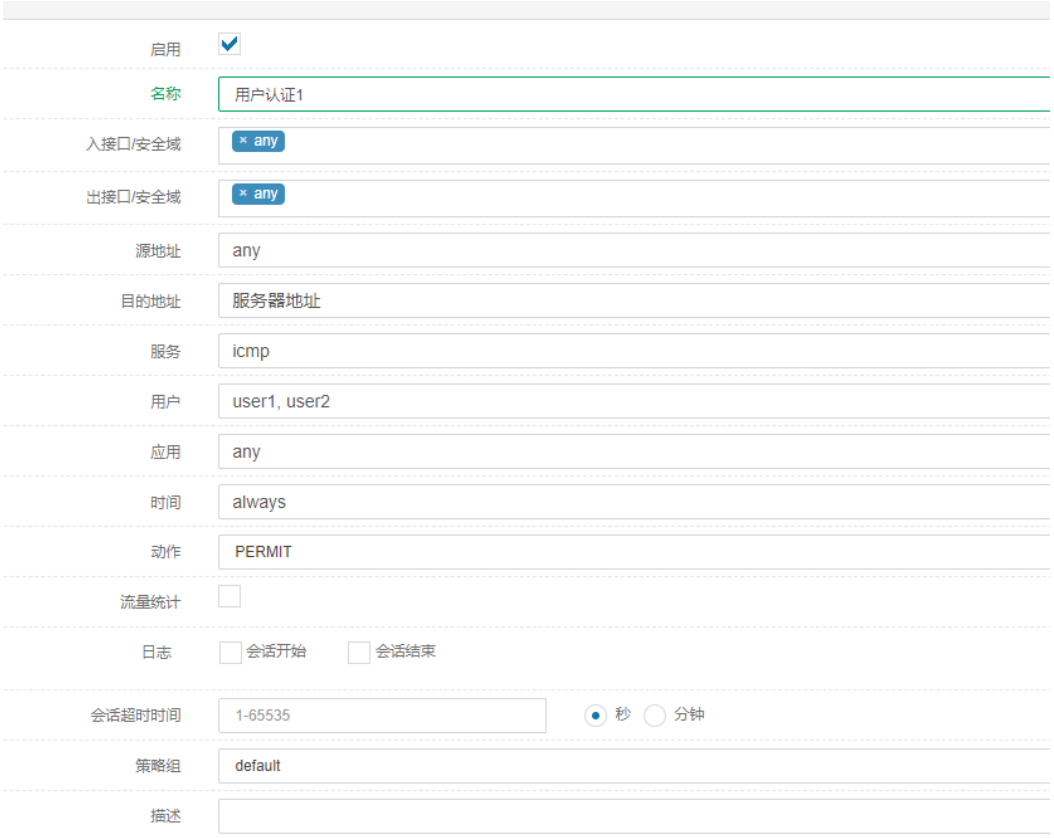
1. 进入**对象>地址对象>地址节点**，配置地址对象”服务器对象”包含服务器地址，如下图：

2. 进入**对象>用户对象 >用户**，创建用户 user1、user2 和 user3，如下图：

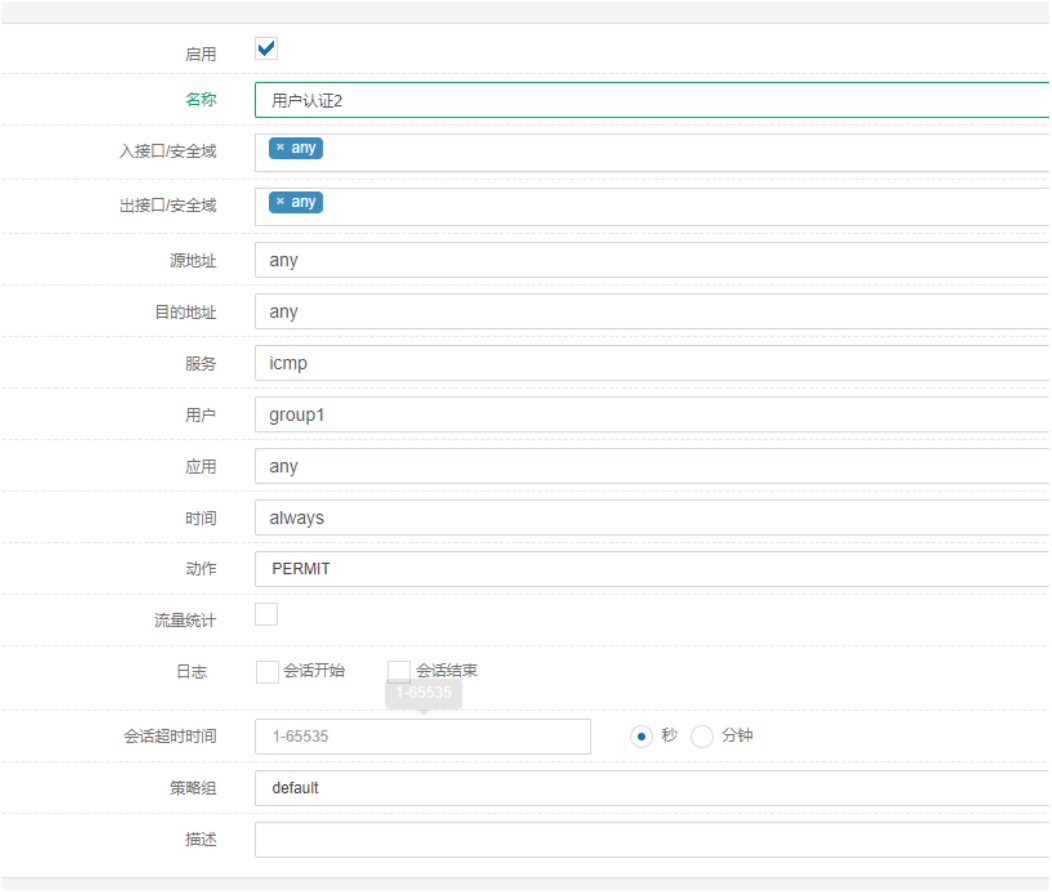
3. 进入**对象>用户对象 >用户组**，创建两个用户组，将三个用户分别加入到 group1 和 group2 用户组中。



4. 进入**策略>防火墙>策略**，点击**新建策略**，输入参数，用户选择 user1 和 user2，目的地址选择“服务器地址”，user1 和 user2 使用 group1 或 group2 用户组进行用户认证后都能匹配该策略，如下图：



5. 进入**策略>防火墙>策略**，点击**新建**，输入参数，用户选择 group1，只有用户使用 group1 用户组进行认证时才能匹配到该条策略，如下图：



注意

用户认证成功之前，认证需要放行的报文如 DNS 请求报文不会匹配防火墙策略，直接放行，用户认证通过后才匹配防火墙策略的查找。

44.6 常见故障分析

44.6.1 故障现象1：匹配上某条策略的数据流没有执行相应的动作

现象	匹配上某条策略的数据流没有执行相应的动作（阻断、放行）
分析	有可能是以下几种情况导致该策略无法生效： 1、 策略匹配没有开启，请查看策略匹配的状态是否为enable。 2、 该策略没有启用，请检查策略状态是否为enable。 3、 由于策略按页面顺序进行匹配，数据流可能匹配到前面的某条策略，请检查配置是否冲突。 4、 配置的防火墙策略是针对到设备本地的访问。

	5、 检查是否开启了策略预编译，且开启后有过策略修改。
解决	1、 启用策略匹配，修改策略匹配状态为enable。 2、 启用策略，修改该策略状态为enable。 3、 依据需求调整策略顺序。 4、 防火墙策略只对转发流量生效，不对到设备本地的流入或流出流量进行控制。 5、 若开启了策略预编译后策略进行了修改没有重新预编译还是会按照以前的策略匹配执行，可将预编译开关关闭或重新执行策略预编译，再验证匹配。

44.6.2 故障现象2：配置基于应用的防火墙策略不能匹配

现象	配置指定应用分类如搜索引擎和网络协议允许其他全部拒绝，查看搜索引擎应用没有允许通过
分析	应用识别需要一个学习过程，在应用没有识别之前该条策略不会匹配，而是继续向下匹配其他防火墙策略，而后续若没有该条会话的放行策略，则该应用由于首包就阻断了导致一直无法识别。
解决	1、 后续添加放行策略，保证有策略可以放行该应用从而使得该应用可以正确识别，应用识别后能正确匹配到防火墙策略。 2、 对于基于应用的访问控制，推荐使用应用控制策略来实现更好的应用控制效果。

44.6.3 故障现象3：防火墙策略部分接口不能选择

现象	期望配置添加一条防火墙策略入接口选择**vlan20**接口，但是策略配置时无法选择该接口
分析	检查**vlan20**接口是否已经加入到了安全域中，除物理接口以外的接口，当接口加入到安全域后，则防火墙策略配置时只能选择安全域接口
解决	接口选择安全域接口或者将接口从安全域中划出都可以

45 第45章 本地安全策略

45.1 本地安全策略概述

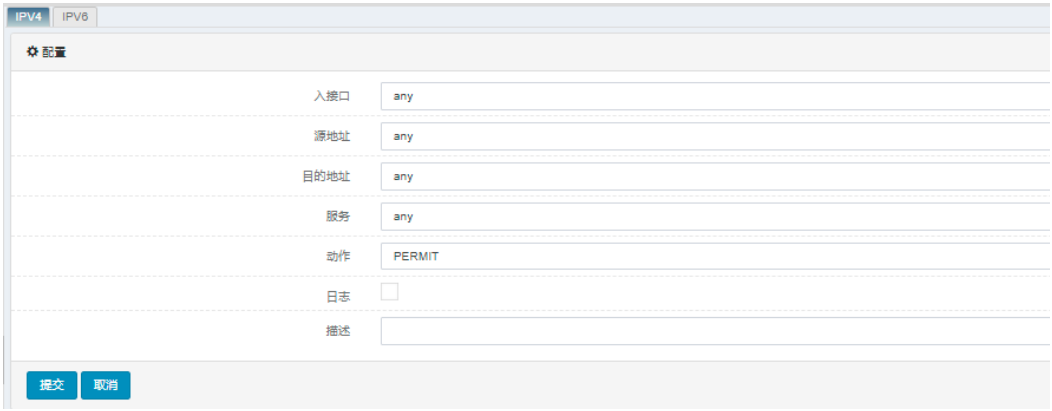
通过配置本地安全策略，能够对访问本机的数据流进行有效的控制和管理。当设备收到数据报文时，把该报文的入接口、源地址、目的地址以及服务与用户配置的策略匹配，决定是否建立这条数据流，并且把这条流和匹配的策略关联起来，从而确定如何处理该流的后续报文，实现允许、丢弃，决定哪些用户和数据能够访问本机。

45.2 配置本地安全策略

45.2.1 创建本地安全策略

配置步骤：

1. 进入**策略>本地安全>策略**，点击**新建**。



参数说明：

入接口：数据流的流入方向，可以指定某个特定接口，any 表示所有接口。

源地址：数据流的源地址，可以引用已定义的某个地址对象或地址对象组，any 表示可以源地址可以匹配所有对象。。

目的地址：数据流的目的地址，可以引用已定义的某个地址对象或地址对象组，any 表示目的地址可以匹配所有对象。

服务：数据流的服务属性，包括协议、源端口和目的端口，可以引用某个系统预定义服务、自定义的服务对象或服务对象组，any 表示服务可以匹配所有对象。

动作：对符合匹配条件的数据流执行的动作，PERMIT 为允许，DENY 为

拒绝。

日志：发送日志功能。动作为 PERMIT 时，级别是信息。动作为 DENY 时，级别是通知。

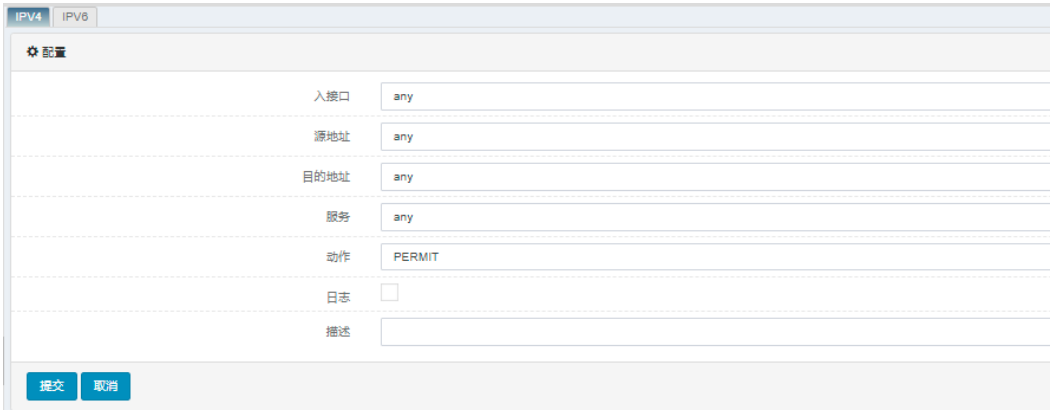
描述：策略的描述信息。

2. 配置完毕后，点击**提交**。

45.2.2 编辑本地安全策略

配置步骤：

1. 进入**策略>本地安全>策略**，点击 **ID** 字段。



2. 编辑完成后，点击**提交**。

45.2.3 删除本地安全策略

配置步骤：

1. 进入**策略>本地安全>策略**，如下图：

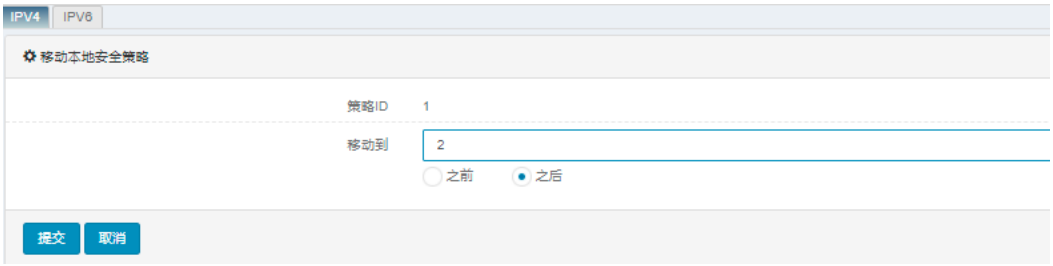
2. 点击✖，删除策略。

45.2.4 移动本地安全策略

配置步骤：

6. 进入**策略>本地安全>策略**，如下图：

7. 点击 调整对应策略顺序。



策略 ID：需要被移动的策略 ID 号。

移动到：参考策略 ID 号。

之前：移动到参考策略 ID 之前。

之后：移动到参考策略 ID 之后。

45.2.5 插入本地安全策略

配置步骤：

6. 进入**策略>本地安全>策略**，如下图：

4. 点击，插入一条新的策略到参考策略之前。

45.2.6 启用本地安全策略

配置步骤：

1. 进入**策略>本地安全>策略**，如下图。

2. 勾选 **启用**，可以启用一条策略。

注意

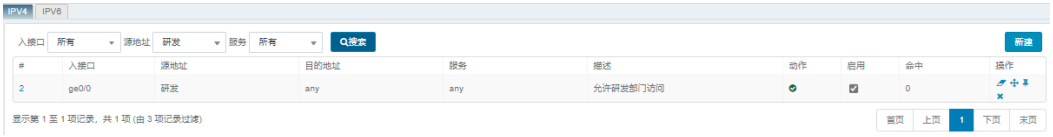
本地安全策略缺省为不启用，配置后必须手工启用才能使其生效。

45.2.7 查看本地安全策略列表

配置步骤：

1. 进入**策略>本地安全>策略**，如下图：

2. 输入过滤条件，搜索指定策略



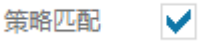
45.2.8 策略配置模块

在策略配置模块可以开启或者关闭整个策略匹配模块，也可以设置策略全部不匹配时执行的默认动作。

配置步骤：

4. 进入**策略>本地安全>策略配置**，如下图：

5. 勾选或者取消**策略匹配**的复选框，实现整个策略匹配模块的开启和关闭。



若勾选则开启策略匹配模块，访问本地的数据包都要经过本地安全策略的匹配；否则为关闭策略匹配模块，访问本地的数据包都不进行本地安全策略的匹配。

6. **策略默认动作**，可选择 permit 或者 deny，此动作为匹配不到本地安全

策略时的默认动作。

注意

1. 本地安全策略默认策略匹配关闭且动作为 permit。
2. 广播和多播流量不受控制。
3. mgt 口的流量不受控制。

45.3 配置案例

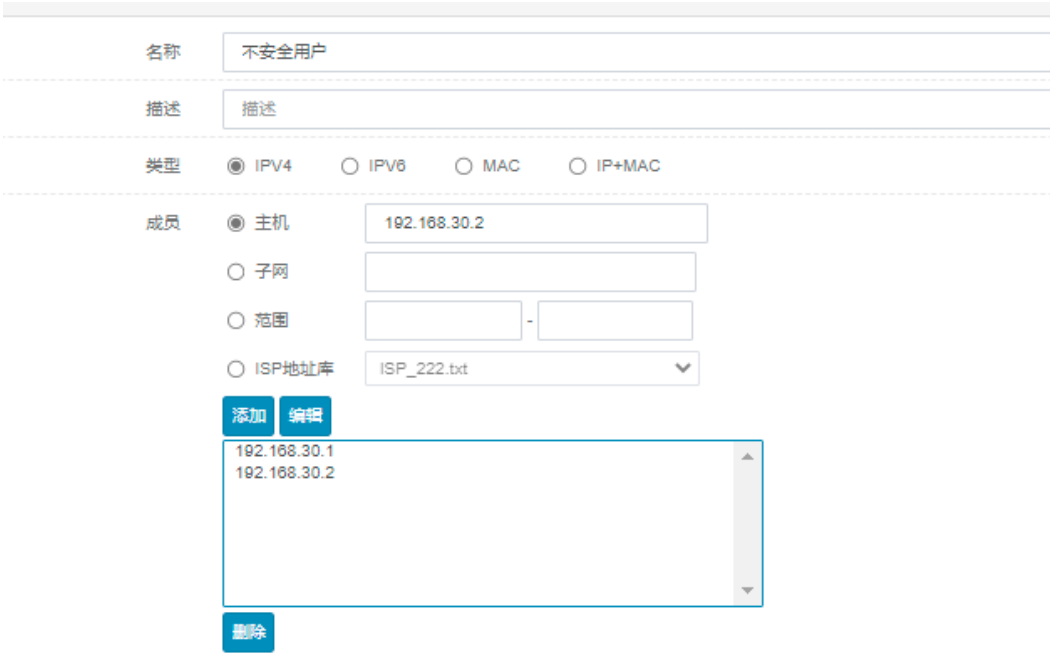
45.3.1 配置案例：阻断不安全用户访问设备

案例描述:

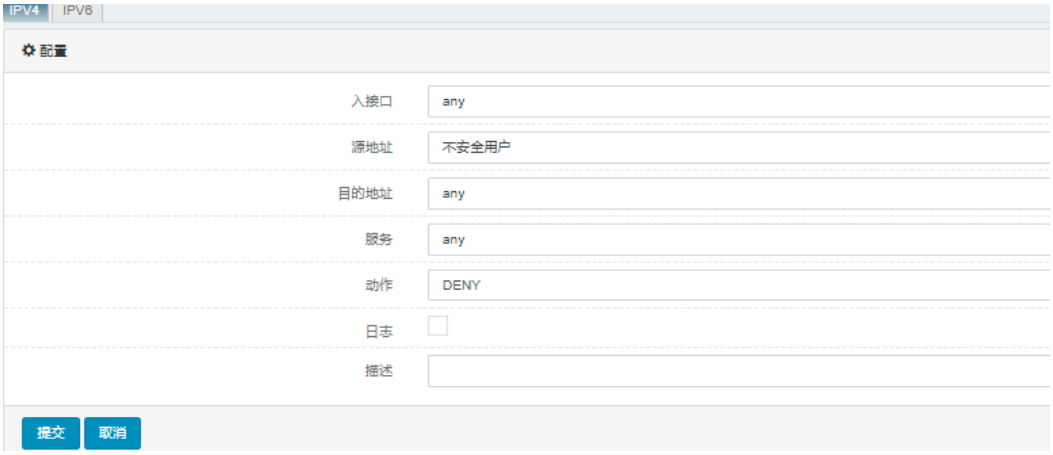
阻断某些不安全用户访问设备。

配置步骤:

1. 进入**对象>地址对象>地址节点**，配置地址对象”不安全用户”，如下图：



7. 进入**策略>本地安全>策略，**点击**新建**，如下图：



3. 点击**提交**。

4. 进入**策略>本地安全 >策略**，如下图：

5. 勾选**启用**完成设置。

46 第46章 防护策略

46.1 安全防护策略概述

为了防止网络设备受到恶意攻击，T 系列防火墙加入了攻击防护功能。

通过配置安全防护策略能够对经过设备的数据流进行有效的监控，并判断是否受到了恶意攻击。若设备开启了安全防护功能，设备会将收到数据报文的源地址、目的地址、协议、服务等信息和用户配置的安全防护策略进行匹配，判断此报文是否需要判断攻击，如果需要则把这条流与匹配的攻击策略关联起来，且省略该流的后续报文匹配策略的动作，而符合策略的报文则根据配置的某种防护功能（包括攻击防护、入侵防护、病毒防护、web 防护、威胁情报）对报文进行处理，从而决定哪些数据包能进出、哪些数据包需要丢弃。

在没有配置任何攻击防护策略的情况下，对于经过设备的所有数据包，其缺省为不开启策略匹配。

安全防护策略在 IPv4 或 IPv6 配置相同入接口时，按照从上往下的匹配原则，只对通过设备的数据包进行处理，对于设备本身发出的数据包不进行限制。

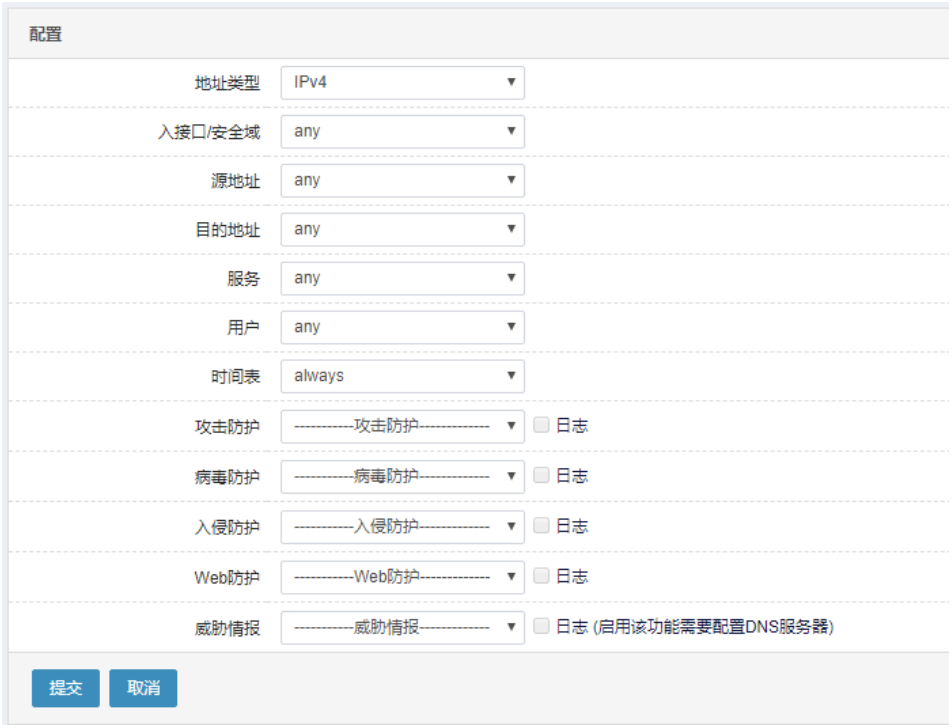
46.2 配置安全防护策略

46.2.1 配置策略的基本要素

安全防护策略的基本要素是匹配条件和动作。匹配条件包括数据流的入接口、源地址、目的地址、服务和策略生效的时间范围。其中，数据流的方向通过指定入接口、源地址、目的地址来确定，服务和时间范围都可以直接引用已定义的对象。

配置步骤：

4. 进入**策略>安全防护>防护策略**，点击新建。



参数说明：

地址类型：安全策略分为 IPv4 和 IPv6 两种类型，数据包匹配相应协议类型的安全策略。

入接口：数据流的流入方向，可以指定某个特定接口，any 表示所有接口。

源地址：数据流的源地址，可以引用已定义的某个地址对象或地址对象组，any 表示源地址为任意。

目的地址：数据流的目的地址，可以引用已定义的某个地址对象或地址对象组，any 表示目的地址为任意。

服务：数据流的服务属性，包括协议、源端口和目的端口，可以引用系统预定义服务、自定义的服务对象或服务对象组，any 表示服务为任意。

用户：用户对象，可以引用已定义的某个用户对象，any 表示用户对象为任意。

时间表：策略生效的时间，可以引用已配置的时间对象，always 表示所有时间。

攻击防护：开启攻击防护，对匹配的报文进行控制，防止 FLOOD 攻击和防扫描。

病毒防护：针对内外网入口处进行实时的病毒扫描，实现工作站被动防御病毒之外的主动病毒防御，并还提供文件扫描功能，

入侵防护：入侵防御可以检测到特定的网络行为，并可以选择放行、阻

断、阻断源 ip 等动作，以达到保护网络的功能。

web 防护：web 防护主要针对 XSS 攻击和 SQL 注入攻击进行防御。并根据预设的动作进行阻断或者放行。

威胁情报：威胁情报通过云端检查报文的 IP 和域名信息，得到主机的威胁情况，并根据预设的动作进行阻断或者放行。

日志：配置安全防护策略中各防护模块的日志过滤，支持日志信息在本地内存、syslog 服务器(日志控制中心)及 Email 这三种方式进行记录，每种方式都可以配置过滤的等级，当产生的日志高于或等于配置的过滤等级时，才会输出日志信息。

5. 配置完毕后，点击**提交**。

提示	创建一条新的安全防护策略时，必须引用相同协议类型的地址对象；系统会自动生成该策略的 ID 号，策略 ID 是安全防护策略的唯一标识。不同协议类型的安全防护策略的 ID 是相互独立的。
注意	个别模块的日志量较大，请谨慎开启并选择合适的过滤级别；本地日志是记录在系统缓存中的，由于系统缓存有限，当缓存满时，新的日志信息会覆盖老的信息。

46.2.2 启用安全防护策略

配置好的安全防护策略必须启用才能使其生效。

配置步骤：

3. 进入**策略>安全防护>防护策略**，如下图：

4. 勾选**启用**可以启用一条策略。

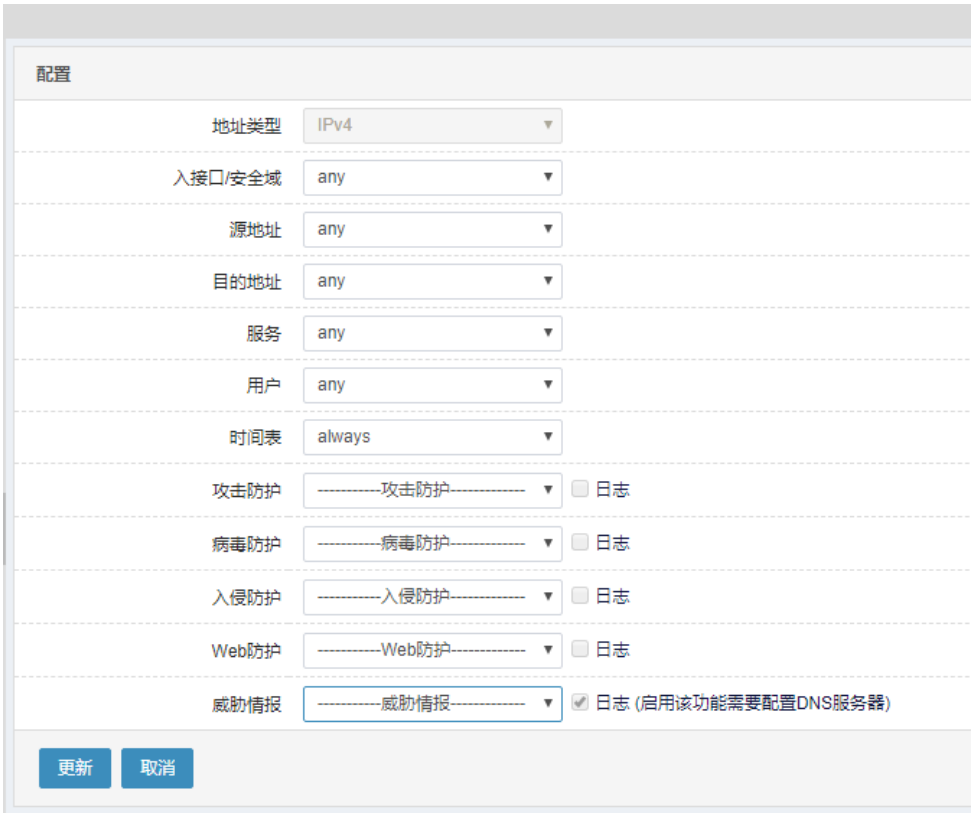
注意	策略缺省为不启用，配置后必须手工启用才能使其生效。

46.2.3 编辑安全防护策略

配置步骤：

3. 进入**策略>安全防护>防护策略**，对某条存在的安全防护策略点击策略 ID 号进入编辑界面

4. 可以对安全策略里面的内容进行编辑修改，修改完毕后点击**更新**。



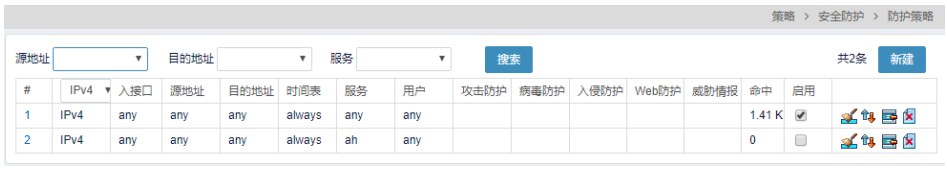
注意

编辑策略时，地址类型不能改变。

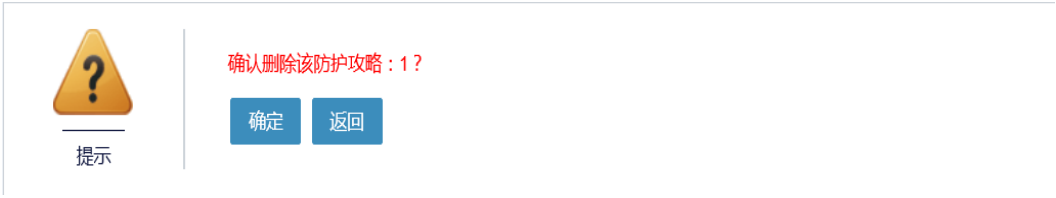
46.2.4 删除安全防护策略

配置步骤：

1. 进入**策略>安全防护>防护策略**，如下图：



2. 点击删除策略，然后点击**确定**删除。



46.2.5 调整安全防护策略的顺序

通过移动策略可以调整安全防护策略的匹配顺序，从而使位置在前的策略优先匹配。

配置步骤：

1. 进入**策略>安全防护>防护策略**，如下图：

2. 点击移动策略。

策略 ID：需要被移动的策略的 ID 号。

移动到（策略 ID）：参考策略的 ID 号。

之前：移动策略到参考策略之前。

之后：移动策略到参考策略之后。

3. 点击**提交**。

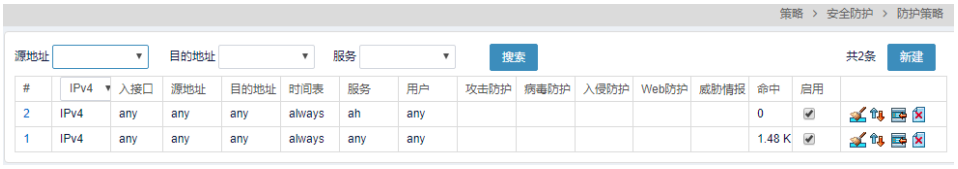
注意

只有定义相同协议类型的策略，才能调整顺序。

46.2.6 插入一条攻击防护策略

配置步骤：

1. 进入**策略>安全防护>防护策略**，如下图：



2. 点击 插入一条新的策略到参考策略之前。

3. 点击**更新**。

注意

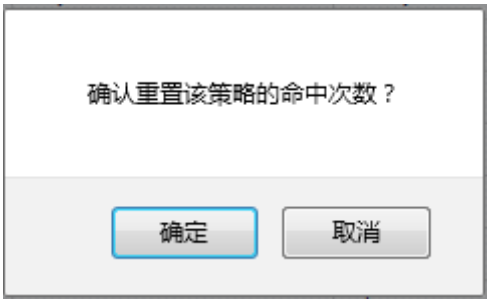
插入策略中的地址类型、源地址、目的地址都必须跟参考策略的类型相同。

46.2.7 重置安全防护策略的命中计数

配置步骤：

1. 进入**策略>安全防护>攻击防护>防护策略**，如下图：

2. 点击  重置策略的命中计数，点击**确定**进行重置。



46.2.8 查询攻击防护策略

查询步骤：

1. 进入**策略>安全防护>防护策略**，如下图：

2. 在下拉框中分别选择**源地址**、**目的地址**、**服务**，点击**搜索**查询配置中与关键字相符的所有安全策略。

46.3 配置案例

46.3.1 案例1：创建安全防护策略

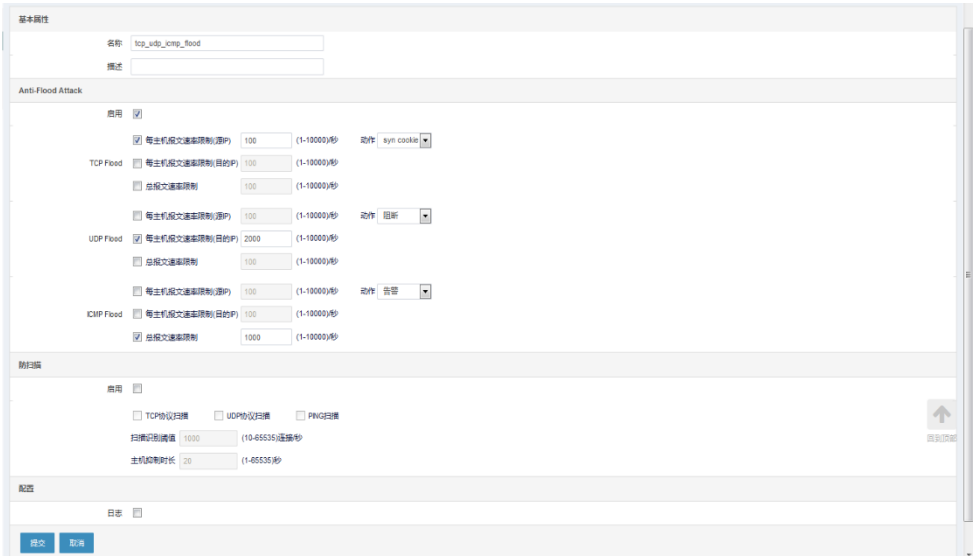
案例描述

设备的 vlan1 连接内网，vlan2 连接外网。若外网的每源 IP 向内网发出的 TCP 连接请求速率超过 100，就会触发设备 TCP syncookie 功能，验证连接请求方是否为攻击源，若是攻击源，设备将连接请求报文丢弃（开启 Syncookie 功能可能会消耗设备性能）；若外网向内网某一 DNS 服务器发出的 DNS 连接请求报文速率超过 2000，就会触发设备的 UDP Flood 功能，将超过阈值的 DNS 连接请求报文丢弃；若外网向内网发送的 ICMP 请求报文总速率超过 1000，就会触发设备的告警功能，提示内网网络可能受到 ICMP 攻击；配置攻击防护防 Flood 策略，实时监控网络状况，保护网络不受攻击影响。

配置步骤：

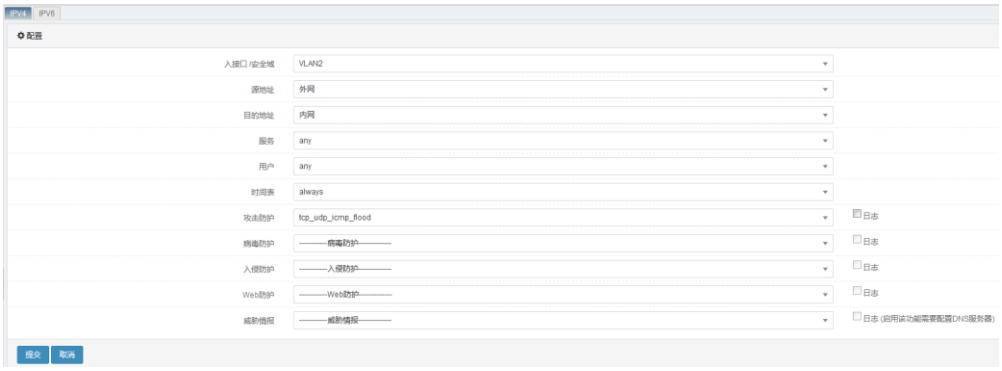
4. 进入**对象>地址对象>地址节点**，配置地址对象“内网”和“外网”，如下图：

5. 进入**策略>安全防护>攻击防护**，点击**新建**。



6. 进入**策略>安全防护>防护策略**，点击**新建**，选择对应的参数，如下

图：



7. 点击**提交**。

8. 进入**策略>安全防护>防护策略**，勾选**启用**完成配置，如下图：

46.3.2 案例2：创建安全防护防扫描策略

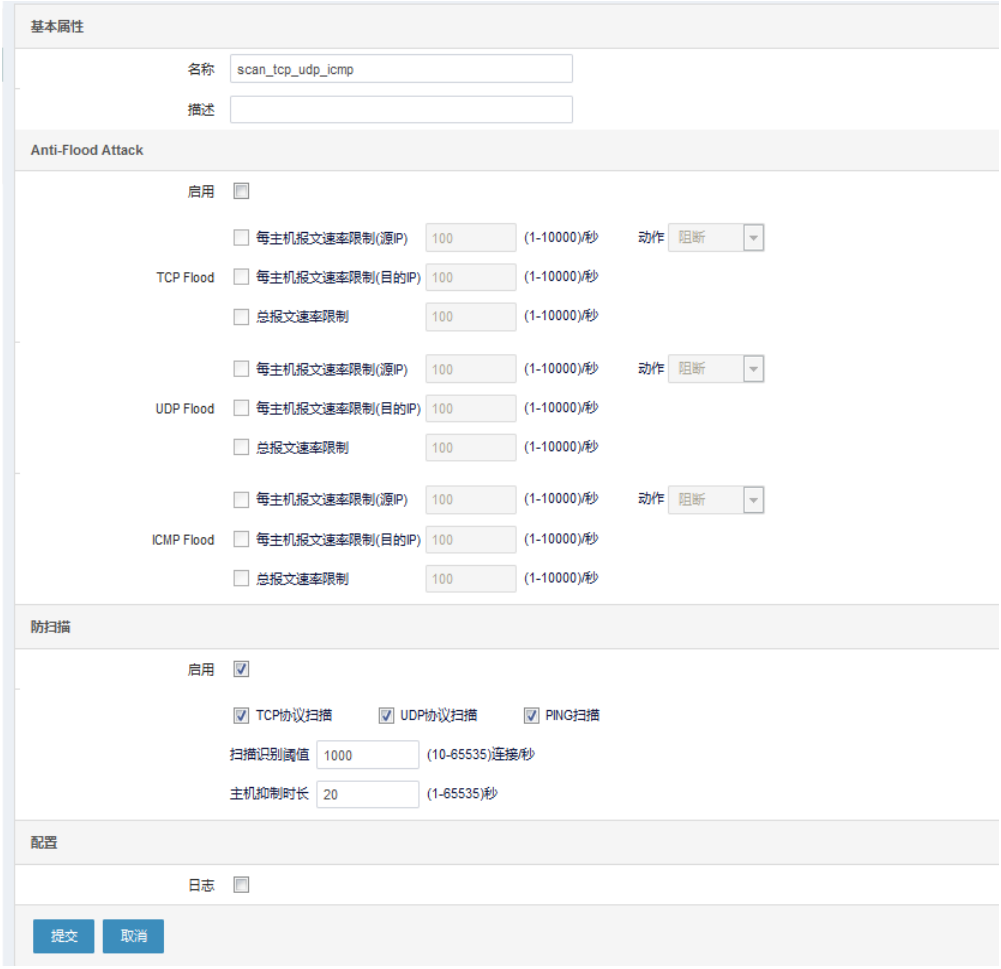
案例描述

设备的 vlan1 连接内网，vlan2 连接外网，为了预防外网向内网发起扫描攻击，设备需要开启防扫描策略。若外网某一源地址 1 秒内向内网某一服务器的超过 1000 个不同端口发送了 TCP 连接请求报文（或者 UDP 连接请求报文），则触发了设备的防扫描功能，在接下来的 20 秒内，此源地址的所有 TCP 请求报文（或 UDP 请求报文）将被阻断；若外网某一源地址 1 秒内向内网超过 1000 个不同主机发送 ICMP 请求报文，则触发了设备的防扫描功能，在接下来的 20 秒内，此源地址的所有 ICMP 请求报文将被阻断。

配置步骤：

1. 进入**对象>地址对象>地址节点**，配置地址对象“内网”和“外网”，如下图：

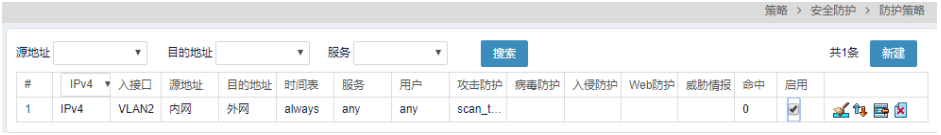
2. 进入**策略>安全防护>攻击防护>安全防护表**，点击**新建**。



3. 进入**策略>安全防护>防护策略**，点击**新建**，选择对应的参数，如下图：

4. 点击**提交。**

5. 进入**策略>安全防护>攻击防护>策略**，勾选**启用**完成配置，如下图：



46.4 常见故障分析

46.4.1 故障现象：某些应该匹配上某条策略的数据流没有匹配上该策略

现象	匹配上某条策略的数据流没有受到相应的限制。某些应该匹配上某条策略的数据流没有匹配上该策略。
分析	有可能是以下几种情况导致该策略无法生效： ➢ 该策略没有启用，请检查策略状态是否为启用； ➢ 由于策略在IPv4或IPv6有相同入接口时按从上往下的原则进行匹配，数据流可能匹配到前面的某条策略，请检查配置是否冲突。
解决	启用该策略，如果和其他策略的配置冲突，可以根据需求修改策略或者改变策略的顺序。

47 第47章 攻击防护

47.1 攻击防护概述

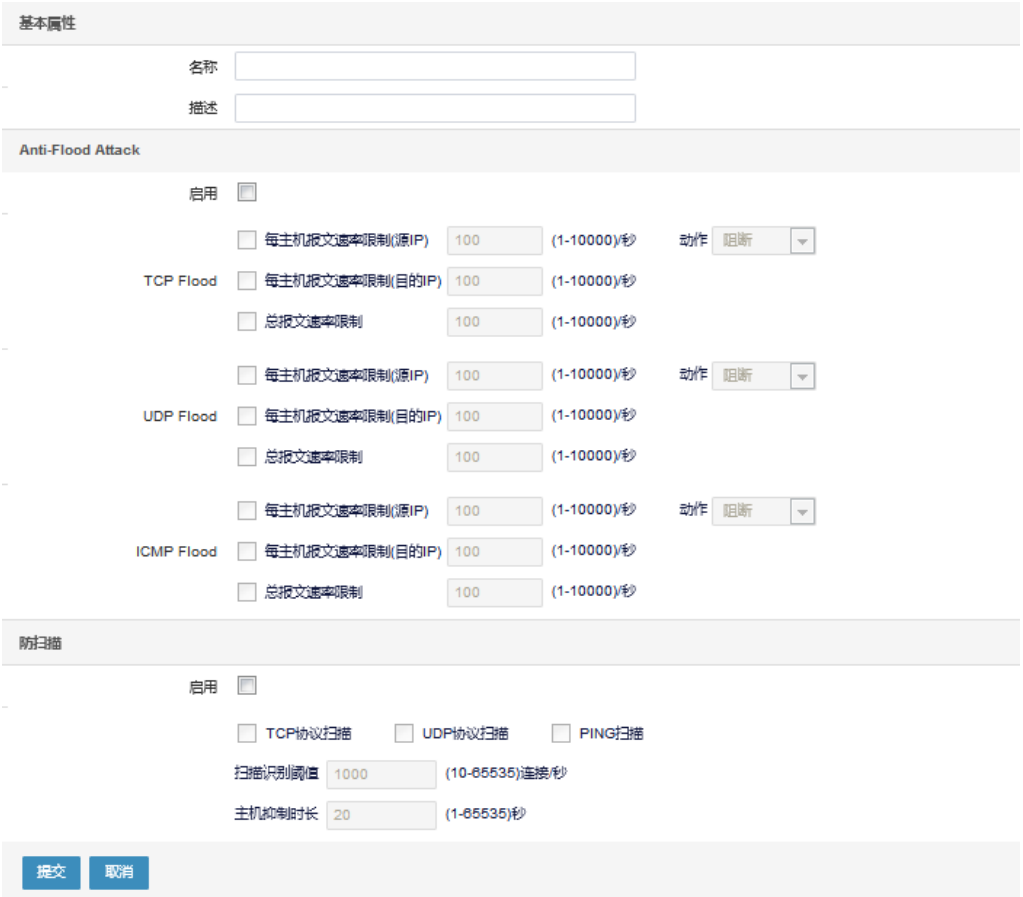
攻击防护是防 FLOOD 攻击和防扫描安全功能的配置模版。攻击防护功能需要在安全防护策略中引用才能起作用。符合策略的报文则根据攻击防护中的配置实现告警、丢弃、syncookie 等动作，从而决定哪些数据包能进出、哪些数据包需要丢弃。

47.2 配置攻击防护

47.2.1 创建攻击防护

配置步骤：

2. 进入**策略>安全防护>攻击防护**，点击**新建。**



名称：攻击防护名称，支持中文名称。

描述：攻击防护的简单描述信息。

Anti-Flood Attack：配置是否启用防 Flood 攻击。

TCP Flood：选择启用 TCP 协议的防 Flood 攻击功能。TCP Flood 即 SYN Flood 攻击，是众多攻击形式的一种方式。SYN Flood 利用 TCP 协议的缺陷，向服务器端发送大量伪造的 TCP 连接请求之后，自身不再做出应答，使得服务器端的资源迅速耗尽，从而无法及时处理其它正常的服务请求，严重的时候甚至会导致服务器系统的崩溃。

防火墙设备的防 SYN Flood 攻击采用了业界最新的 syncookie 技术，在很少占用系统资源的情况下，可以有效地抵御 SYN Flood 对受保护服务器的攻击。**识别门限**：配置 syn 报文个数的阈值，即防 TCP Flood 攻击的启动门限，缺省配置为 100。**动作**：阻断、警告、syncookie。

UDP Flood：选择启用 UDP 协议的防 Flood 攻击功能。**识别门限**：配置 UDP 报文个数的阈值，即防 UDP Flood 攻击的启动门限，缺省配置为 100。**动作**：阻断、警告。

ICMP Flood：选择启用 ICMP 协议的防 Flood 攻击功能。**识别门限**：配置 ICMP 报文个数的阈值，即防 ICMP Flood 攻击的启动门限，缺省配置为 100。**动作**：阻断、警告。

防扫描：配置是否启用防扫描攻击。

TCP 协议扫描：根据实际网络情况，当受到 TCP 扫描攻击时，可以配置防 TCP 扫描。

当一个源 IP 地址在 1 秒内将含有 TCP SYN 片段的 IP 封包发送给位于相同目标 IP 地址的不同端口（或者不同目标地址的相同端口）数量大于配置的阈值时，即认为其进行了一次 TCP 扫描，系统将其标记为 TCP SCAN，并在配置的阻断时间内拒绝来自于该台源主机的所有其它 TCP SYN 包。

启用防 TCP 扫描，可能会占用比较多的内存。

UDP 协议扫描：根据实际网络情况，当受到 UDP 扫描攻击时，可以配置防 UDP SCAN 扫描。

当一个源 IP 地址在 1 秒内将含有 UDP 的 IP 封包发送给位于相同目标 IP 地址的不同端口（或者不同目标地址的相同端口）数量大于配置的阈值时，即进行了一次 UDP 扫描，系统将其标记为 UDP SCAN，并在配置的阻断时间内拒绝来自于该台源主机的所有其它 UDP 包。

启用防 UDP 扫描，可能会占用比较多的内存。

PING 扫描：根据实际网络情况，当受到 PING 扫描攻击时，可以配置防 PING 扫描。

当一个源 IP 地址在 1 秒内发送给不同主机的 ICMP 封包超过门限值时，即进行了一次地址扫描。此方案的目的是将 ICMP 封包(通常是应答请求) 发送给各个主机，以期获得至少一个回复，从而查明目标地址。防火墙设备

在内部记录从某一远程源地点发往不同地址的 ICMP 封包数目。当某个源 IP 被标记为地址扫描攻击，则系统在配置的阻断时间内拒绝来自该主机的其它更多 ICMP 封包。

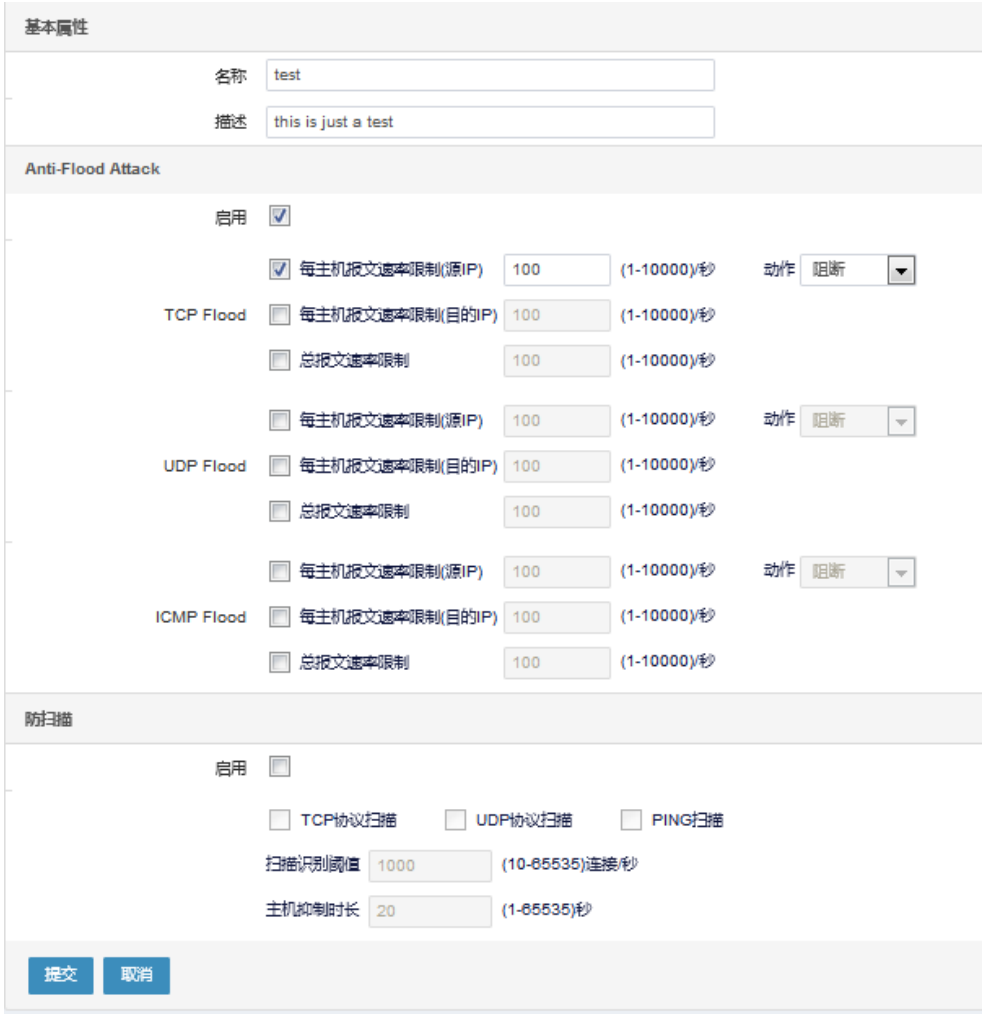
启用防 PING 扫描，可能会占用比较多的内存。

主机抑制时长：设置防扫描功能的阻断时间，当系统检测到扫描攻击时，在配置的时长内拒绝来自于该台源主机的所有其它攻击包，缺省配置为 20 秒。

扫描识别阈值：防扫描功能的扫描识别门限，超过阈值时，该源 IP 被标记为扫描攻击，来自于该台源主机的所有其它攻击包都被阻断，缺省配置为 1000。

请谨慎配置限制数量，当内部网络是通过 NAT 的方式上网时，由于源 IP 都相同，如果配置值过小，会导致防 Flood 攻击生效。

2. 输入攻击防护**名称**和**描述**，配置好各项功能：



3. 点击**提交**，完成对攻击防护的配置，显示如下页面：

47.2.2 编辑攻击防护

已经创建的攻击防护可以编辑修改。

1. 进入**策略>安全防护>攻击防护**，如下图：

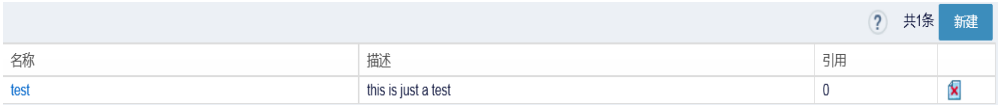
2. 单击需要修改的攻击防护**名称**，进行修改编辑。

可以对该攻击防护进行配置修改，其中名称不能改变。

3. 点击**更新**完成修改的配置。

47.2.3 删除攻击防护

1.进入**策略>安全防护>攻击防护**，如下图：



2.选择需要删除的攻击防护，点击 进行删除。

3.点击**确定**，完成攻击防护的删除。

注意 正在被安全防护策略引用的攻击防护，其删除按钮为灰色，不能被删除。

47.2.4 在安全防护策略中引用攻击防护

攻击防护只有在安全防护策略中被引用才能生效，符合安全防护策略的报文才能受该攻击防护的保护。

47.3 配置案例

47.3.1 案例1：创建安全防护防Flood策略

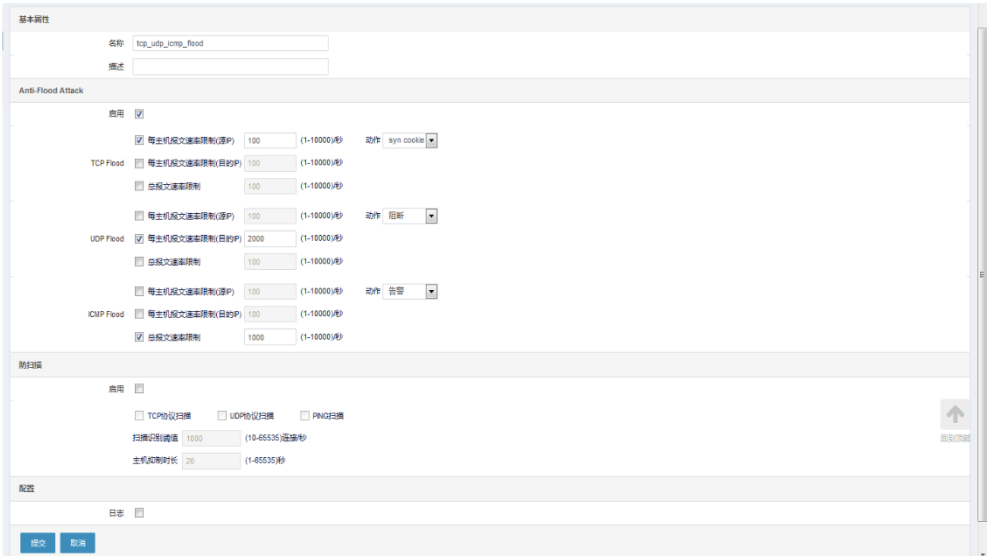
案例描述

设备的 vlan1 连接内网，vlan2 连接外网。若外网的每源 IP 向内网发出的 TCP 连接请求速率超过 100，就会触发设备 TCP syncookie 功能，验证连接请求方是否为攻击源，若是攻击源，设备将连接请求报文丢弃（开启 Syncookie 功能可能会消耗设备性能）；若外网向内网某一 DNS 服务器发出的 DNS 连接请求报文速率超过 2000，就会触发设备的 UDP Flood 功能，将超过阈值的 DNS 连接请求报文丢弃；若外网向内网发送的 ICMP 请求报文总速率超过 1000，就会触发设备的告警功能，提示内网网络可能受到 ICMP 攻击；配置攻击防护防 Flood 策略，实时监控网络状况，保护网络不受攻击影响。

配置步骤：

1. 进入**对象>地址对象>地址节点**，配置地址对象“内网”和“外网”，如下图：

2.进入**策略>安全防护>攻击防护**，点击**新建**。



3. 进入**策略>安全防护>防护策略**，点击**新建**，选择对应的参数，如下图：

4.点击**更新**。

5.进入**策略>安全防护>防护策略**，勾选**启用**完成配置，如下图：

47.3.2 案例2：创建安全防护防扫描策略

案例描述

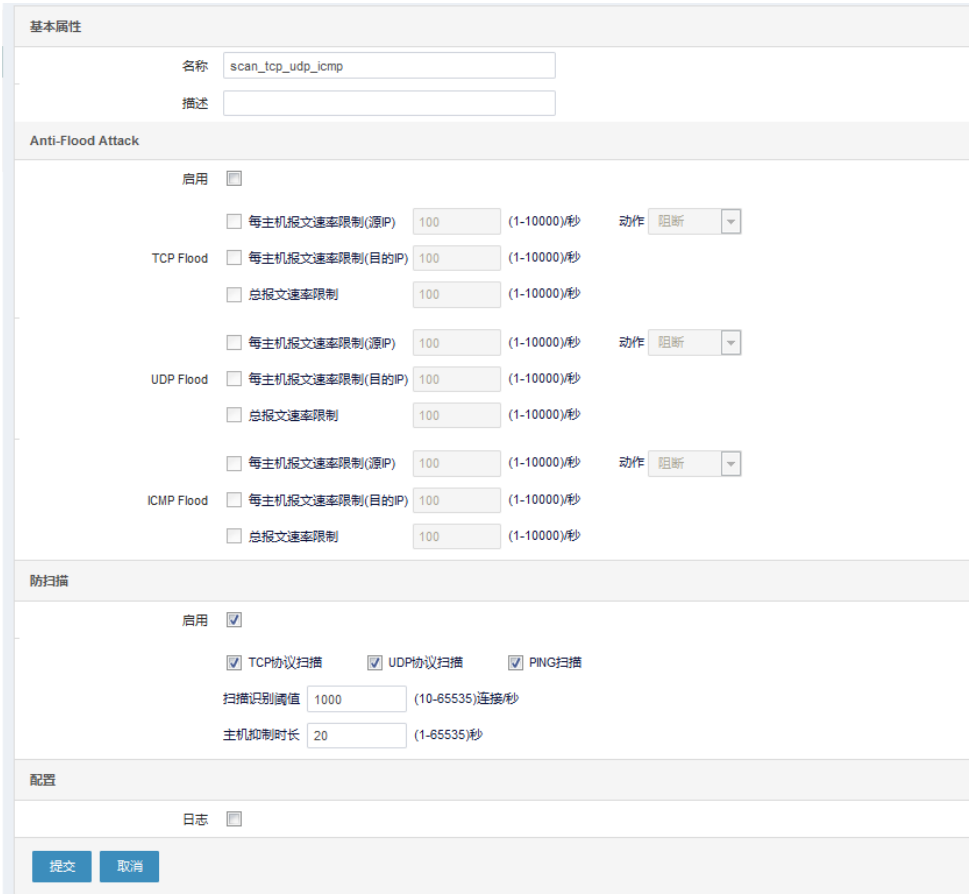
设备的 vlan1 连接内网，vlan2 连接外网，为了预防外网向内网发起扫描攻击，设备需要开启防扫描策略。若外网某一源地址 1 秒内向内网某一服务器的超过 1000 个不同端口发送了 TCP 连接请求报文（或者 UDP 连接请求报文），则触发了设备的防扫描功能，在接下来的 20 秒内，此源地址的所有 TCP 请求报文（或 UDP 请求报文）将被阻断；若外网某一源地址 1 秒内向内网超过 1000 个不同主机发送 ICMP 请求报文，则触发了设备的防扫描功能，在接下来的 20 秒内，此源地址的所有 ICMP 请求报文将被阻断。

配置步骤：

1.进入**对象>地址对象>地址节点**，配置地址对象“内网”和“外网”，如下

图：

2.进入**策略>安全防护>攻击防护>安全防护表**，点击**新建**。



3.进入**策略>安全防护>攻击防护>策略**，点击**新建**，选择对应的参数，如下图：

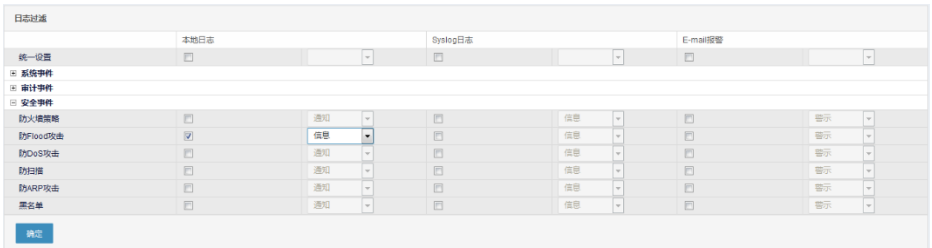
6. 点击**更新**。

7. 进入**策略>安全防护>攻击防护>策略**，勾选**启用**完成配置，如下图：

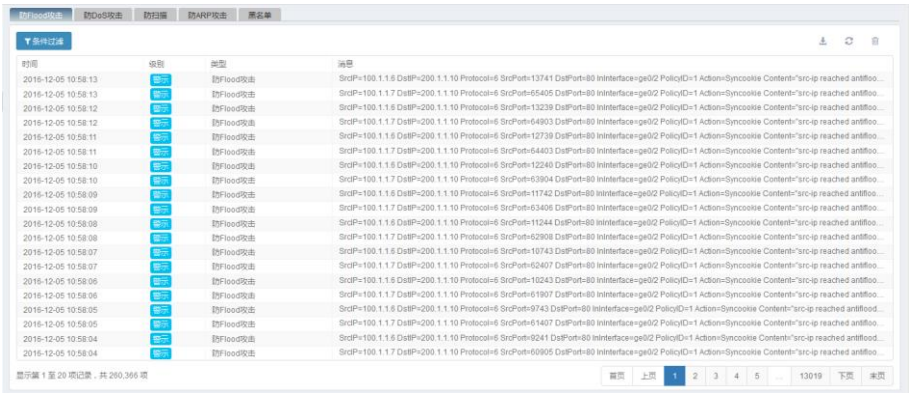
47.4 攻击防护监控与维护

47.4.1 查看攻击防护日志

1. 进入**日志>日志管理>日志过滤**，勾选防 Flood 攻击模块的相关日志，并设置日志的级别，点击**确定**。



2. 进入**日志>安全日志>防 Flood 攻击**里查看相关的防 Flood 攻击安全日志。



47.5 常见故障分析

47.5.1 故障现象：防flood功能不能正常工作

现象	防flood功能不能正常工作。
分析	若策略匹配成功，但是防flood功能不起作用，有可能是以下几种情况导致防flood功能无法生效： ➢ 检查安全防护对象中的防flood总开关是否勾选； ➢ 由于防flood中分为syn flood、udp flood、icmp flood，检查报文类型是否选对 ➢ 检查所配置的门限值是否过大 检查所配置的防flood的动作是否正确。
解决	修改原有配置，以保证防flood功能能正常工作。

48 第48章 病毒防护

48.1 病毒防护概述

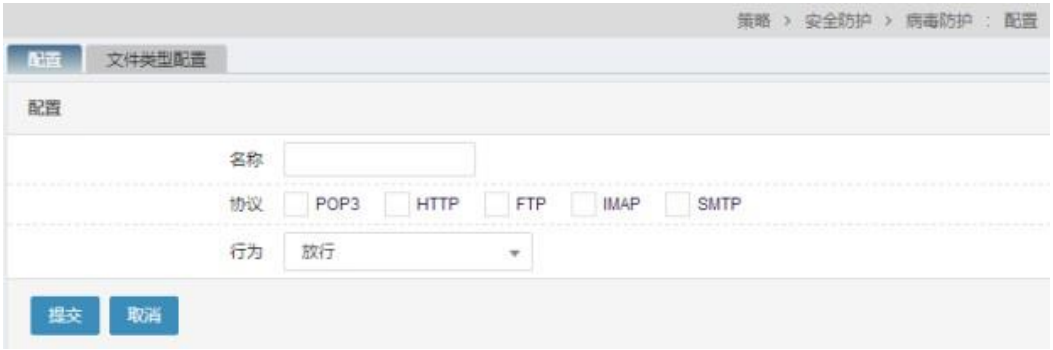
针对内外网入口处进行实时的病毒扫描，将外来病毒隔离在内网之外，实现工作站被动防御病毒之外的主动病毒防御。同时还提供文件扫描功能，可以对特定的文件类型进行扫描。我们可以在诸如 HTTP、FTP、IMAP、POP3、SMTP 等应用协议时进行文件扫描，预置模板扫描所有协议且对病毒执行阻断操作。

48.2 配置病毒防护

48.2.1 新建病毒防护模板

配置步骤：

1.进入**策略>安全防护>病毒防护**，点击**新建**。



参数说明：

名称：病毒防护模板名称。

协议：数据流的应用协议，至少选择一个。

行为：对符合匹配条件的数据流执行的动作，放行或者阻断。

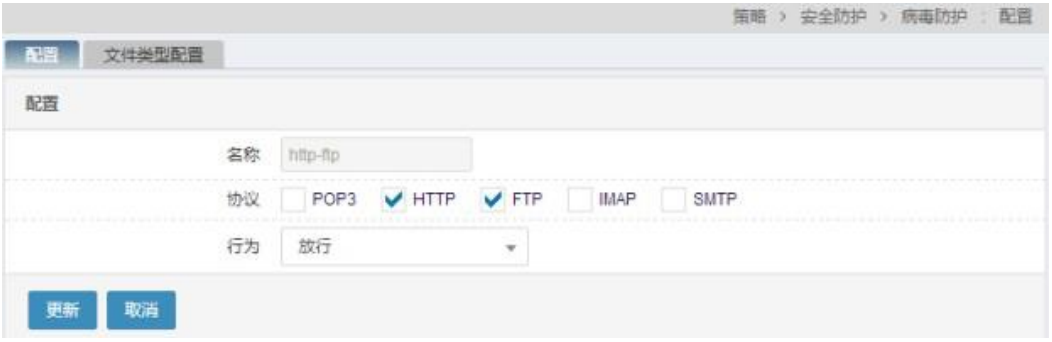
2.配置完毕后，点击**提交**。

48.2.2 编辑病毒防护模板

配置步骤：

1.进入**策略>安全防护>病毒防护**，对某条存在的模板点击名称进入编辑界面，ALL 为预置模板

2.可以对模板里面的协议和动作进行编辑修改，修改完毕后点击**更新**。



48.2.3 删除病毒防护模板

配置步骤：

1.进入**策略>安全防护>病毒防护**，如下图：

2.点击 删除模板。

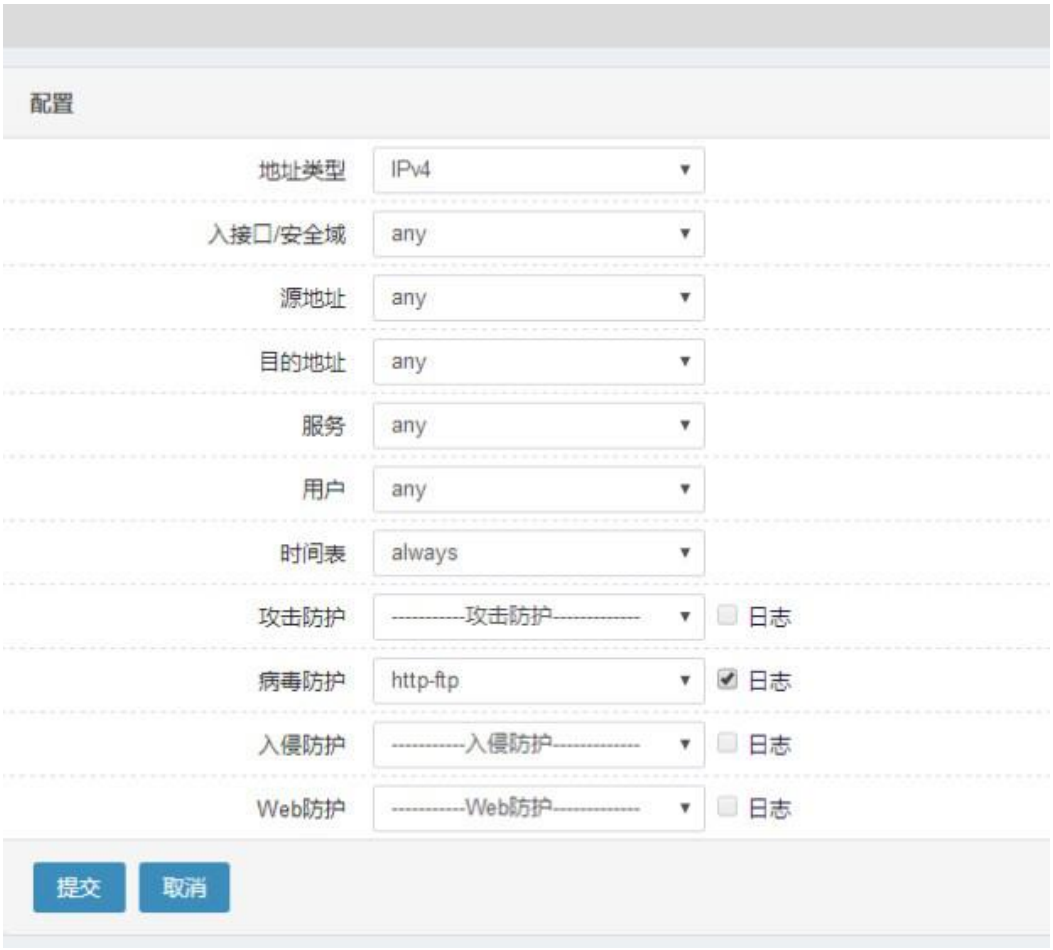
注意

被防护策略引用的模板和预置模板不能被删除。

48.2.4 防护策略引用病毒防护模板

配置步骤：

1.进入**策略>安全防护>防护策略**，点击**新建**，配置匹配条件，选择要引用的病毒防护模板



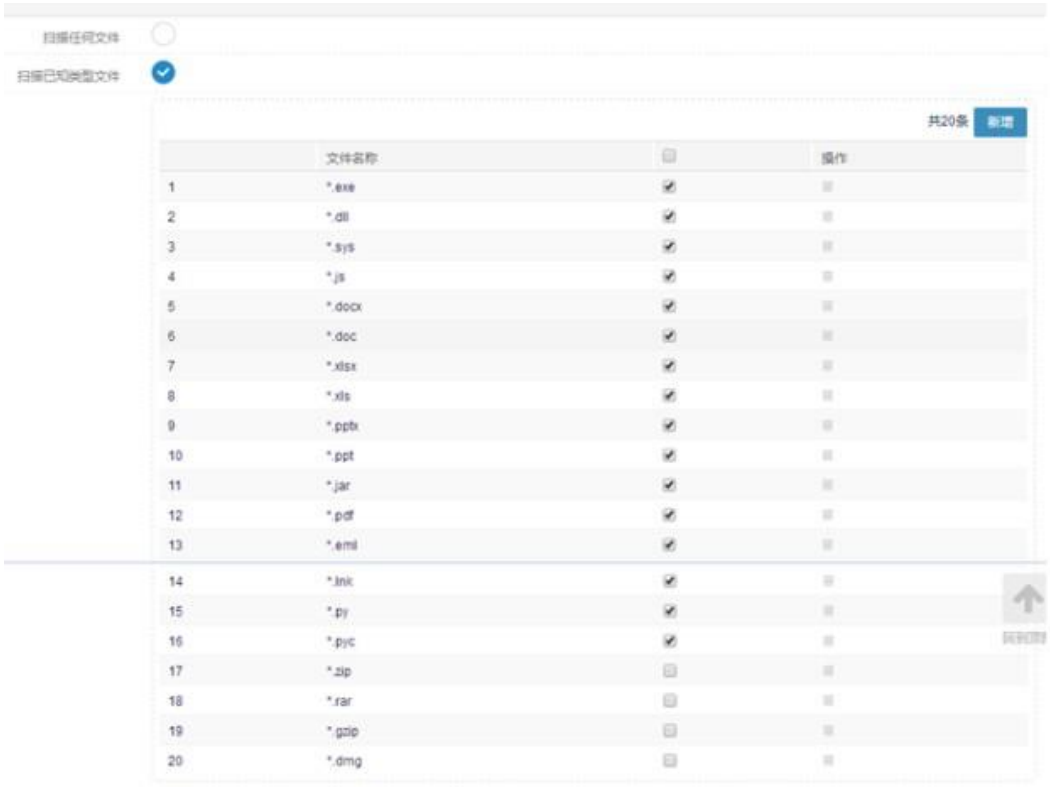
2.点击**提交**。

48.3 配置文件类型

48.3.1 文件扫描配置

配置步骤：

1. 进入**策略>安全防护>病毒防护>文件类型配置**，勾选**扫描已知类型文件**，允许对特定的文件类型进行文件扫描，有系统预定义的文件类型，也可以自己定义文件类型。



2. 勾选**扫描任何文件**，扫描经过设备的一切文件。

48.3.2 新增文件类型

配置步骤：

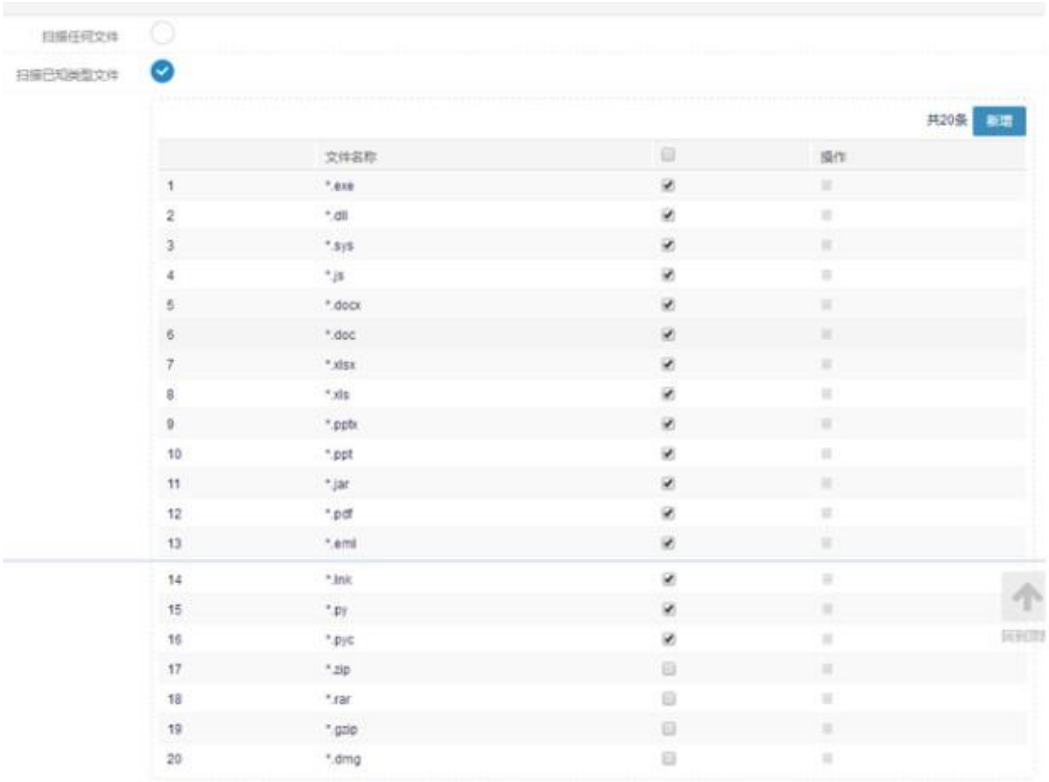
1. 进入**策略>安全防护>病毒防护>文件类型配置**，勾选**扫描已知类型文件**，点击**新增**

2. 配置好之后，点击**确定**

48.3.3 删除文件类型

配置步骤：

1. 进入**策略>安全防护>病毒防护>文件类型配置**，勾选**扫描已知类型文件**



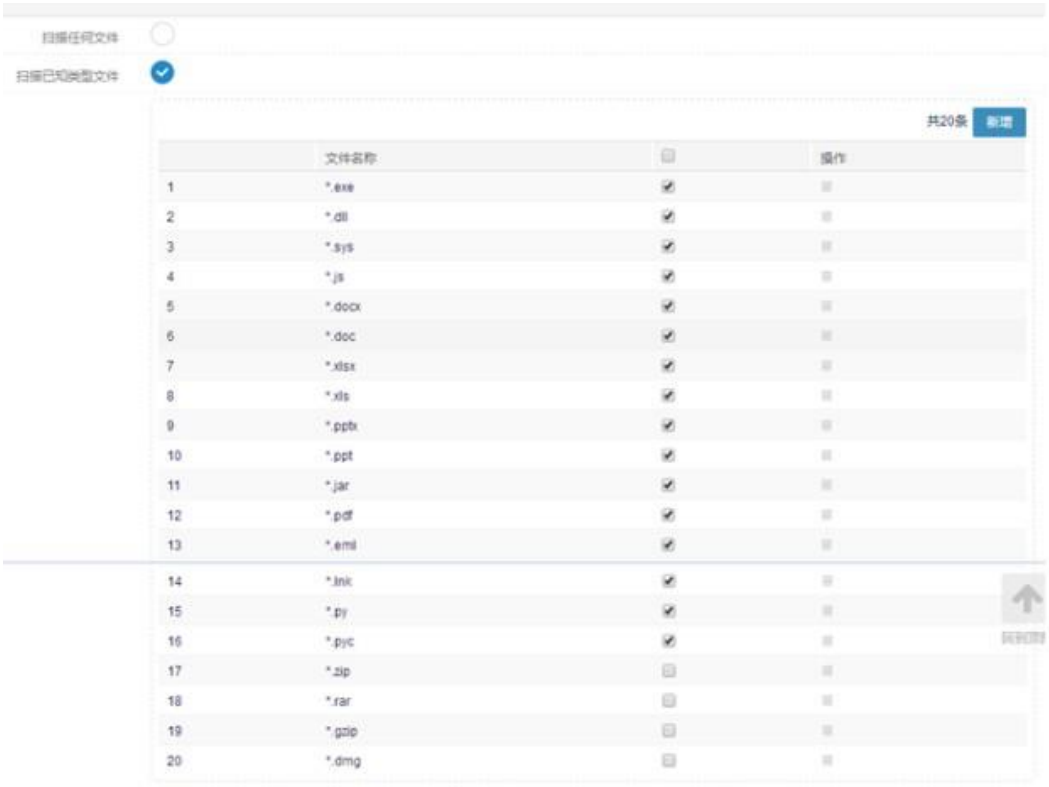
2. 选择需要删除的文件类型，点击 进行删除。

注意 预定义的文件类型，其删除按钮为灰色，不能被删除。

48.3.4 文件类型的启用和不启用

配置步骤：

1. 进入**策略>安全防护>病毒防护>文件类型配置**，勾选**扫描已知类型文件**



2. 选择需要启用或者不启用的文件类型，点击  进行启用，或者  不启用

3. 还可以点击最上面的按钮，全部启用和不启用。

48.4 配置案例

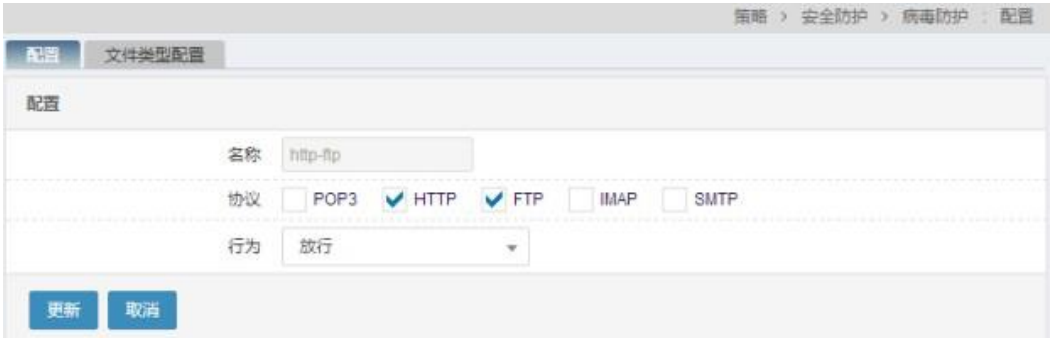
案例描述：

设备的 vlan1 连接内网，vlan2 连接外网。若内网的主机从外网下载文件，文件中带有病毒，就会触发设备病毒防护功能，根据配置对病毒文件做相应处理。

配置步骤：

1. 进入**对象>地址对象>地址节点**，配置地址对象“内网”和“外网”，如下图：

2. 进入**策略>安全防护>病毒防护**，点击**新建**。



3. 进入**策略>安全防护>病毒防护>文件类型配置，**勾选 **扫描任何文件**

4. 进入**策略>安全防护>防护策略**，点击**新建**，选择对应的参数，如下图：

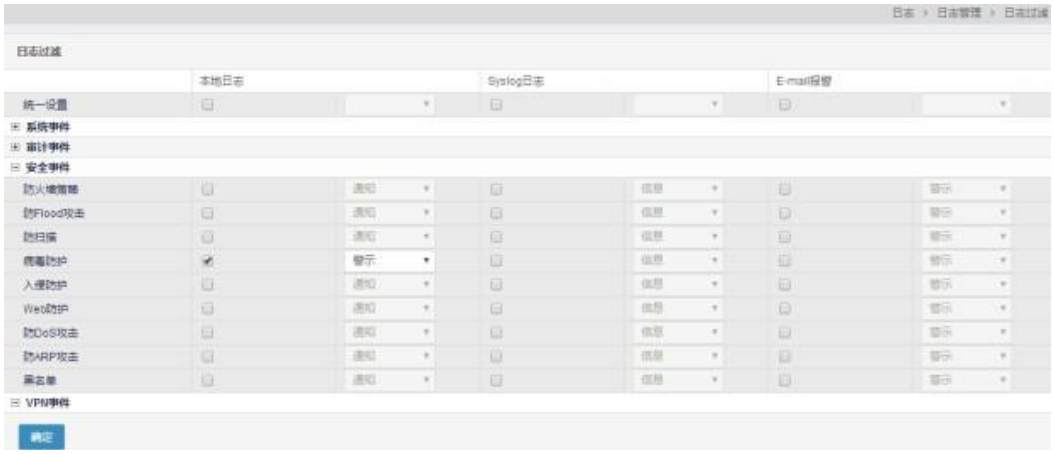
5. 点击**提交**

6. 进入**策略>安全防护>防护策略**，勾选**启用**完成配置，如下图：

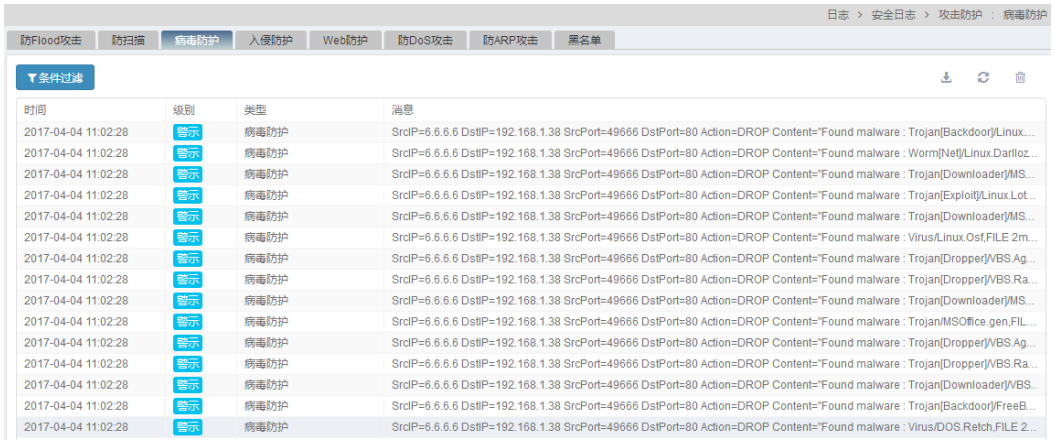
48.5 病毒防护监控

48.5.1 查看病毒防护日志

3. 进入**日志>日志管理>日志过滤**，勾选防病毒防护模块的相关日志，并设置日志的级别，点击**确定。**



4. 进入**日志>安全日志>攻击防护>病毒防护**里查看相关的病毒防护安全日志。



49 第49章 入侵防护

49.1 入侵防护概述

随着互联网的飞速发展，网络环境也变得越来越复杂，恶意攻击、木马、蠕虫病毒等混合威胁不断增大，单一的防护措施已经无能为力，企业需要对网络进行多层、深层的防护来有效保证其网络安全，而入侵防御系统(IPS)则是提供深层防护体系的保障。

防火墙设备入侵防御利用事件特征可以检测到特定的网络行为，并可以选择放行、阻断、阻断源 ip 等动作，以达到保护网络的目的。 防火墙设备入侵防御的事件特征库可以在启明星辰的网站上进行动态升级，以实时跟踪最新的网络威胁，保护网络的安全。

49.2 配置事件集

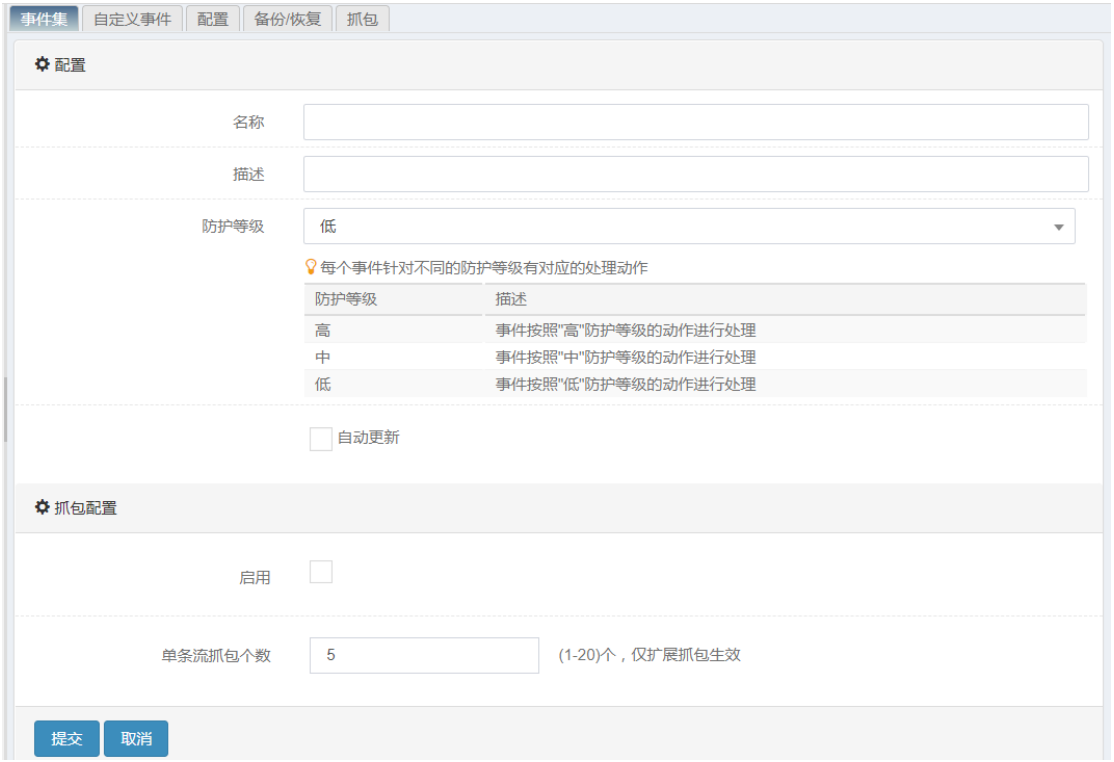
49.2.1 新建事件集

配置步骤：

1．进入**策略>安全防护>入侵防护**，如下图：

由粗体显示的事件集名称，是系统预定义的事件集。

2．点击**新建**，创建事件集，如下图：



参数说明：

名称：事件集名称。

描述：事件集的描述。

防护等级：事件集的防护等级。

自动更新：勾选后，自定义事件集会随入侵防护特征库的升级而更新事件，默认不启用。需要在 48.5 全局配置中进行相关配置。

抓包配置启用：该事件集是否启用抓包功能，默认不启用。

单条流抓包个数：扩展抓包每条流最大抓取的报文数量，默认值是 5。

3．配置完毕后，点击**提交**。

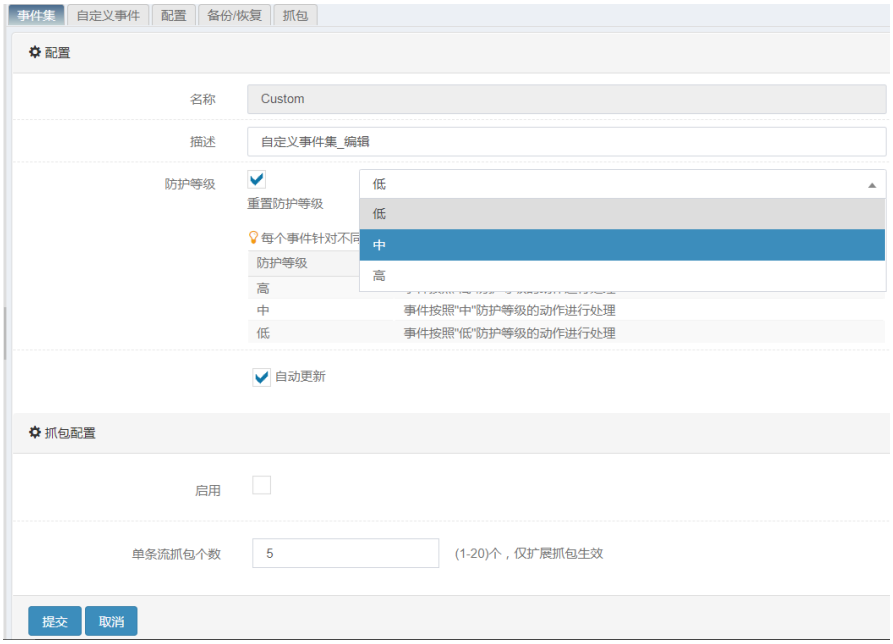
49.2.2 编辑事件集

配置步骤：

1．进入**策略>安全防护>入侵防护**，对于某条存在的事件集，点击 按钮进入编辑界面。

2.可以对事件集的描述、防护等级、自动更新、抓包配置进行编辑修改，

修改完毕后点击**提交**。



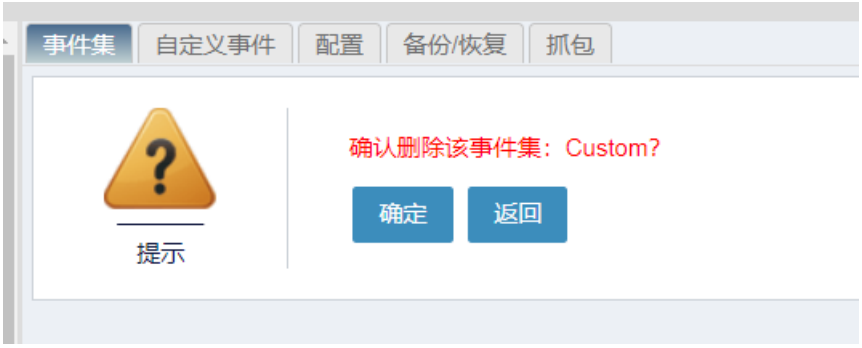
注意	编辑事件集时，选择重置防护等级，事件集里的事件的动作会被重置为相应防护等级对应的默认动作，不选择重置防护等级，事件集里事件的动作不会被改变。

49.2.3 删除事件集

配置步骤：

1. 进入**策略>安全防护>入侵防护**，如下图：

2. 对于某条存在的事件集，点击 按钮删除。



3. 点击**确定**，如下图。

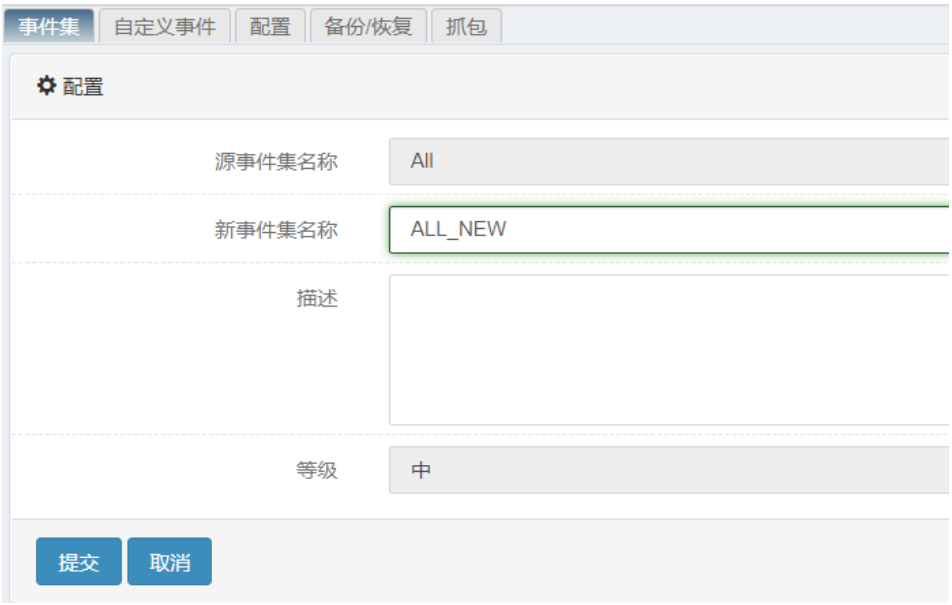
注意

预定义的事件集不能被删除，被防护策略引用的事件集也不能被删除。

49.2.4 复制事件集

配置步骤：

1. 进入**策略>安全防护>入侵防护**，，对于某条存在的事件集，点击 按钮进入复制界面。

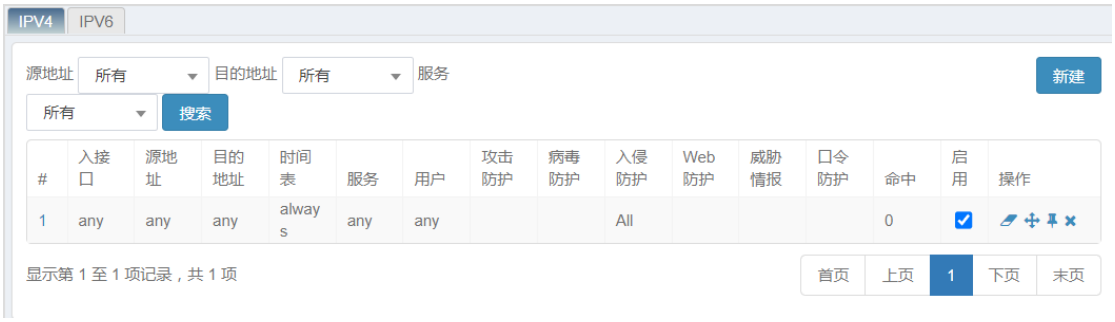


2. 配置完毕后，点击**提交**。

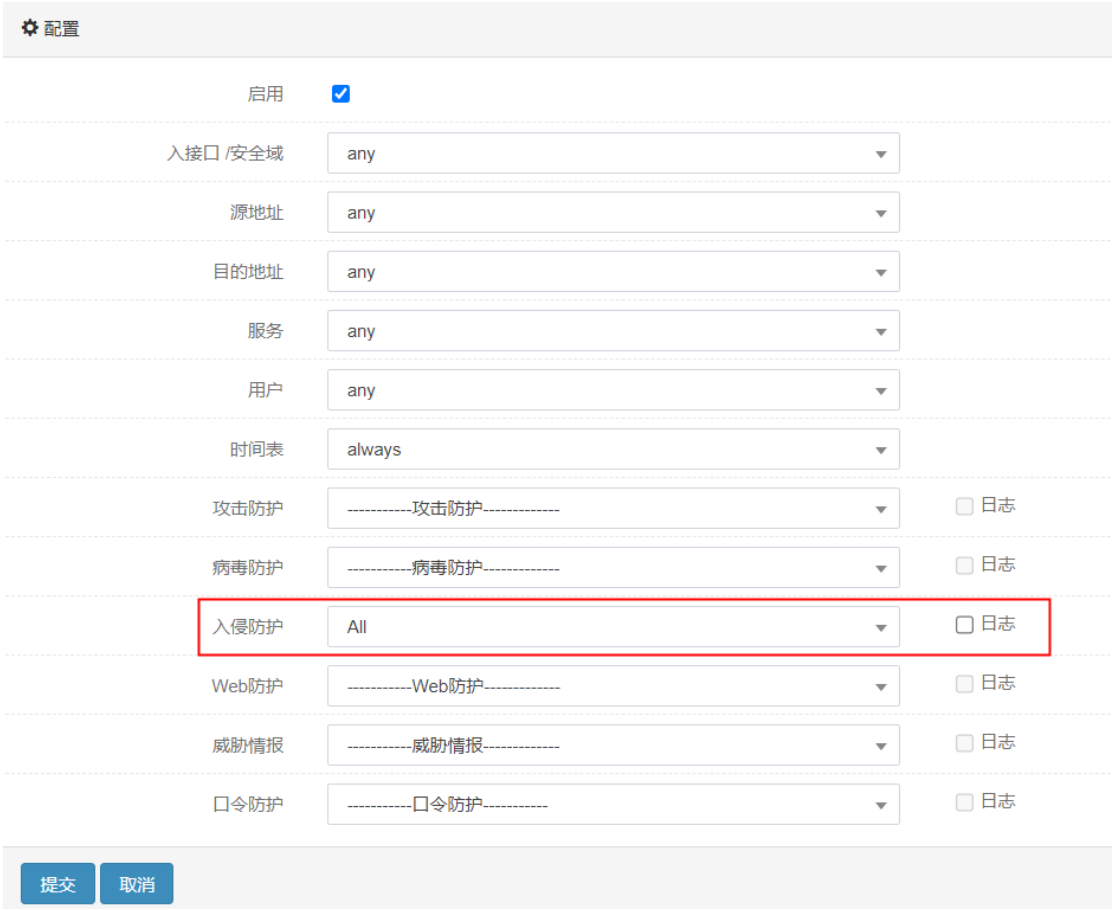
49.2.5 防护策略引用事件集

配置步骤：

1. 进入**策略>安全防护>防护策略**，如下图：



2. 点击**新建** ，创建防护策略。



3. 配置完成后，点击**提交** 。

49.3 事件集中事件配置

49.3.1 查看事件

配置步骤：

1. 进入**策略>安全防护>入侵防护**，

2. 点击事件集名称或者  ，查看事件集中的事件，如下图：

49.3.2 在线说明

配置步骤：

选择一个待检查的事件集（比如 All 事件集），点击名称之后进入展示该事件集包含所有事件的页面。然后将某种分类展开（例如展开“可疑行为”分类），通过点击事件名称的方式打开事件详细描述的方式进行查看 CNCVE 的展示，如下图所示：

注意

页面语言选择中文，描述为中文；

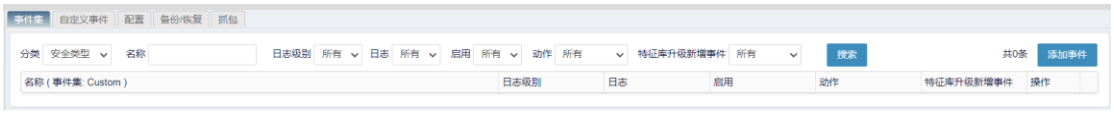
选择为英文，描述为英文。

并不是所有的事件都存在 CNVCEID，入侵防护特征库中如果存在 CNCVEID 页面上就会进行展示，如果没有则页面上不会有该字段的展示。

49.3.3 添加事件

配置步骤：

1. 进入**策略>安全防护>入侵防护**，
2. 点击事件集名称，进入到添加事件界面。



3. 点击**添加事件**，页面显示出可以添加的事件，如下图：

4. 勾选要添加的事件，或者是要添加的事件大类。
5. 配置完成后，点击**提交**。

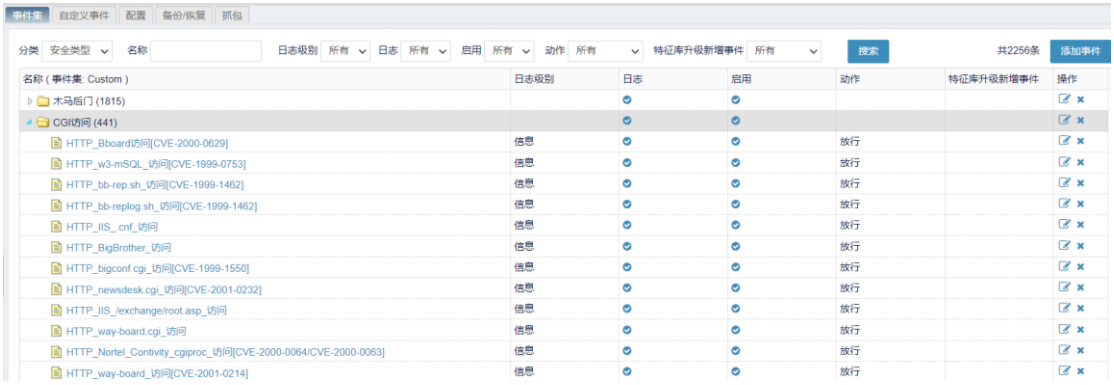
注意

一个事件被添加到事件集后，再次点击添加事件按钮，这个事件将不再显示。

49.3.4 删除事件

配置步骤：

1. 进入**策略>安全防护>入侵防护**，点击事件集名称，进入到编辑事件集中事件页面，

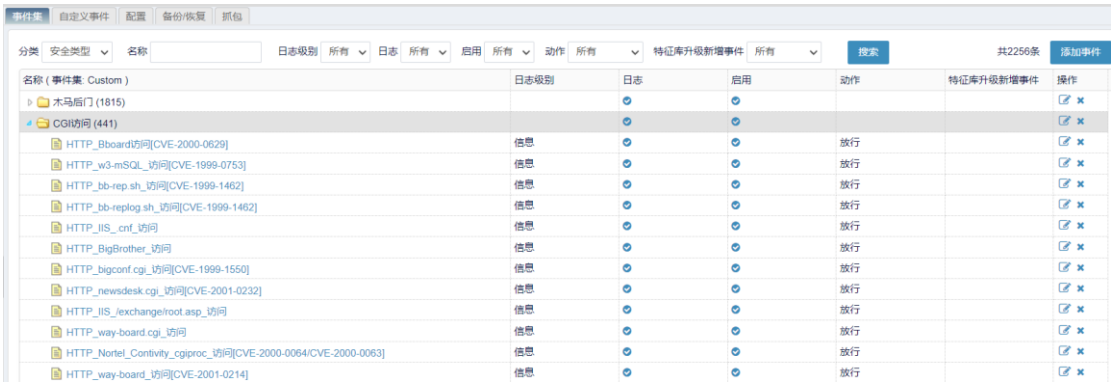


2. 点击  ，可以删除一个事件，或者一类事件。

49.3.5 编辑事件

配置步骤：

1. 进入**策略>安全防护>入侵防护**，点击事件集名称，进入到编辑事件集中事件页面，



2. 点击  ，修改事件配置，可以修改单个事件，也可以修改一类事件，如下图：

3. 修改完成后，点击**提交**。

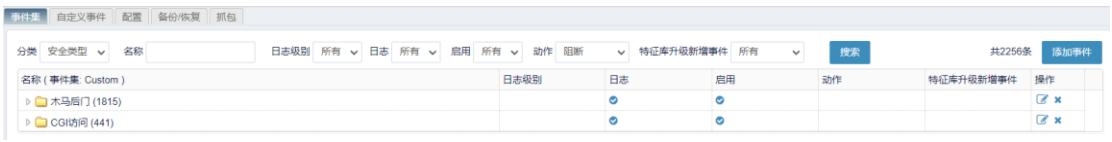
注意

编辑一类事件时，这类事件下所有事件配置都会被修改。

49.3.6 搜索事件

配置步骤：

1. 进入**策略>安全防护>入侵防护**，点击事件集名称，进入到编辑事件集中事件页面，
2. 可以在上面的搜索栏，输入搜索条件，点击**搜索**，如下图：



49.4 自定义事件配置

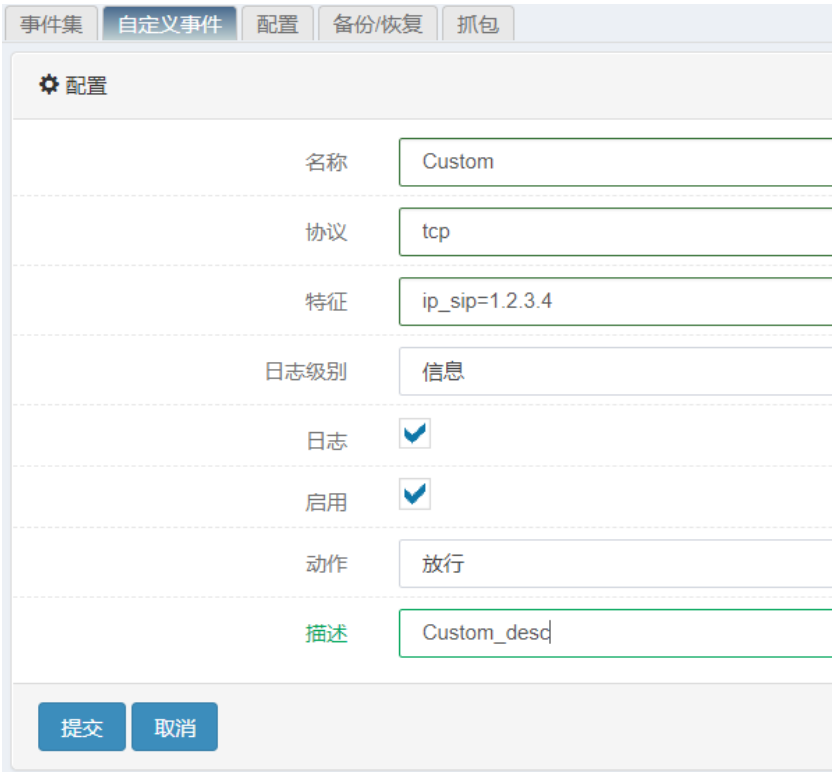
49.4.1 添加自定义事件

配置步骤：

1. 进入**策略>安全防护>入侵防护>自定义事件**，：

显示自定义事件，默认无。

2. 点击**新建**，如下图：



参数说明：

名称：自定义的事件名称。

特征：特征匹配串，描述方法见下面的注意说明。

级别：指定该事件的级别。

启用：是否启用该事件。

日志：是否对该特征事件进行日志记录。

动作：数据匹配该事件时的处理方式。

描述：可以对该事件进行简要说明，最多支持 127 个字符。

3. 配置完成后，点击**提交**。

注意

特征串支持如下描述方法：

1) 支持并且条件。如：icmp_type=8&icmp_payload^abcde

2) 支持多取值或的方式定义。如：icmp_type=0,8

3) 支持搜索偏移和深度定义。如：icmp_payload[10,100]^abcde

4) 支持多种运算符号，等于=，大于>，小于<，不等于~，包含^，不包含!

5) 支持转义符号%：

■ 转义 2 个 16 进制数为一个字节：
icmp_payload^abc%0a%0d

■ 转义表达式中特殊符号如'%'、'['、']'为它本来字符含义（不作特殊解释）：icmp_payload^abc%%defwxy

■ 有些特殊含义符号无法转义成为原有字符含义，比如',' '|', '&'这些符号作为表达式的逻辑关系，不能够使用%转义，建议使用这些字符的 16 进制数加%表示原有字符含义。

6) 支持大小写（不）敏感定义。默认使用大小写敏感方式，敏感方式需要在参数中指明，如：

■ icmp_payload^aBcD，表明大小写敏感

■ icmp_payload[,,nocase]^aBcD，表明大小写不敏感

■ icmp_payload[,,case]^aBcD，明确指明大小写敏感

7) 支持值类型参数，可以使用转义和不转义方式：默认对于使用转义符定义方式。不转义方式需要在参数中指明，如：

■ icmp_payload^abc%0adef

■ icmp_payload^[s]abc%20def

■ icmp_payload=[r]*abc.[c|h]

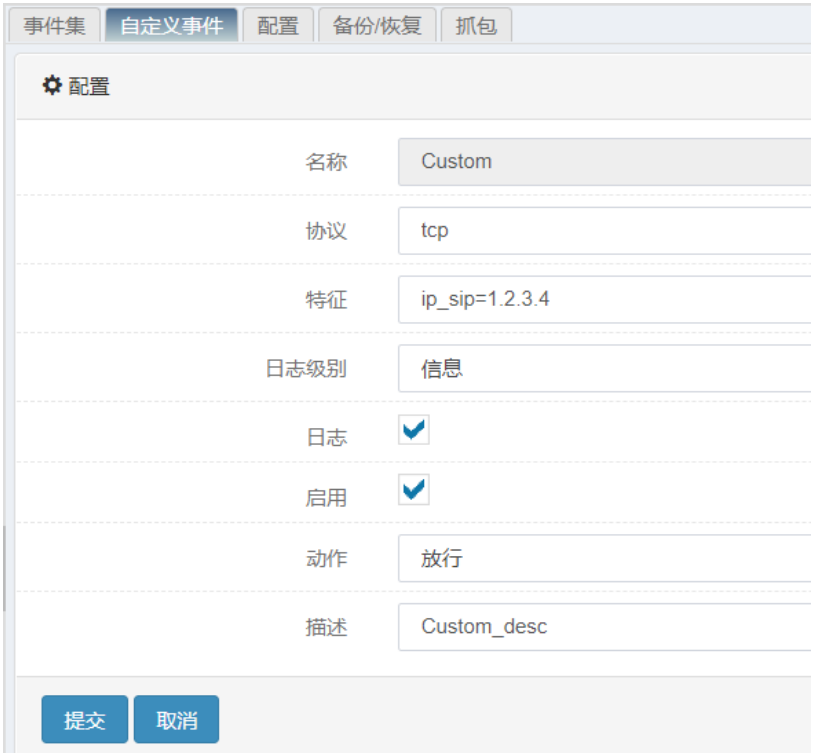
8) 支持值有效的定义方式：在表达式中仅使用协议变量名表示值有效：

■ telnet_user^root&telnet_passwd

49.4.2 编辑自定义事件

配置步骤：

1. 进入**策略>安全防护>入侵防护>自定义事件**，
2. 点击事件名称，进入编辑界面，如下图：



3. 配置完成后，点击**提交**

注意

创建自定义事件时，不能创建相同协议和特征的事件。

49.4.3 删除自定义事件

配置步骤：

1. 进入**策略>安全防护>入侵防护>自定义事件**，

2. 点击 ，删除单个自定义事件，如下图

3. 点击 ，清空所有的自定义事件。

注意

当有自定义事件被事件集引用时，不能执行清空操作，会显示清空失败。

49.4.4 引用自定义事件

配置步骤：

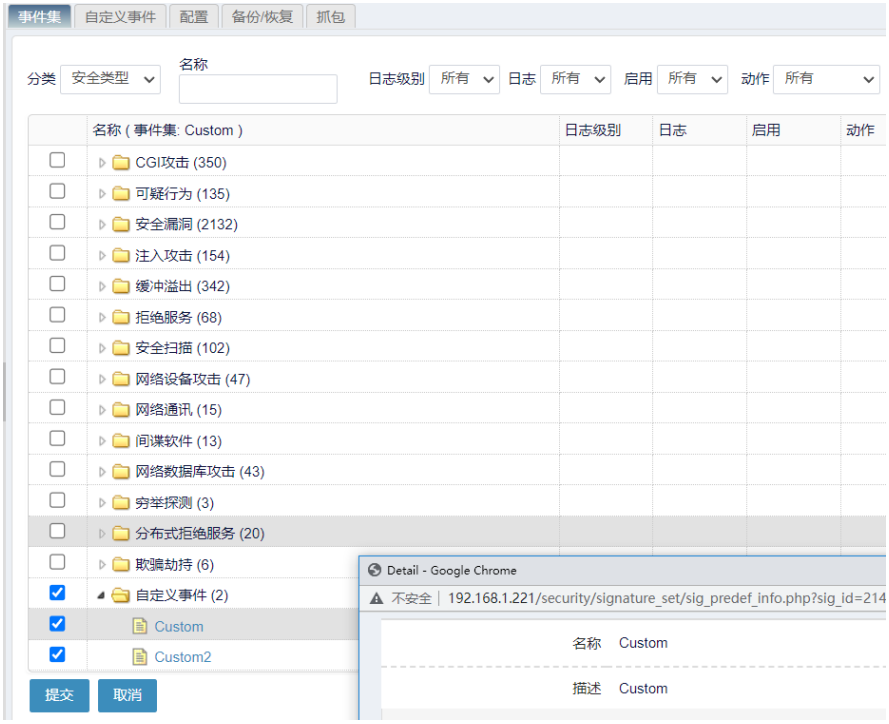
1. 进入**策略>安全防护>入侵防护**，点击要添加事件的事件集名称，进入到添加事件界面，
2. 点击**添加事件**，页面显示出可以添加的事件。

3. 选择自定义事件（可以选一个，也可以选所有），点击**提交。**

49.4.5 自定义事件在线说明

配置步骤：

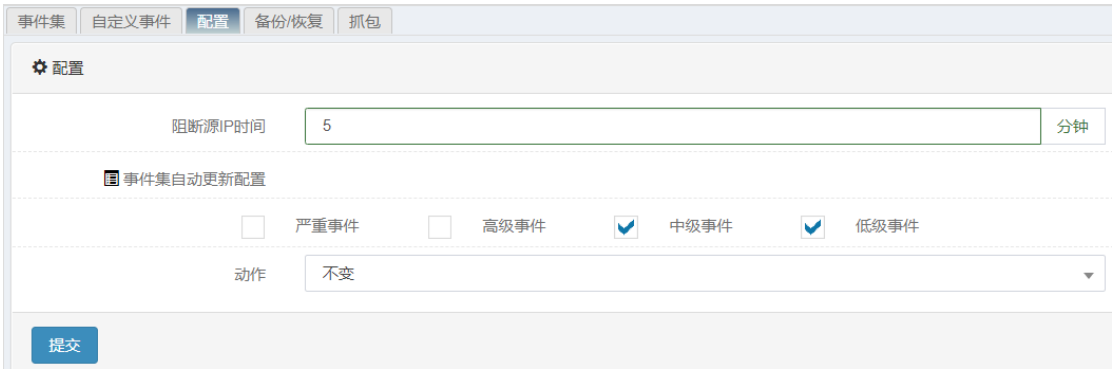
引用自定义事件时，点击事件名称，会显示出事件描述，如下图：



49.5 全局配置

配置步骤：

1. 进入**策略>安全防护>入侵防护>配置**，



参数说明：

阻断源 ip 时间：配置阻断源 ip 时间，默认 5 分钟

事件集自动更新配置：当某个自定义事件集勾选了自动更新时，入侵防护特征库升级后，会根据事件集自动更新配置将相应等级的新增事件添加到该自定义事件集中，并根据配置的动作修改新增事件在自定义事件集中的动作，默认动作是不变，即不改变新增事件的动作。

严重事件：将等级为严重的事件添加到勾选自动更新的事件集中。

高级事件：将等级为高级的事件添加到勾选自动更新的事件集中。

中级事件：将等级为中级的事件添加到勾选自动更新的事件集中。

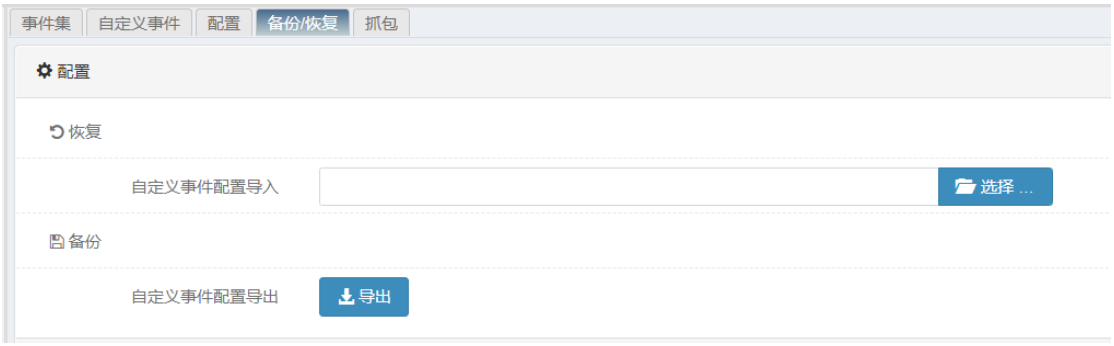
低级事件：将等级为低级的事件添加到勾选自动更新的事件集中。

动作：分为放行和不变，默认是不变。

2. 点击 **提交。**

49.6 自定义事件配置备份恢复

进入**策略>安全防护>入侵防护>备份恢复**



自定义事件配置导入：选择配置文件导入到设备中。

自定义事件配置导出：将设备中的配置文件导出。

49.7 IPS抓包

49.7.1 IPS抓包概述

可以通过启用 IPS 抓包功能，抓取实际网络中命中被引用的入侵防护事件的数据包，便于分析网络状态，追踪入侵防护模块的问题。

49.7.2 IPS抓包配置

进入**策略>安全防护>入侵防护>抓包**，可看到如下界面，配置抓包方式以及抓包时间后，点击在线抓包开关，在线抓包开启后，可以抓取命中事件的数据包。

参数说明：

在线抓包开关：是否开启 IPS 抓包，只有在开启状态下，才会抓取相应的报文。

抓包方式：单包抓包和扩展抓包两种。单包抓包只抓取命中事件的一个报文，扩展抓包会抓取命中事件及命中事件前的多个报文（扩展抓包可抓取的报文个数在事件集中配置，默认抓取 5 个）

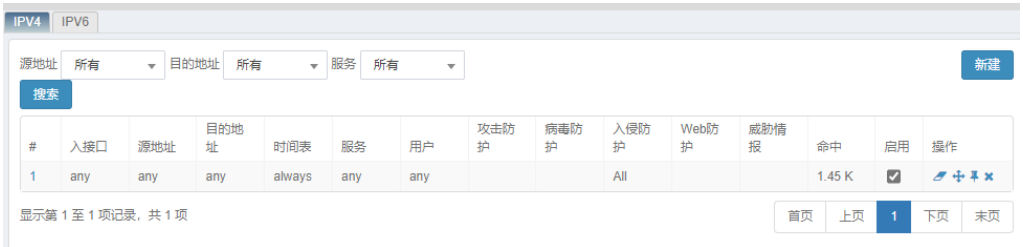
抓包时间：每次开启在线抓包的持续时间，最大十二小时。

注意

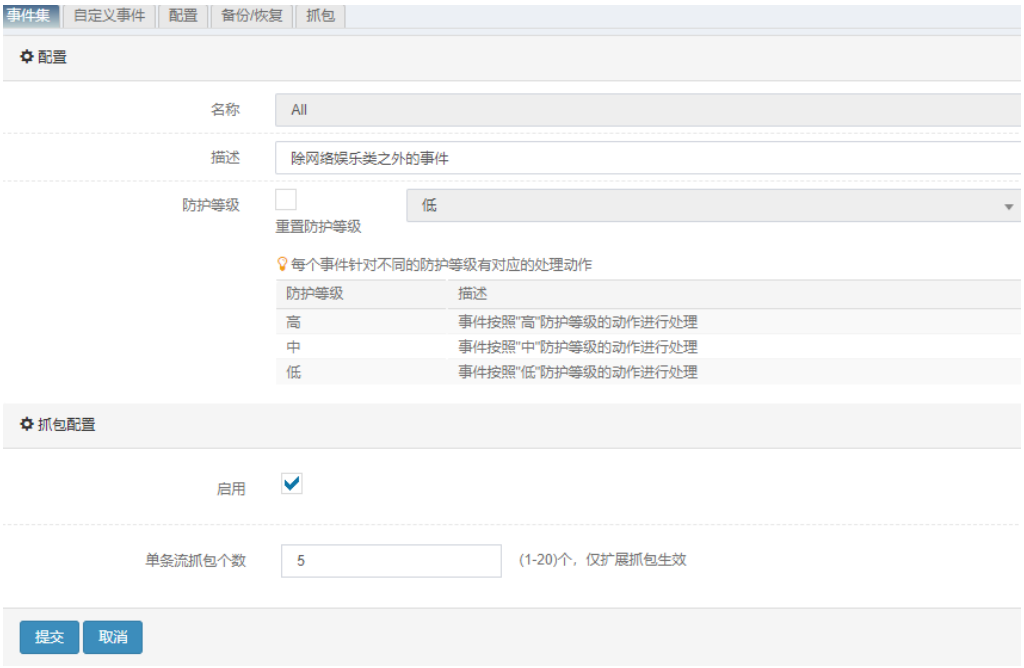
8. 只有对应事件集启用抓包后，在线抓包开关打开才能抓到命中事件集中事件的报文。
9. 最多可保存的文件个数与硬盘剩余空间大小有关，没有硬盘的设备最大保存 1000 个。

49.7.3 IPS抓包配置案例

1.进入**策略>安全防护>防护策略，**配置入侵防护引用 All 事件集，并启用策略

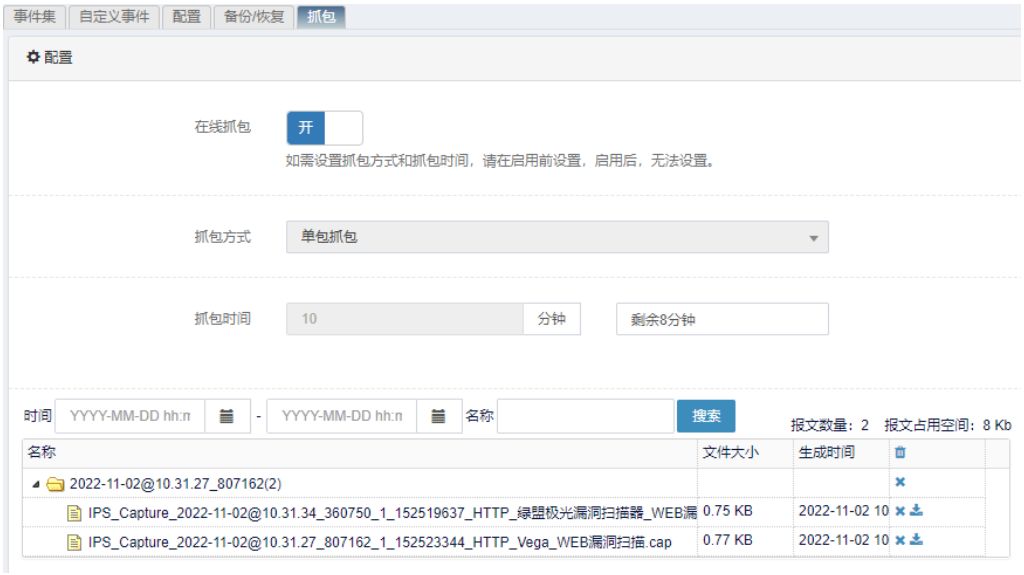


2.进入**策略>安全防护>入侵防护>事件集，编辑 All 事件集，抓包**配置启用，并配置单条流抓包个数，点击提交。



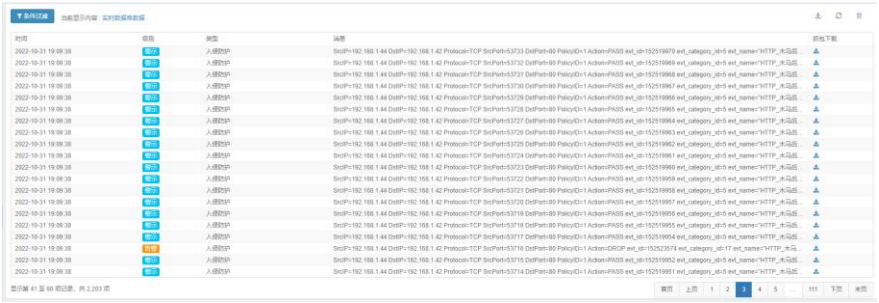
3.进入**策略>安全防护>入侵防护>抓包，**配置抓包方式和抓包时间，启用在线抓包

4.在配置的抓包时间内，有流量触发 All 事件集中的事件后，抓包页面会展示抓到的报文：



点击报文后的  ，可下载报文进行分析。下载后可使用 wireshark 软件打开查看。

如果入侵防护启用了本地日志功能，到日志>安全日志>入侵防护中，可以看到抓到攻击报文的日志后面多了一个  ，可下载报文进行分析。



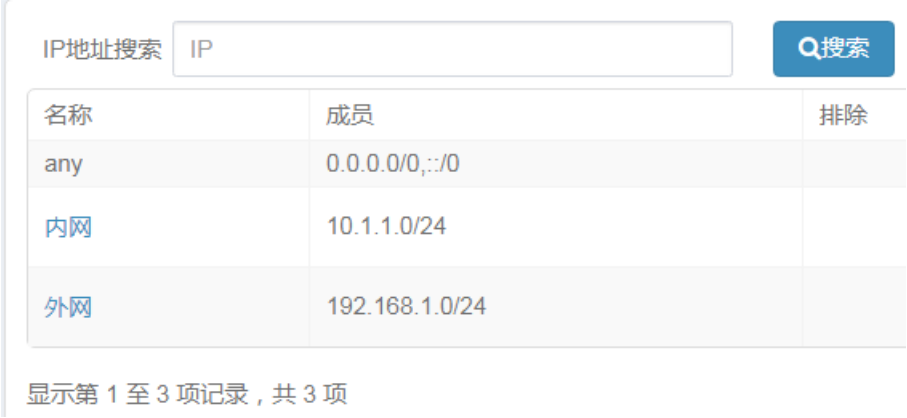
49.8 配置案例

案例描述：

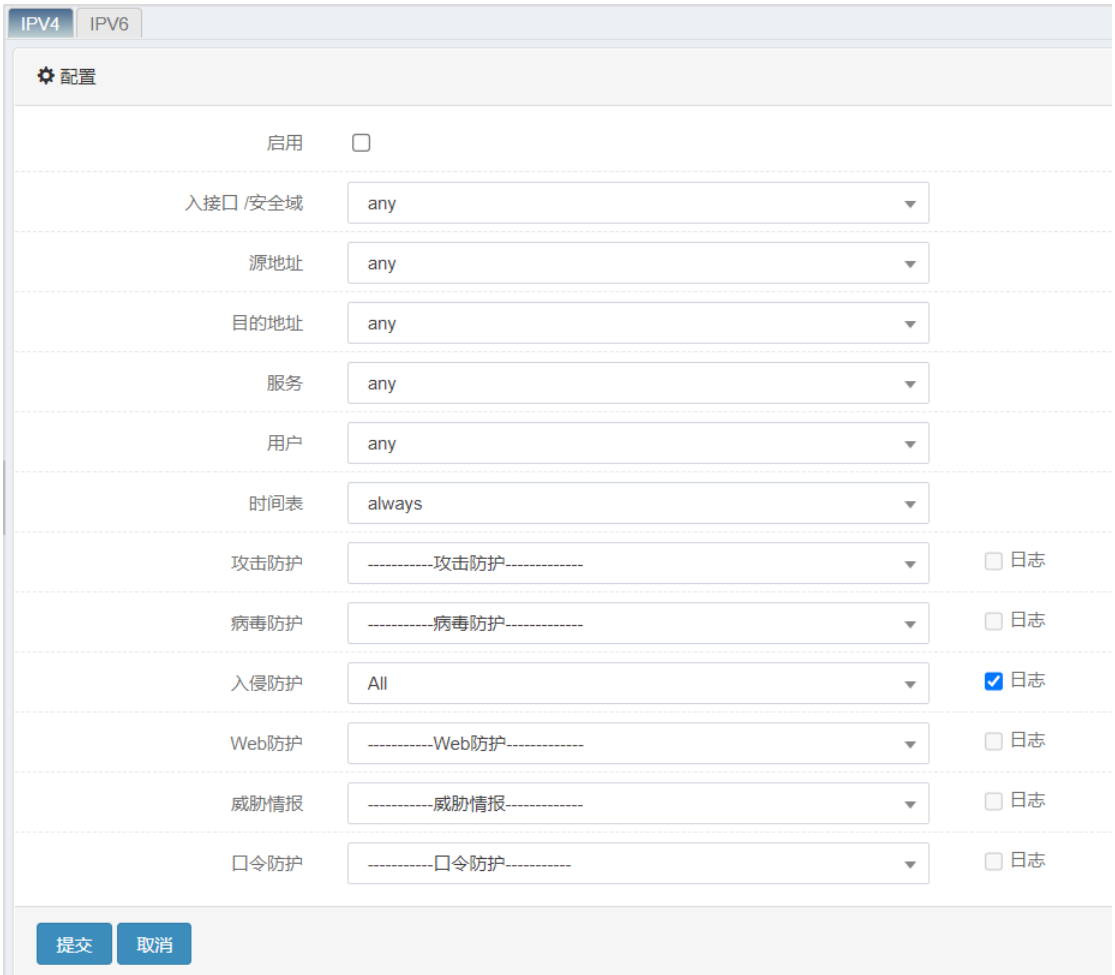
设备的 vlan1 连接内网，vlan2 连接外网。内网访问外网，若外网带有恶意攻击、木马、蠕虫病毒等威胁，就会触发设备入侵防护功能，检测入侵事件类型，根据配置对入侵事件做相应处理。

配置步骤：

1.进入**对象>地址对象>地址节点**，配置地址对象“内网”和“外网”，如下图：

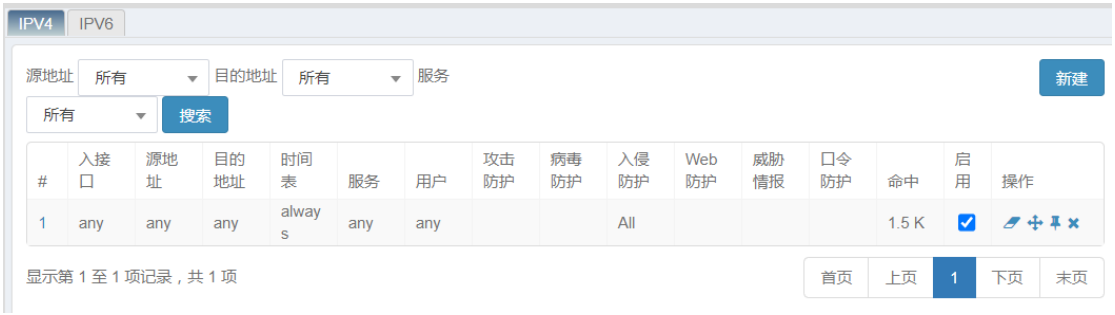


2.进入**策略>安全防护>防护策略**，点击**新建**，选择对应的参数，如下图：



3.点击**提交**

4.进入**策略>安全防护>防护策略**，勾选**启用**完成配置，如下图：

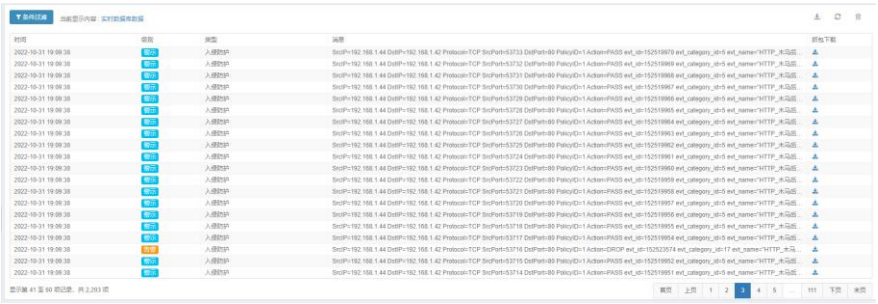


49.9 入侵防护监控

49.9.1 查看入侵防护日志

1.进入**日志>日志管理>日志过滤**，勾选防入侵防护模块的相关日志，并设置日志的级别，点击**确定**。

2.进入**日志>安全日志>入侵防护**里查看相关的入侵防护安全日志。



50 第50章 Web 防护

50.1 Web防护概述

Web 防护策略防护的攻击有两种，分别是 XSS 攻击和 SQL 注入攻击。XSS 是一种经常出现在 web 应用中的计算机安全漏洞，它允许恶意 web 用户将代码植入到提供给其它用户使用的页面中，这些代码包括 HTML 代码和客户端脚本。SQL 注入攻击也是黑客对数据库进行攻击的常用手段之一，该攻击针对相当大一部分代码没有对用户输入数据的合法性进行判断的现状，通过提交一段数据库查询代码，根据程序返回的结果，获得某些数据。

本模块基于特征库的方式对两种攻击进行防御，针对两种攻击采用特征匹配的方式，对通过 HTTP 提交的信息采用模式匹配的方式进行检查，发现符合 xss/sql 特征的攻击，即提交日志，并根据预设的动作阻断或者放行连接。

50.2 配置Web防护

50.2.1 配置策略的基本要素

Web 防护策略的基本要素是名称和 SQL 攻击防护开关和 XSS 攻击防护开关。建立好模板策略的两种攻击动作有“放行”，“拒绝”。

配置步骤：

1. 进入**策略>安全防护>Web 防护**，点击新建。

参数说明：

名称：该策略的名称。

SQL 注入：SQL 注入攻击防护的开关。

动作：放行或阻断。

XSS 攻击：XSS 攻击防护的开关。

动作：放行或阻断。

2. 配置完毕后，点击**提交**。

创建一条新的 Web 防护策略时，名称是唯一的标识，SQL 攻击和 XSS 攻击只有启用了才会生效。

50.2.2 编辑Web防护

配置步骤：

1. 进入**策略>安全防护>Web 防护**，对某条存在的 Web 防护策略点击策略的名字进入编辑界面。

2. 可以对 Web 防护策略里面的内容进行编辑修改，修改完毕后点击**提交。**

Web 防护会有一个默认的开启 SQL 注入攻击和 XSS 攻击的 default 模板。

50.2.3 删除Web防护策略

配置步骤：

1. 进入**策略>安全防护>Web 防护策略**，如下图：


新建
过滤:
名称
SQL注入
动作
XSS攻击
动作
操作
default
阻断
阻断
防护
阻断
阻断
显示第 1 至 2 项记录，共 2 项

2. 点击 删除策略。

51 第51章 威胁情报

51.1 威胁情报概述

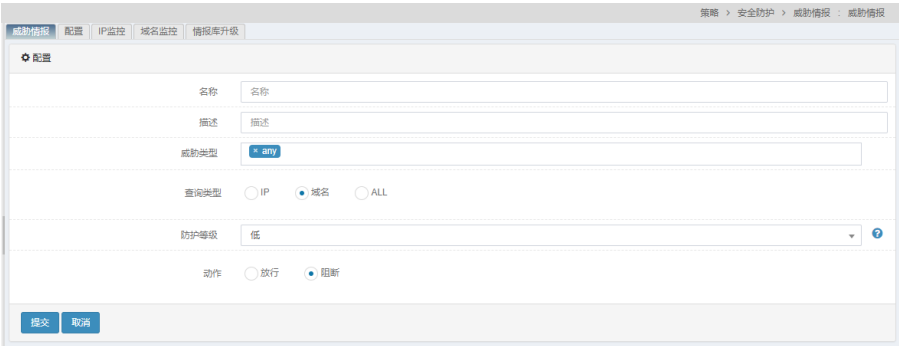
威胁情报防护通过查询离线库和云端平台得到 IP 地址和域名的威胁情况，对用户访问的目的 IP 地址和域名进行威胁分类和威胁等级检查，如果发现有 IP 地址或者域名的威胁情况超过策略中设置的防护等级，即提交日志，并根据预设的动作阻断或者放行。

51.2 配置威胁情报

51.2.1 配置威胁情报

配置步骤：

1. 进入**策略>安全防护>威胁情报**，点击新建。



参数说明：

名称：该策略的名称。

描述：该策略的描述。

威胁类型：该策略可匹配的威胁类型，共有 17 种。

查询类型：查询类型有三种，IP、域名和 ALL（IP 和域名）。

防护等级：防护等级有高、中、低三种。

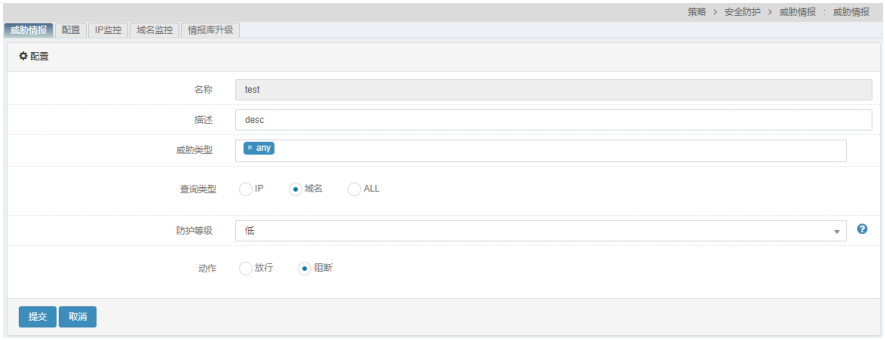
动作：放行或阻断。

2. 配置完毕后，点击**提交**。

51.2.2 编辑威胁情报

配置步骤：

1. 进入**策略>安全防护>威胁情报**，对某条存在的威胁情报策略点击策略的名字进入编辑界面。



2. 可以对威胁情报策略里面的内容进行编辑修改，修改完毕后点击**提交**。

51.2.3 删除威胁情报

配置步骤：

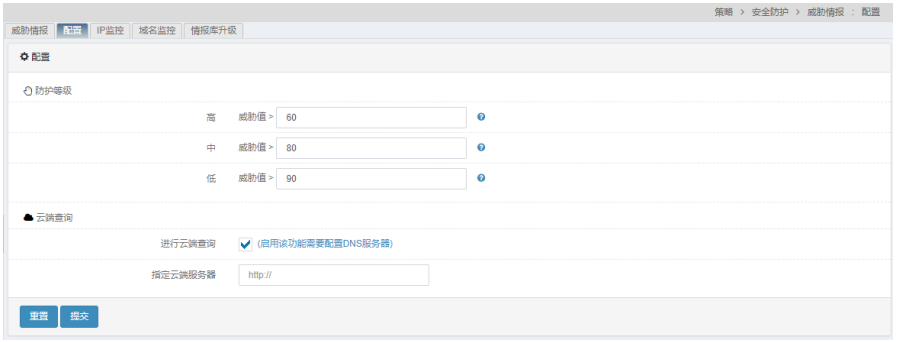
1. 进入**策略>安全防护>威胁情报**，如下图：

2. 点击 删除策略。

51.2.4 配置防护等级

配置步骤：

1. 进入**策略>安全防护>威胁情报**，点击“配置”选项卡进入防护等级配置界面。

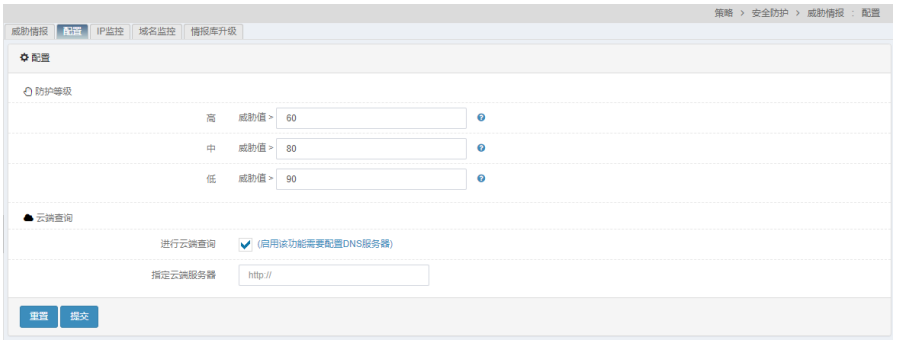


2. 可以对威胁情报策略的防护等级进行修改，修改完毕后点击**提交。**

51.2.5 配置云端查询

配置步骤：

1. 进入**策略>安全防护>威胁情报**，点击“配置”选项卡进入云端查询配置界面。

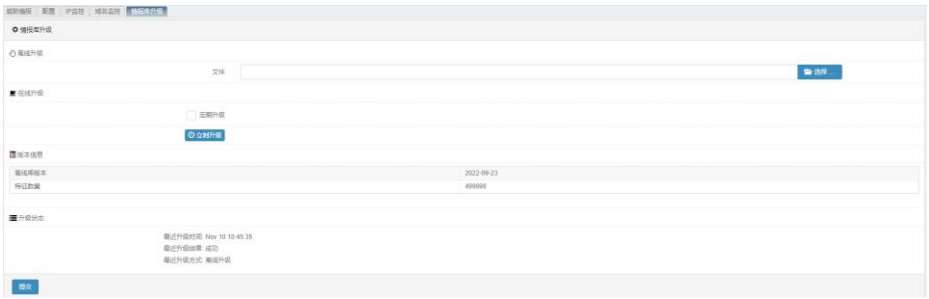


2. 选择是否开启云端查询，可以指定云端查询服务器，修改完毕后点击**提交。**

51.2.6 情报库升级

设备可以离线、在线升级情报库版本。

1. 进入**策略>安全防护>威胁情报**，点击“情报库升级”选项卡进入升级界面。



离线升级:

文件：点击**选择**按钮，选中对应的情报库文件，点击“**升级**”即可

采用手动升级功能时，需要保证升级文件为合法的情报库文件。

在线升级：

定期升级: 启用定期自动升级。

时间: 设置每天自动升级的时间点。

配置好后，点击**提交**。

立即升级：点击此按钮后，系统立即在线升级。

51.3 配置案例

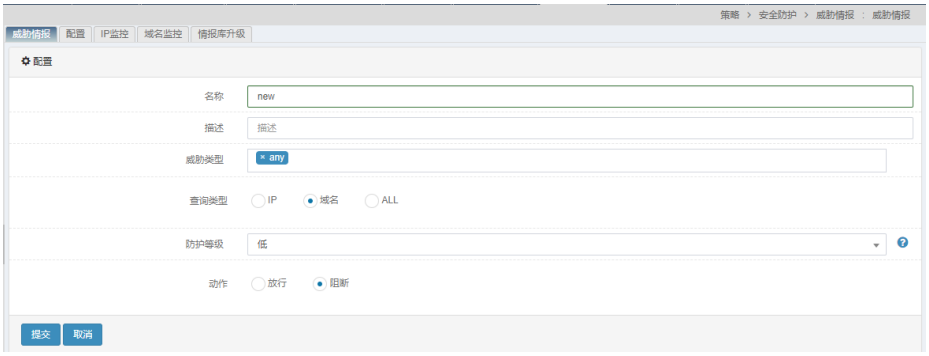
案例描述：

设备的 vlan1 连接内网，vlan2 连接外网。内网访问外网，若检测到内网访问的 IP 地址或者域名威胁值超过策略配置的防护等级，就会触发设备威胁情报防护功能，根据配置做相应阻断或者放行处理。

配置步骤：

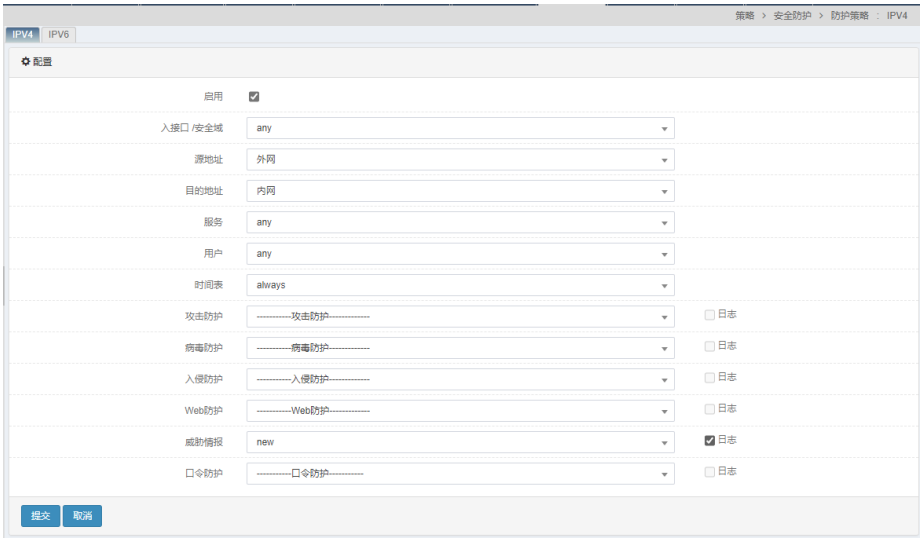
1.进入**对象>地址对象>地址节点**，配置地址对象“内网”和“外网”，如下图：

2. 进入**策略>安全防护>威胁情报**，点击新建。



3.点击**提交**

4.进入**策略>安全防护>防护策略**，点击**新建**，选择对应的参数，如下图：



5.点击**提交**

6.进入**策略>安全防护>防护策略**，勾选**启用**完成配置，如下图：

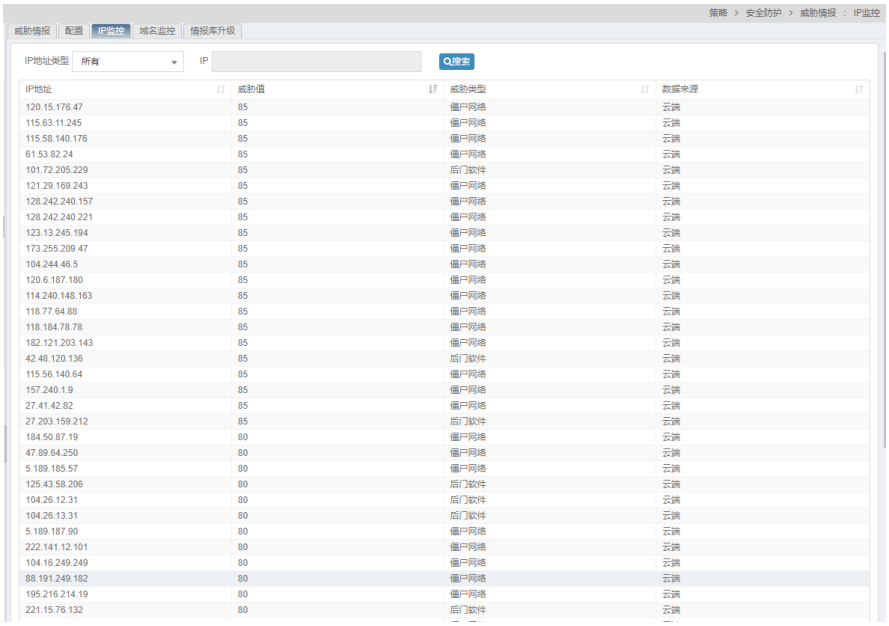
51.4 威胁情报监控

51.4.1 查看IP地址威胁监控

配置步骤：

1. 进入**策略>安全防护>威胁情报**，点击“IP 监控”选项卡进入 IP 地址

监控界面。如下图：



51.4.2 查看域名威胁监控

配置步骤：

1. 进入**策略>安全防护>威胁情报**，点击“域名监控”选项卡进入域名监控界面。如下图：

52 第52章 Dos 防护

52.1 防攻击概述

防 DOS(Denial of Service)攻击设计的目标就是要使设备能够阻止外部的恶意攻击，同时还能使内网正常地与外界通信。不仅保护设备，更要保护内网。当遭受到攻击时，向用户进行报警提示。

常见的 DOS 攻击主要包括 PING of death、tear drop attack、jolt2 attack、syn fragment、land-base、winnuke、smurf 等。

扫描也是网络攻击的一种，攻击者在发起网络攻击之前，通常会试图确定目标上开放的 TCP/UDP 端口，而一个开放的端口通常意味着某种应用。

常见的扫描主要有：

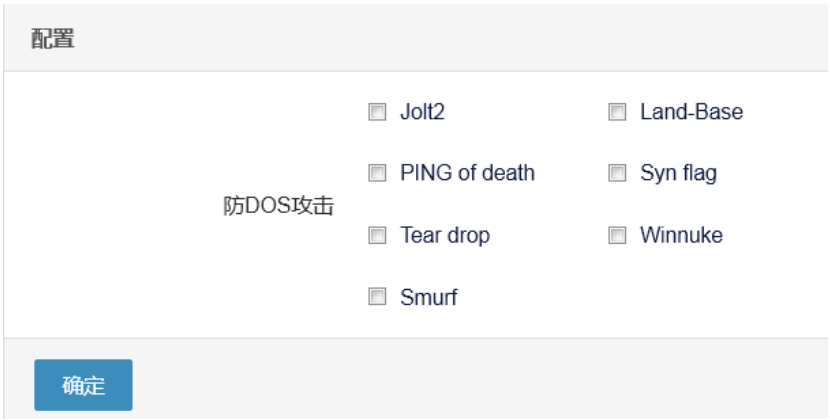
- 垂直（Vertical）扫描：针对相同主机的多个端口
- 水平（Horizontal）扫描：针对多个主机的相同端口
- ICMP (PING) sweeps：针对某地址范围，通过 PING 方式发现存活主机

T 系列防火墙可以有效防范以上几类扫描，从而阻止外部的恶意攻击，保护设备和内网。当检测到此类扫描探测时，向用户进行报警提示。

52.2 配置防攻击

配置步骤：

1. 进入**策略>安全防护>Dos 防护>配置**。



防 DOS 攻击

Jolt2：Jolt2 攻击通过向目的主机发送报文偏移加上报文长度超过 65535 的报文，使目的主机处理异常而崩溃。

配置了防 Jolt2 攻击功能后，T 系列防火墙可以检测出 Jolt2 攻击，丢弃攻击报文并输出告警日志信息。

Land-Base：Land-Base 攻击通过向目的主机发送目的地址和源地址相同的报文，使目的主机消耗大量的系统资源，从而造成系统崩溃或死机。

配置了防 Land-Base 攻击功能后，T 系列防火墙可以检测出 Land-Base 攻击，丢弃攻击报文并输出告警日志信息。

PING of death：PING of death 攻击是通过向目的主机发送长度超过 65535 的 ICMP 报文，使目的主机发生处理异常而崩溃。

配置了防 PING of death 攻击功能后，T 系列防火墙可以检测出 PING of death 攻击，丢弃攻击报文并输出告警日志信息。

Syn flag：Syn-flag 攻击通过向目的主机发送错误的 TCP 标识组合报文，浪费目的主机资源。

配置了防 Syn-flag 攻击功能后，T 系列防火墙可以检测出 Syn-flag 攻击，丢弃攻击报文并输出告警日志信息。

Tear drop：Tear-drop 攻击通过向目的主机发送报文偏移重叠的分片报文，使目的主机发生处理异常而崩溃。

配置了防 Tear-drop 攻击功能后，T 系列防火墙可以检测出 Tear-drop 攻击，并输出告警日志信息。因为正常报文传送也有可能出现报文重叠，因此 T 系列防火墙不会丢弃该报文，而是采取裁减、重新组装报文的方式，发送出正常的报文。

Winnuke：Winnuke 攻击通过向目的主机的 139、138、137、113 端口发送 TCP 紧急标识位 URG 为 1 的带外数据报文，使系统处理异常而崩溃。

配置了防 Winnuke 攻击功能后，T 系列防火墙可以检测出 Winnuke 攻击报文，将报文中的 TCP 紧急标志位为 0 后转发报文，并可以输出告警日志信息。

Smurf：这种攻击方法结合使用了 IP 欺骗和 ICMP 回复方法使大量网络传输充斥目标系统，引起目标系统拒绝为正常系统进行服务。Smurf 攻击通过使用将回复地址设置成受害网络的广播地址的 ICMP 应答请求(PING)数据包，来淹没受害主机，最终导致该网络的所有主机都对此 ICMP 应答请求做出答复，导致网络阻塞。

2．配置完成后，点击**提交**。

52.3 配置案例

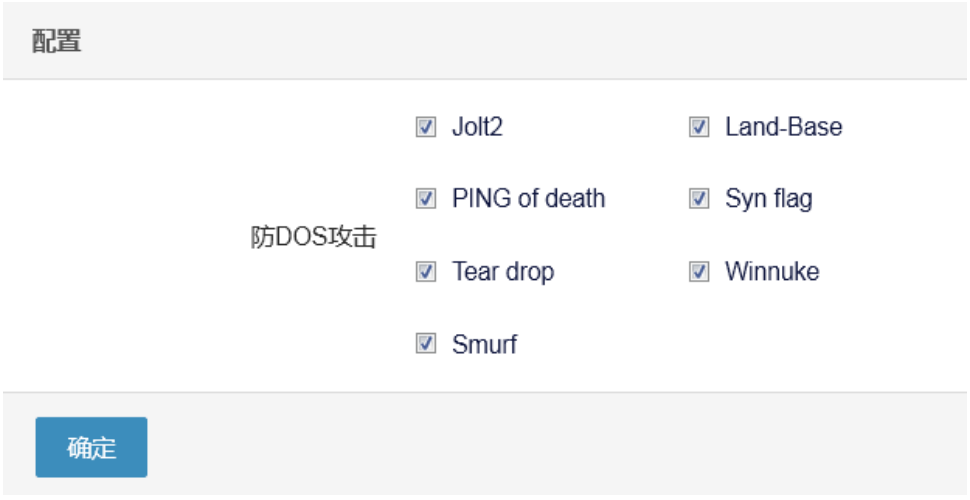
52.3.1 案例1：配置防DOS攻击

案例描述：

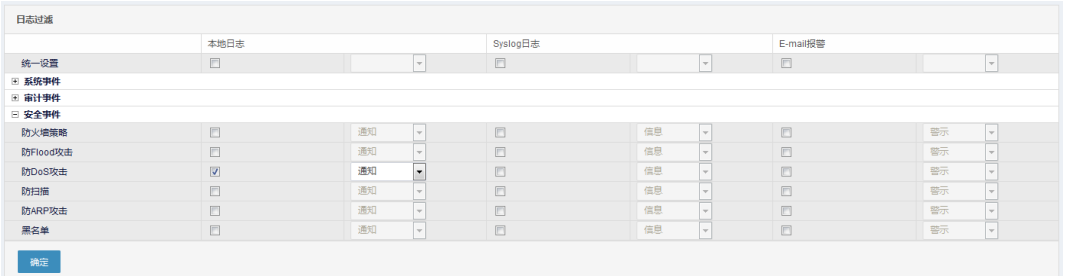
当网络上出现大量的攻击报文时，可通过抓包或查看流信息判断是否受到攻击。攻击报文将会占用大量的资源，影响我们所保护主机的性能，也影响设备的性能。这时要通过抓包或查看流信息来查看受到了何种攻击，并启用对应的防攻击，从而保护内网和设备。若设备收到目的地址和源地址相同的报文，则触发设备的 Land-Base 攻击防护功能，设备将攻击报文丢弃，并发出告警信息。

配置步骤：

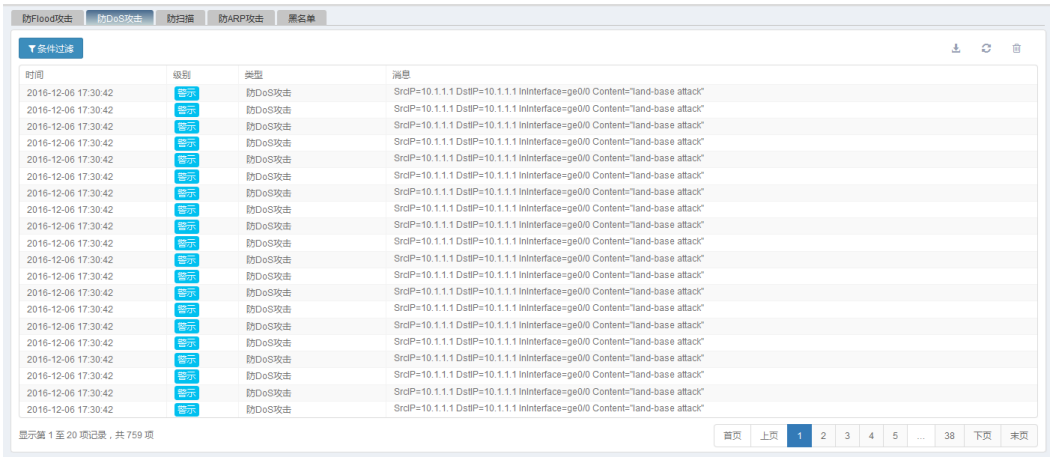
1. 进入**策略>安全防护>DoS 防护>配置**，如下图：



2. 点击**确定**完成设置。
3. 进入**日志>日志管理>日志过滤**，勾选防 DoS 攻击模块的相关日志，并设置日志的级别，点击**确定**。



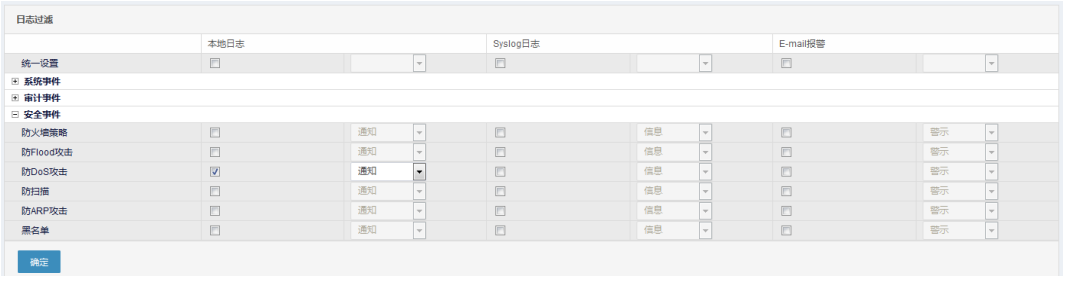
4. 进入**日志>安全日志>防 DoS 攻击**里查看相关的防 DoS 攻击安全日志。



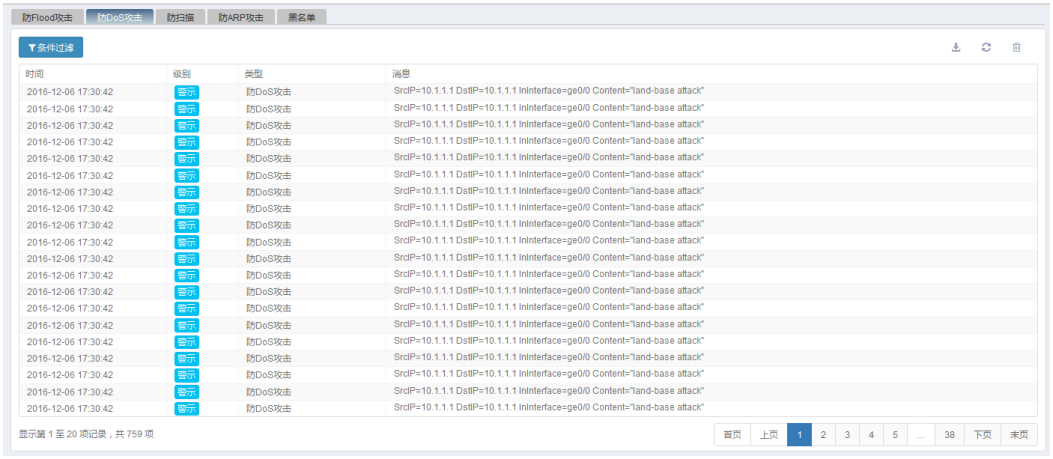
52.4 防攻击监控与维护

52.4.1 查看防攻击日志

1. 进入**日志>日志管理>日志过滤**，勾选防 DoS 攻击模块的相关日志，并设置日志的级别，点击**确定**。



2. 进入**日志>安全日志防 DoS 攻击**里查看相关的防 DoS 攻击安全日志。



52.5 常见故障分析

52.5.1 故障现象：SYN Flood攻击防御失效

现象	SYN Flood的攻击防御失效，SYN Flood报文穿过T1T系列防火墙。
分析	SYN Flood攻击防御失效的原因可能有以下几个：防SYN Flood攻击的服务没有启动或者攻击门限设置过高。
解决	1．查看系统中的TCP半连接数是否有显示，如果TCP半连接数为“-”，表示IP Inspect模块没有启动。 2．查看配置中防SYN Flood攻击服务是否是启动的，如果未启动，启动防SYN Flood攻击服务。 3．查看攻击门限设置是否过高，如过高，可降低攻击门限。

52.5.2 故障现象：配 置防扫描后没有报警，没有拒包

现象	通过抓包或流收集后，确定已经受到了扫描攻击，而此时设备没有报警，没有拒包。
分析	可能是以下几种情况导致： 1．扫描识别门限设置得太大，导致扫描计数还没有达到门限值。 2．同时配置了防扫描、防SYN Flood和会话管理中的TCP半连接数目限制，三者功能有重叠，可能其它功能已经触发导致防扫描功能未起作用。
解决	检查配置，如果是因为门限值设置得太大，根据实际需求修改到合适的值。

53 第53章 ARP 攻击防护

53.1 ARP攻击防护概述

在局域网中，通信前必须通过 ARP 协议将 IP 地址转换为 MAC 地址。ARP 协议对网络安全具有重要的意义，但是当初 ARP 方式的设计没有考虑到过多的安全问题，留下很多隐患，使得 ARP 攻击成为当前网络环境中遇到的一个非常典型的安全威胁。

通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的 ARP 通信量，使网络阻塞，攻击者只要持续不断的发出伪造的 ARP 响应包就能更改目标主机 ARP 缓存，造成网络中断或中间人攻击。

受到 ARP 攻击后会出现无法正常上网、ARP 包爆增、不正常或错误的 MAC 地址、一个 MAC 地址对应多个 IP、IP 冲突等情况。ARP 攻击因为技术门槛低，易于实现，在现今的网络中频频出现，有效防范 ARP 攻击已成为确保网络畅通的必要条件。

T 系列防火墙的 ARP 攻击防护功能能有效识别 ARP 欺骗攻击和 ARP flood 攻击，对疑似攻击的行为告警，并配合 IP-MAC 绑定、主动保护发包及关闭 ARP 学习等功能有效防范 ARP 攻击造成的损害。

53.2 配置ARP攻击防护

53.2.1 缺省配置信息

ARP 攻击防护功能默认不启用。缺省设置信息如下表所示：

表53-1 ARP 攻击防护功能缺省配置信息

内容	缺省设置	备注
启用/禁止防ARP欺骗	不启用	可更改设置
启用/禁止主动保护	不启用	可更改设置
主动保护时间间隔	1秒	可更改设置
主动保护列表	空	可添加列表
启用/关闭ARP学习	启用	可更改设置
启用/禁止状态ARP flood攻击防御	不启用	可更改设置
ARP攻击识别阈值	300	可更改设置
ARP攻击主机抑制时长	60秒	可更改设置

53.2.2 ARP攻击防护基本配置

ARP 攻击防护配置分为防 ARP 欺骗攻击配置和防 ARP flood 攻击配置。

配置步骤：

1.进入**策略>安全防护>ARP 攻击防护>配置**

参数说明：

防 ARP 欺骗：点选**启用**，对检测到的 ARP 欺骗攻击告警。

主动保护：点选启用主动保护发包功能，每隔一定时间间隔发送一次主动保护列表上的免费 ARP 报文。

时间间隔：发送主动保护列表上的 ARP 的时间间隔，缺省配置为 1 秒。

关闭 ARP 学习：默认启用 ARP 学习，关闭后只要是不匹配 IP-MAC 绑定表的报文都将被丢弃。

防 ARP Flood：点选**启用**防 ARP Flood 攻击。

ARP 攻击识别阈值：一秒内收到 ARP 报文的数量，缺省配置为 300。

攻击主机抑制时长：设置阻断时间，当系统检测到攻击时，在配置的时长内拒绝来自于该台源主机的所有其它包，缺省配置为 60 秒。

2.点击**提交：**完成设置。

注意

关闭了 ARP 学习后，任何报文只要不匹配 IP-MAC 绑定表，都将被丢弃，因此强烈建议在关闭此功能前一定要先绑定需要使用的 IP-MAC。

提示

只有选择启用防 ARP 欺骗后才能配置主动保护和 ARP 学习功能；

只有选择启用主动保护才能配置主动发包时间间隔；

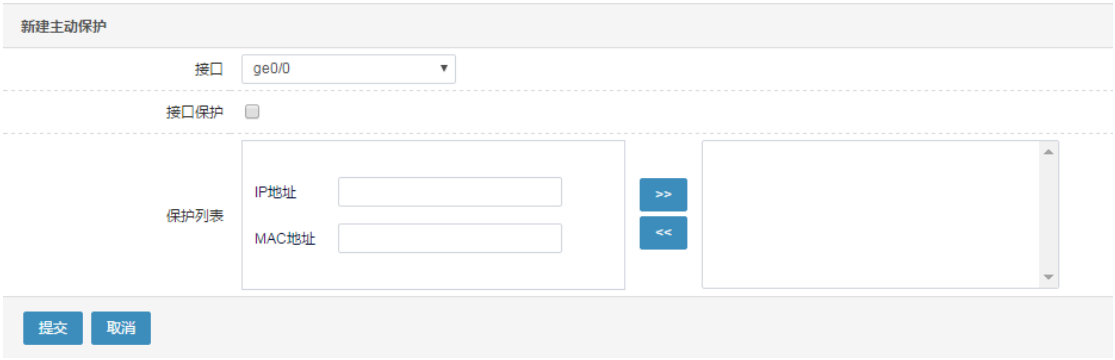
只有选择启用防 ARP flood 攻击后才能配置 ARP 攻击识别阈值和攻击主机抑制时长。

53.2.3 主动保护列表配置

配置主动保护列表，在开启配置中的主动保护后，将自动广播列表中的免费 ARP 报文。

配置步骤：

1.进入**策略>安全防护> ARP 攻击防护>主动保护列表** 点击**新建：**



参数说明：

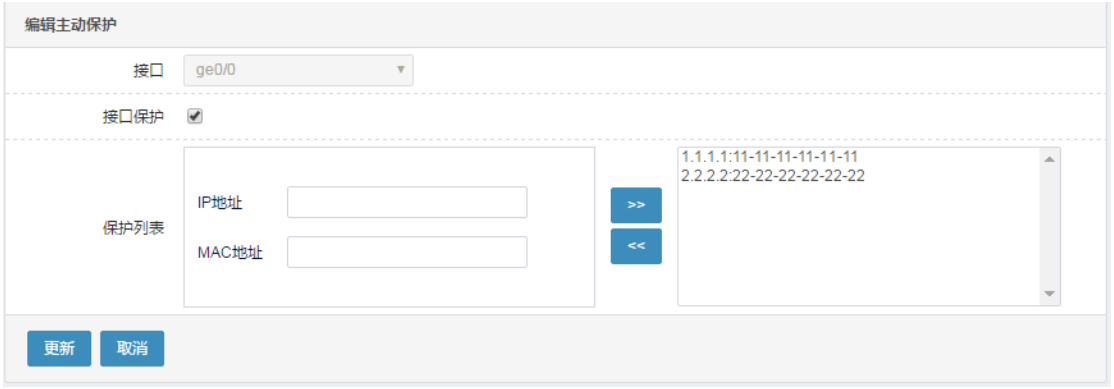
接口：ARP 报文发送接口

接口保护：在保护列表中加入接口地址

IP 地址&MAC 地址：广播 ARP 报文的 IP 和 MAC

2.点击**提交：**完成设置

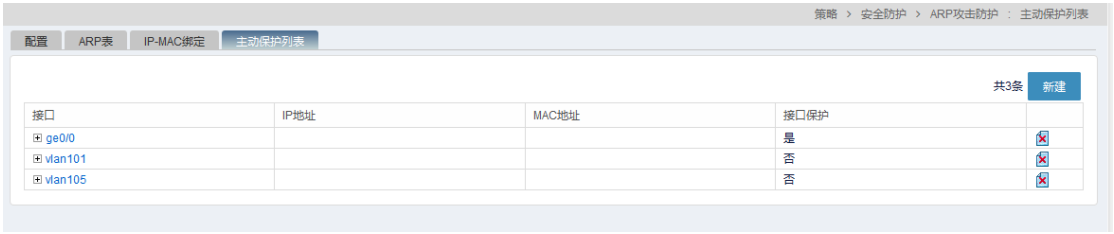
点击接口名称进行编辑



不能对接口进行修改，其他参数和操作同**新建**。

删除主动保护列表

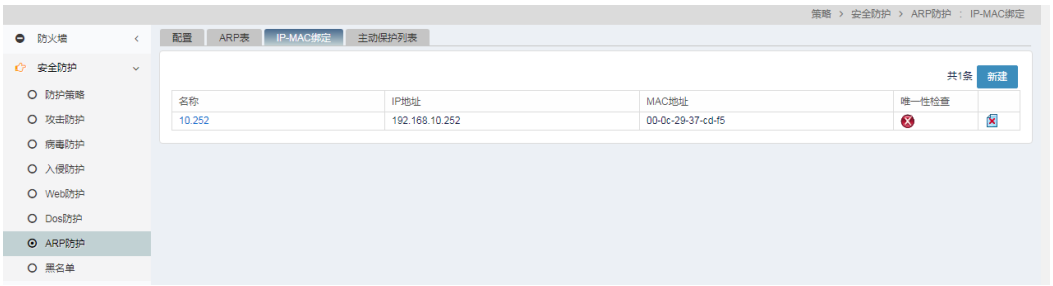
点击  直接删除该接口下的主动保护列表配置。



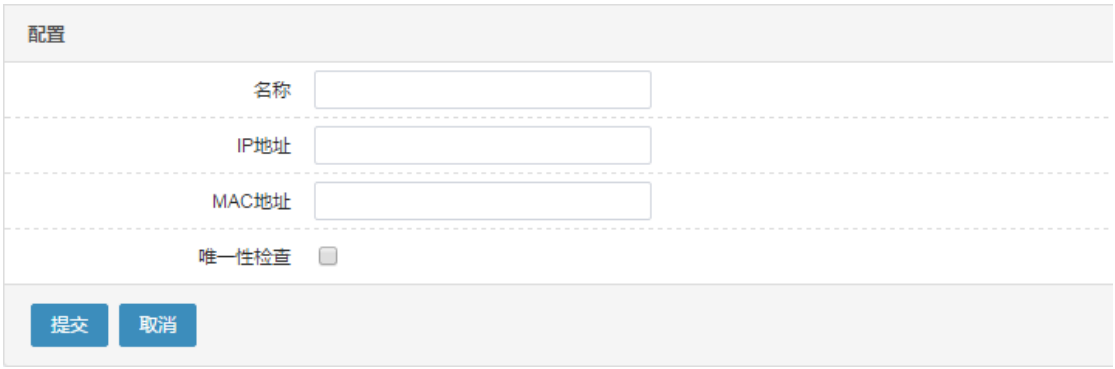
53.2.4 IP-MAC绑定配置

配置步骤：

2. 进入**策略>安全防护>ARP 攻击防护>IP-MAC 绑定**



点击**新建：**



参数说明：

名称：IP-MAC 绑定的名称

IP 地址：IP-MAC 中的 IP 地址

MAC 地址：IP-MAC 中的 MAC 地址

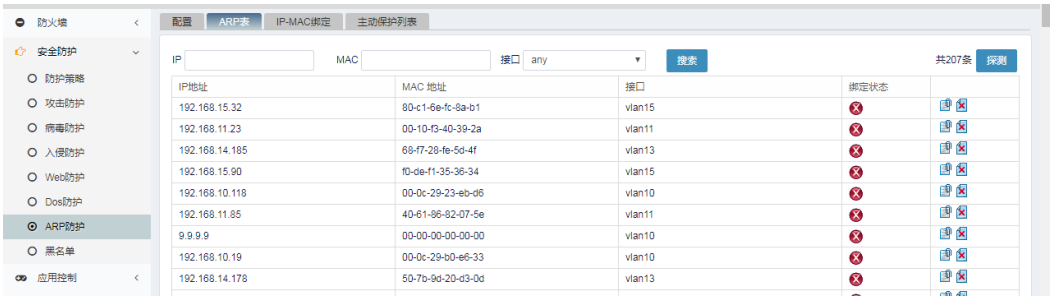
唯一性检查：选定后，一个 MAC 只能与一个 IP 地址绑定

3. 点击**提交：**完成设置

53.2.5 ARP表

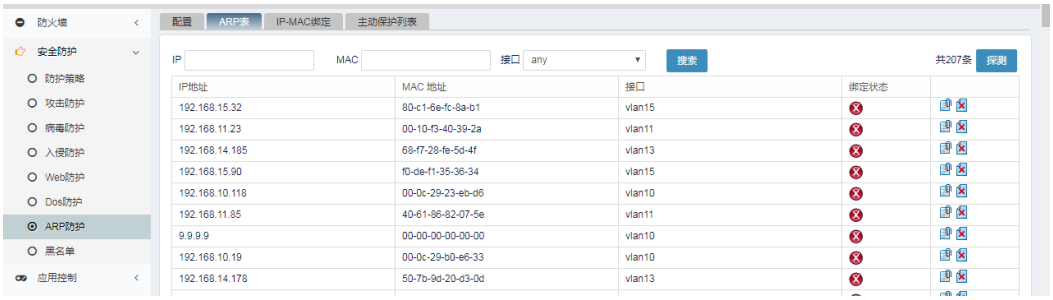
进入**策略>安全防护>ARP 攻击防护>ARP 表**

可以根据 IP、MAC 和接口进行搜索



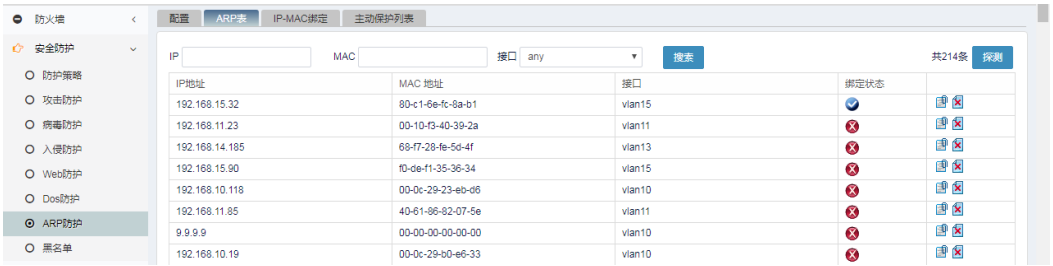
ARP 表中直接进行 IP-MAC 绑定

进入**策略>安全防护>ARP 表**

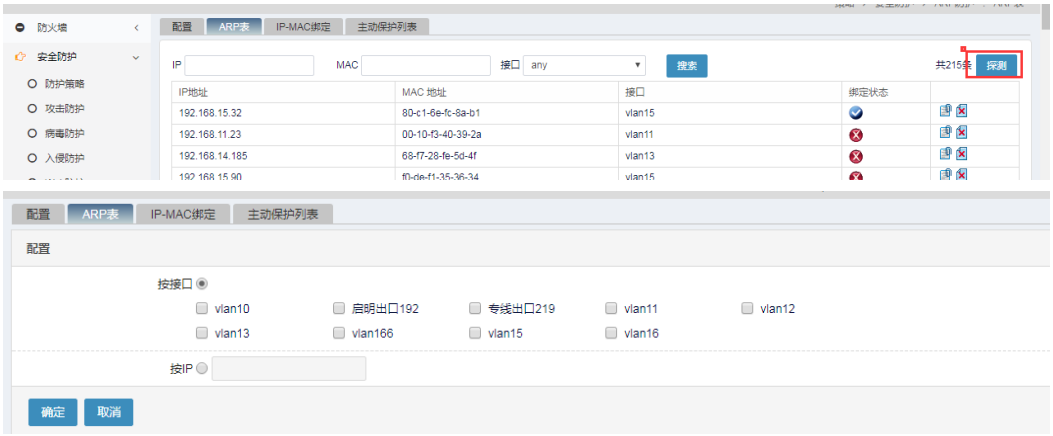


点击  绑定设备已经完成学习的 IP-MAC 地址对。

绑定成功后，ARP 表页面会显示 



ARP 探测：点击右上角的探测按钮，可以根据接口或者 IP 进行探测



选择接口时，会对本接口下的所有设备进行探测

选择 IP 时，只探测相应 IP 地址

53.3 配置案例

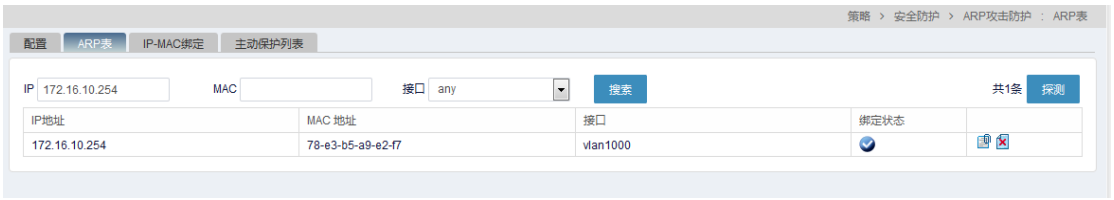
53.3.1 配置案例：配置防ARP欺骗和防 ARP Flood

案例描述：

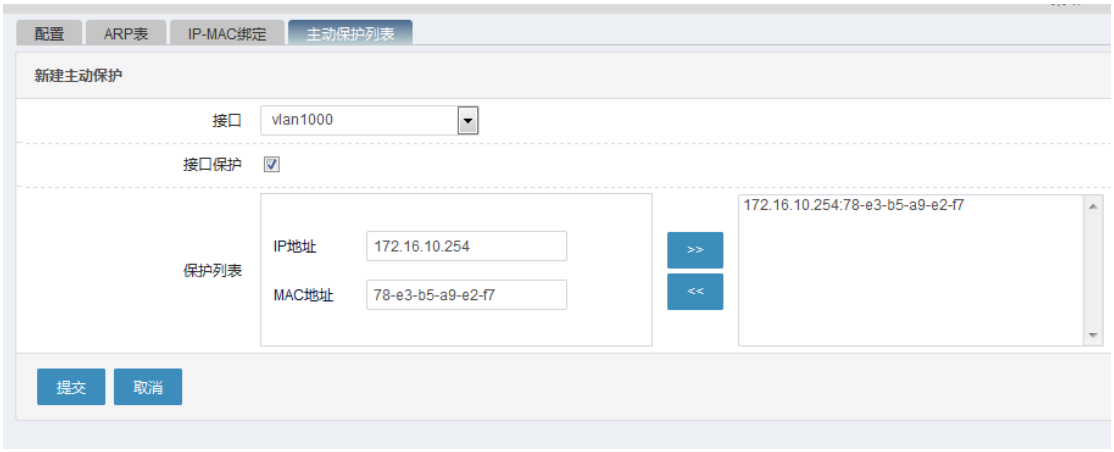
配置防 ARP 欺骗和防 ARP Flood，检测网络中是否有 ARP 攻击

配置步骤：

1. 绑定 IP-MAC，可以在 ARP 表中，绑定设备已经完成学习的 IP-MAC 地址对，其他没有在线的主机可以通过手工添加的方式完成。



2. 配置主动防护列表，对内部关键的主机资源进行保护。通过主动发送这些关键主机的 ARP 信息，达到防止 ARP 欺骗的目的。如增加内部邮件服务器地址：



点击**提交**。

3. 在**配置**页面启动 ARP 防欺骗攻击和主动保护以及防 ARP Flood

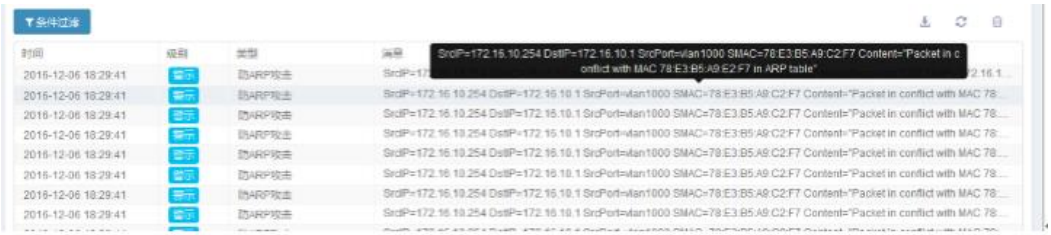
点击提交。

4. **查看日志，是否有 ARP Flood 攻击包**

日志>安全日志>防 ARP 攻击，查看 ARP Flood 日志

5. **查看日志，是否有 ARP 欺骗攻击包**

日志>安全日志 >防 ARP 攻击，查看 ARP 欺骗日志



53.4 常见故障分析

53.4.1 故障现象：PC无法上网

现象	配置防ARP欺骗后无法上网
分析	配置关闭了ARP学习，又没有在IP-MAC绑定表中加入PC
解决	在绑定表中加入PC

54 第54章 IP 黑名单防护

54.1 IP黑名单概述

用户发现有可疑流量时，可在 T 系列防火墙中配置 IP 黑名单进行防护。流经 T 系列防火墙的流量命中 IP 黑名单配置的过滤条件时，在设定时间内可以精确阻断该流量。

IP 黑名单支持 IPv4、IPv6、用户区域及 ISP 四种类型，创建时需要配置阻断方向、加入分组、阻断的类型及地址和设定超时时间，其中用户区域及 ISP 类型超时时间设置为永久。按照阻断方向匹配 IP 黑名单地址的报文在生效时间段内不再进行投递，直接做丢弃处理。

IP 黑名单可由非手动添加的阻断方式创建，支持对会话选择性的进行实时阻断、APT 联动中选择性将风险源 IP 进行隔离、入侵防护阻断、WEB 应用防护阻断、口令防护阻断及资产防护阻断方式添加至黑名单。IP 黑名单支持对黑名单配置的导入和导出，方便对大量的黑名单地址进行配置和备份操作。IP 黑名单首页根据未超时黑名单的命中数从大到小进行 TOP100 展示。

所有 IP 黑名单均被进行分组管理，可通过 IP 黑名单组对其下黑名单进行整组启停和设定超时时间。系统内置名为 default、non_manually_addition_block、abnormal_assets_block 三个默认组，用于分组管理手动添加、非手动阻断生成及资产黑名单。

54.2 配置IP黑名单阻断方向

配置步骤：

2. 进入**策略>安全防护>IP 黑名单**，选择**阻断方向配置**，设置 IP 黑名单的阻断方向，如下图：

源 IP：选择流经报文的源 IP 进行黑名单匹配命中。

源或目的 IP：对流经报文先进行源 IP 的黑名单匹配，若未命中，再进行目的 IP 的黑名单匹配。

54.3 配置IP黑名单组

54.3.1 创建IP黑名单组

配置步骤：

1. 进入**策略>安全防护>IP 黑名单**，选择 **IP 黑名单组**，如下图：

名称：IP 黑名单组名称。

开始时间 ：IP 黑名单组配置创建时的系统时间。

结束时间 ：IP 黑名单组生效周期结束的时间。

剩余生效时间：IP 黑名单组剩余的生效时间。

成员数：IP 黑名单组下 IP 黑名单成员的个数。所有 IP 黑名单组下成员数累计不可超过设备 IP 黑名单规格数。

启用：IP 黑名单组对其下 IP 黑名单成员是否进行阻断流经设备流量的整组控制。

2. 点击**新建**按钮，创建 IP 黑名单组，如下图：

参数说明：

名称：IP 黑名单组名称。

启用：勾选启动或取消停止 IP 黑名单组下 IP 黑名单成员整组匹配流量。

超时 ：设定 IP 黑名单组的超时时间，支持有效时间、绝对周期时间和无时间设定选项。有效时间可按照分钟(0-9999)、天(0-9999)及月(0-600)三种单位配置，默认为 5 分钟，配置成‘0’表示永久生效。绝对时间可配置起始与结束的周期时间，格式为年月日时分秒。选择无时间设定时，IP 黑名单超时时间由自身时间设置，IP 黑名单组有超时时间设置时，除类型为用户区域及 ISP 的 IP 黑名单外，组下其它成员的超时时间均由 IP 黑名单组时间设置。

提示

系统内置名为 default、non_manually_addition_block、abnormal_assets_block 三个默认 IP 黑名单组，默认组不可删除及修改组名称。其中 abnormal_assets_block 组用于放置管理资产黑名单，该组配置的超时时间设置为永久不可修改。

不同 IP 黑名单组下，可以拥有相同地址的 IP 黑名单成员。

54.3.2 删除IP黑名单组

配置步骤：

1. 进入**策略>安全防护>IP 黑名单**，选择 **IP 黑名单组**，如下图：

2. 除默认组外，可点击 ✖ 对应删除某条 IP 黑名单组及其组下的所有 IP 黑名单。

54.3.3 修改IP黑名单组

配置步骤：

1. 进入**策略>安全防护>IP 黑名单**，选择 **IP 黑名单组**，点击组名称。

2. 可对 IP 黑名单组里面的可内容进行修改，修改完毕后点击**提交**。

注意

编辑修改 IP 黑名单组时，名称不能改变。

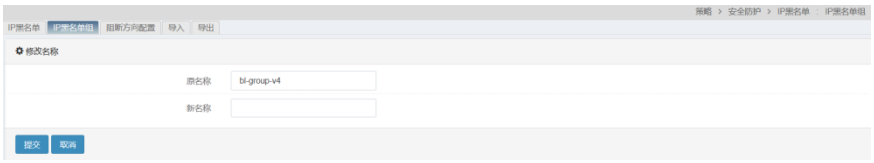
如果进入默认组 abnormal_assets_block 编辑页面，则可修改项只有启用勾选框，改默认组时间固定为永久。

54.3.4 修改IP黑名单组名称

配置步骤：

3. 进入**策略>安全防护>IP 黑名单**，选择 **IP 黑名单组**，如下图：

2. 点击 修改某个 IP 黑名单组名称。



注意

新名称不能使用系统默认组名、系统已存在组名称。

54.3.5 启停IP黑名单组

配置步骤：

1. 进入**策略>安全防护>IP 黑名单**，选择 **IP 黑名单组**，如下图：

2. 点击 勾选框快捷操作 IP 黑名单组下黑名单成员是否进行对流经设

备流量的匹配阻断。

54.3.6 查询IP黑名单组

1. 进入**策略>安全防护>IP 黑名单**，选择 **IP 黑名单组**，如下图：

2. 输入名称，点击  进行查找包含其输入内容的 IP 黑名单组。

54.4 配置IP黑名单

54.4.1 创建IP黑名单

4. 进入**策略>安全防护>IP 黑名单**，选择 **IP 黑名单**，如下图：

地址：IP 黑名单所阻断的 IP 地址或用户区域、ISP 名称所包含的 IP 地址。

开始时间 ：IP 黑名单或所属组配置创建时的系统时间。

结束时间 ：IP 黑名单或所属组生效周期结束的时间。

剩余生效时间：IP 黑名单或所属组剩余的生效时间。

添加方式：黑名单的添加方式。从 IP 黑名单配置页添加时添加方式是手工添加，从会话统计页面通过阻断按钮添加时添加方式是实时阻断，入侵防护方式添加 IP 黑名单的添加方式是入侵防护阻断，apt 联动添加 IP 黑名单的添加方式是隔离，waf 方式添加 IP 黑名单的添加方式是 web 应用防护阻断，口令防护方式添加时添加方式是口令防护阻断，资产黑名单的添加方式显示为资产防护阻断。

所在组：IP 黑名单所属组的名称。

命中：流经设备流量匹配到 IP 黑名单地址的命中数。

注意

防火墙设备目前 IP 黑名单规格根据设备内存不同初始化为 5 万-100 万条(包括 ipv4、ipv6、用户区域及 ISP 类型 IP 黑名单总和):

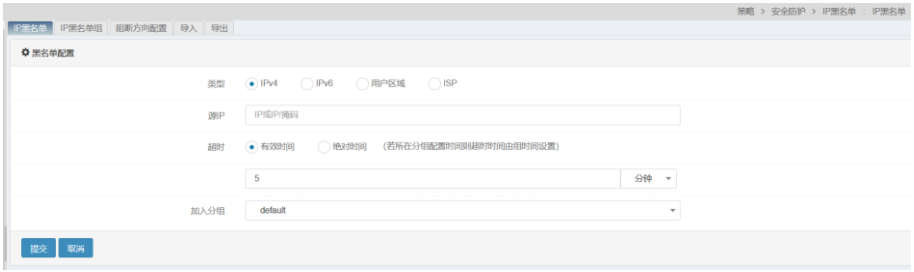
2GB 内存 IP 黑名单规格 5 万条;

4GB 内存 IP 黑名单规格 20 万条;

8GB/16GB 内存 IP 黑名单规格 50 万条;

32GB 内存 IP 黑名单规格 100 万条;

5. 点击**新建**按钮创建 IP 黑名单，如下图:



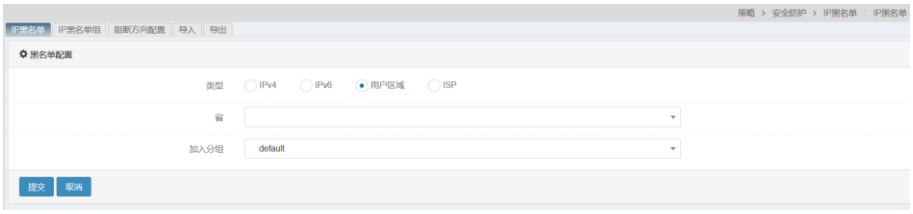
参数说明:

类型: IP 黑名单有 IPv4、IPv6、用户区域和 ISP 四种类型，选择其一。

源 IP: 期望 IP 黑名单所阻断的 ipv4 或者 ipv6 地址。

超时 : 设定 IP 黑名单的超时时间，支持有效时间和绝对时间设定选项。有效时间可按照分钟(0-9999)、天(0-9999)及月(0-600)三种单位配置，默认为 5 分钟，配置成‘0’表示永久生效。绝对时间可配置起始与结束的周期时间，格式为 YYYY-MM-DD hh:mm:ss。用户区域、ISP 类型的 IP 黑名单超时时间固定为永久。

加入分组: IP 黑名单所属的 IP 黑名单组。可选除 abnormal_assets_block 组之外的系统当前存在的所有组。

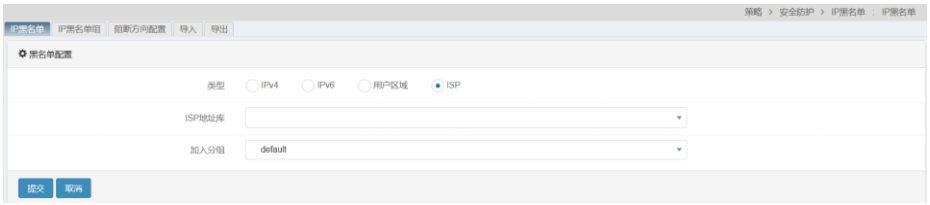


参数说明:

类型: 用户区域类型。

省: 以 34 个区域名称区分不同的 IP 地址归属，为 IPv4 类型。

加入分组: IP 黑名单所属的 IP 黑名单组，可选除 abnormal_assets_block 组之外的系统当前存在的所有组。



参数说明：

类型：ISP 类型。

ISP 地址库：以名称表示的 ISP 地址库，为 IPv4 类型。

加入分组：IP 黑名单所属的 IP 黑名单组，可选除 abnormal_assets_block 组之外的系统当前存在的所有组。

配置完毕后，点击**提交**。

黑名单配置阻断的 IP 时要与黑名单的类型对应上。

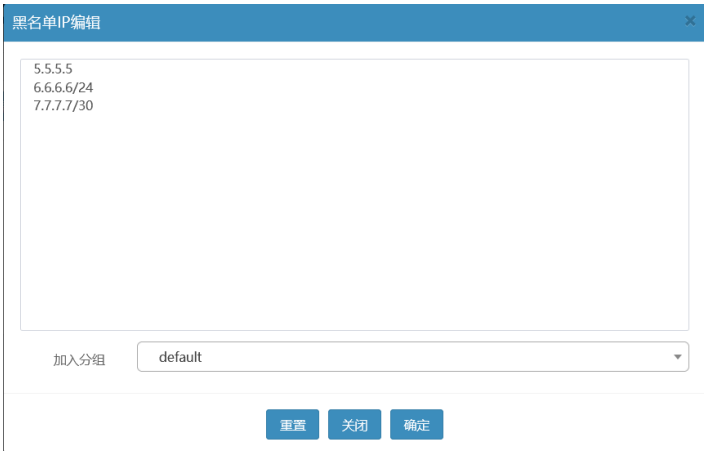
黑名单阻断的 IP 地址不能配置成广播地址和全 0 地址。

黑名单 IPv4 类型配置子网地址时支持掩码为 1~32，IPv6 类型仅支持 64、80、96、112、128 位掩码配置。

54.4.2 编辑创建IP黑名单

配置步骤：

1. 进入**策略>安全防护>IP 黑名单**，点击**编辑**批量创建 IP 黑名单，如下图：



参数说明：

编辑窗口：输入 IPv4 或 IPv4/掩码，支持批量粘贴操作。

加入分组：IP 黑名单所属的 IP 黑名单组，可选除 abnormal_assets_block 组之外的系统当前存在的所有组。

重置：清空编辑窗口已有内容。

关闭 ：取消 IP 黑名单编辑创建操作。

2. 编辑完毕后，点击**确定**，IP 黑名单创建并提示成功编辑添加的条数，如下图：

3. 点击**关闭**，完成 IP 黑名单编辑创建。

提示

通过编辑创建的 IP 黑名单生效时间由所选加入分组时间决定，如果所属组无时间配置，批量创建 IP 黑名单时间为永久。

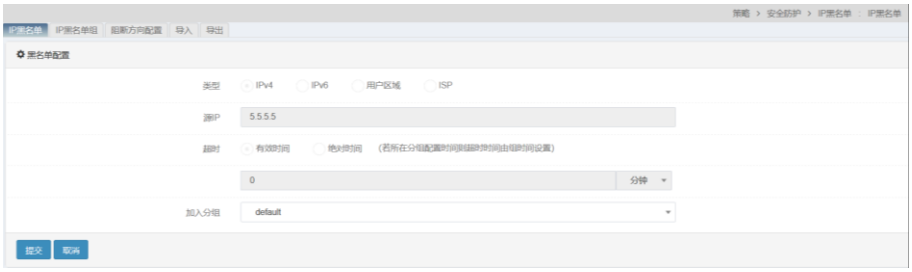
编辑窗口的 IP 黑名单规格为 2048 条。

54.4.3 修改IP黑名单

配置步骤：

1. 进入**策略>安全防护>IP 黑名单**，对于某条 IP 黑名单，点击 IP 黑名单前面的序号进入修改界面。

2. 对 IP 黑名单里面的可内容进行修改，修改完毕后点击**提交**。



注意

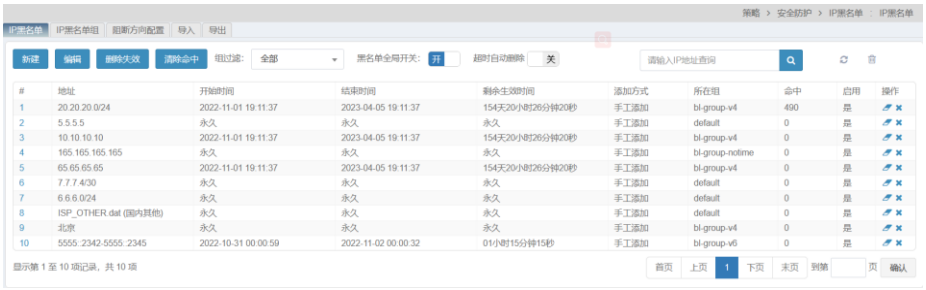
编辑修改 IP 黑名单时，类型和 IP 不能改变。

编辑修改的 IP 黑名单最初所属组如果无时间设置，黑名单成员可直接修改超时时间配置；如果所属组有时间设置，需要重新选择分组后才可配置超时时间，编辑修改后的 IP 黑名单最终时间，由所属组是否配置时间决定。

54.4.4 删除IP黑名单

配置步骤：

4. 进入**策略>安全防护>IP 黑名单**，选择 **IP 黑名单**，如下图：

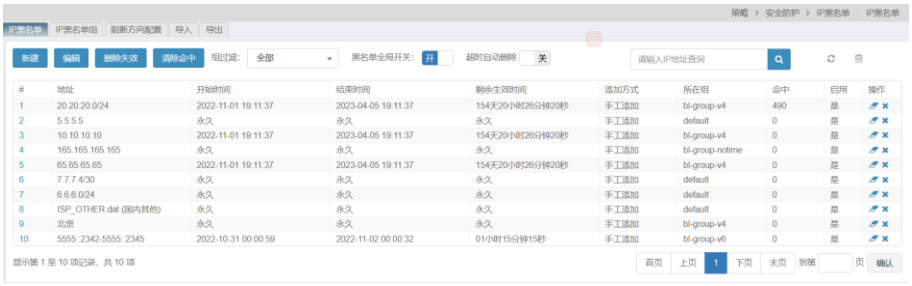


5. 点击 删除某条 IP 黑名单配置或者点击 删除全部 IP 黑名单配置。

54.4.5 删除失效IP黑名单

配置步骤：

1. 进入**策略>安全防护>IP 黑名单**，选择 **IP 黑名单**，如下图：

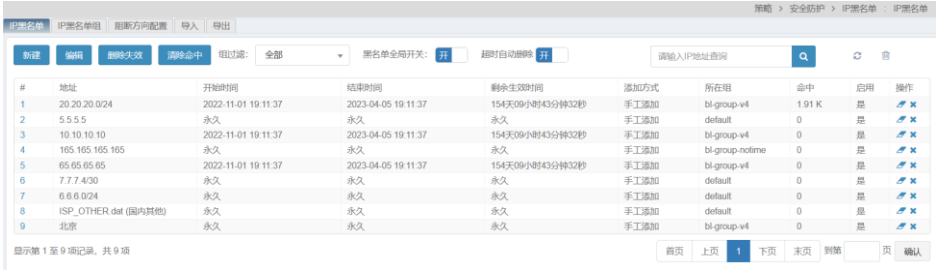


2. 点击 删除失效 删除全部剩余生效时间显示为 0 的 IP 黑名单配置。

54.4.6 超时自动删除IP黑名单

配置步骤：

1. 进入**策略>安全防护>IP 黑名单**，选择 **IP 黑名单**，如下图：



2. 开启 超时自动删除 开 开关后，检查 IP 黑名单表项是否超时的定时器，会

将超时的表项自动删除。

54.4.7 重置IP黑名单命中数

配置步骤：

1. 进入**策略>安全防护>IP 黑名单**，选择 **IP 黑名单**，如下图：

2. 点击 重置某条 IP 黑名单已有命中数，点击 清除命中 重置全部 IP 黑名单命中数。

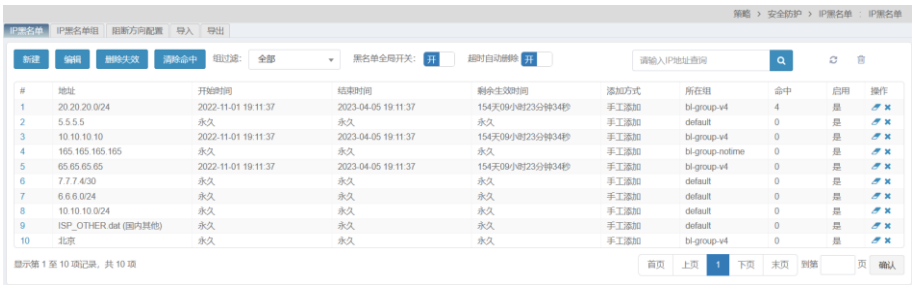
注意

设备重启后 IP 黑名单命中数均重置。

IP 黑名单超时后，已有命中数统计值保留。

54.4.8 查询IP黑名单

1. 进入**策略>安全防护>IP 黑名单**，选择 **IP 黑名单**，如下图：

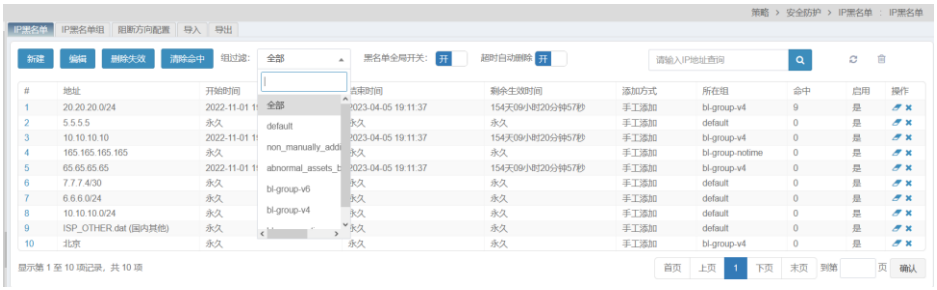


2. 在查询栏输入需要查找的黑名单 IP 地址，点击 进行查找，如下图：

54.4.9 组过滤显示IP黑名单

配置步骤：

1. 进入**策略>安全防护>IP 黑名单**，选择 **IP 黑名单**，如下图：

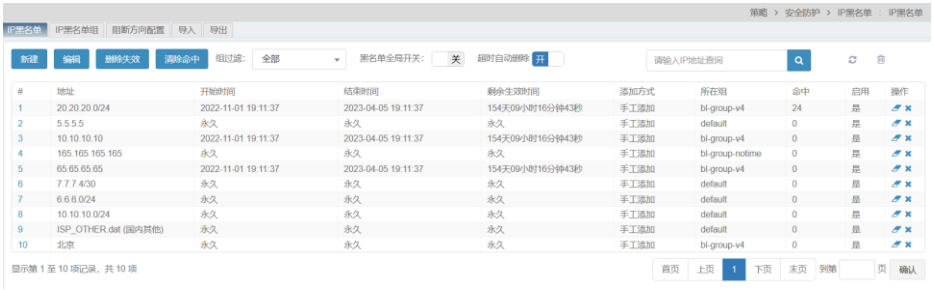


2. 点击 组过滤: 全部 下拉框显示 IP 黑名单组名，根据所选择组展示组下黑名单成员，如下图：

54.4.10 全局开关IP黑名单

配置步骤：

1. 进入**策略>安全防护>IP 黑名单**，选择 **IP 黑名单**，如下图：



2. 关闭 黑名单全局开关: 关 开关后，IP 黑名单下全部黑名单，不再对流经设备流量进行匹配阻断防护。

54.5 IP黑名单配置导入导出

54.5.1 IP黑名单导入

配置步骤：

1. 进入**策略>安全防护>IP 黑名单**，选择**导入**，如下图：

参数说明：

时间：可为导入文件统一设定时间。

所属组：导入文件中 IP 黑名单成员所属组的名称。

上传文件：可导入包含 IP 黑名单配置的文本文件，系统会读取文件中的配置并执行下发。

注意

最终导入文件中除用户区域及 ISP 类型成员，IP 黑名单成员时间设定优先级为：所属组时间>导入设置时间>导入文件中成员自己配置时间。

IP 黑名单导入配置必须如下：

- **IPv4 类型**

1. 有效时间配置：

blacklist-ip (x.x.x.x|x.x.x.x/x|x.x.x.0-x.x.x.255) valid_time_type (min|day|month) timeout x configtime x-x-x x:x:x

x.x.x.x|x.x.x.x/x|x.x.x.0-x.x.x.255 ： IPv4 或 IPv4/掩码类型地址或 IP 范围，掩码可取(1~32)；

x：生效时间（min:0~9999;day:0~9999;month:0~600）；

x-x-x x:x:x ：配置起始的年-月-日 时：分：秒。

2. 绝对时间配置：

blacklist-ip (x.x.x.x|x.x.x.x/x|x.x.x.0-x.x.x.255) starttime x-x-x x:x:x endtime x-x-x x:x:x

x.x.x.x|x.x.x.x/x|x.x.x.0-x.x.x.255 ： IPv4 或 IPv4/掩码类型地址或 IP 范围，掩码可取(1~32)；

x-x-x x:x:x ：配置开始及截至的年-月-日 时：分：秒。

- **纯 IPv4**

x.x.x.x

x.x.x.x/x

纯 IPv4 或 IPv4/掩码类型地址，掩码可取值(1~32)；

- **IPv6 类型**

1. 有效时间配置：

blacklist-ipv6 (x:x::x:x|x:x::x:x/x) valid_time_type (min|day|month) timeout x configtime x-x-x x:x:x

x:x::x:x|x:x::x:x/x ：IPv6 或 IPv6/掩码类型地址，掩码可取(128|112|96|80|64)；

x：生效时间（min:0~9999;day:0~9999;month:0~600）；

x-x-x x:x:x ：配置生效时的年-月-日 时：分：秒。

2. 绝对时间配置：

blacklist-ipv6 (x:x::x:x|x:x::x:x/x) starttime x-x-x x:x:x endtime x-x-x x:x:x

x:x::x:x|x:x::x:x/x ：IPv6 或 IPv6/掩码类型地址，掩码可取(128|112|96|80|64)；

x-x-x x:x:x ：配置生效时的年-月-日 时：分：秒。

- **用户区域类型**

blacklist-region province NAME valid_time_type (min) timeout 0 configtime x-x-x x:x:x

NAME：区域名称，34个区域名称之一；

x-x-x x:x:x ：配置生效时的年-月-日 时：分：秒。

- **ISP 类型**

blacklist-isp NAME valid_time_type (min) timeout 0 configtime x-x-x x:x:x

NAME：ISP地址库名称；

x-x-x x:x:x ：配置生效时的年-月-日 时：分：秒。

注意

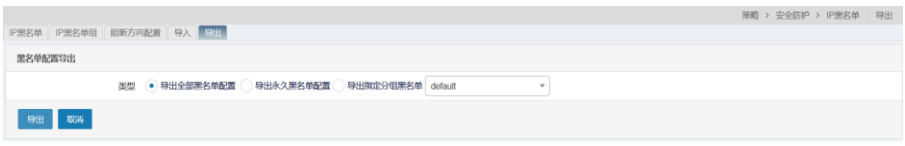
导入文件如果有用户区域类型，导入文档需使用 GB2312 编码。

导入 IP 黑名单的添加方式均为手工添加。

54.5.2 IP黑名单导出

配置步骤：

1. 进入**策略>安全防护>IP 黑名单**，选择**导出**，如下图：



参数说明：

类型：支持三种 IP 黑名单导出方式：导出全部黑名单配置、导出永久黑名单配置和导出指定分组黑名单。

2. 选择类型点击**导出**按钮，设备根据导出类型及导出时间生成已命名的文档后，可操作页面弹窗保存至本地路径。

注意

导出文件如果有用户区域 IP 黑名单类型，导出文档需用 GB2312 编码显示。

IP 黑名单导出前需先对当前配置进行保存。

54.6 配置案例

54.6.1 案例1：创建IP黑名单

配置步骤：

1. 进入**策略>安全防护>IP 黑名单**，选择 **IP 黑名单**，点击**新建**按钮进入配置页面，配置源 IP 为 20.0.0.3 的 IP 黑名单，配置时间及选择加入分组如下图：

2. 点击**提交**，完成配置。

54.6.2 案例2：创建实时阻断IP黑名单

配置步骤：

1. 进入**监控>会话>会话统计**，设置条件后点击**搜索**，搜索当前会话，如下图：

2. 点击需要临时阻断的某条会话最后面的 标记，跳转到 IP 黑名单配置页面，实时阻断添加方式默认加入 non_manually_addition_block 分

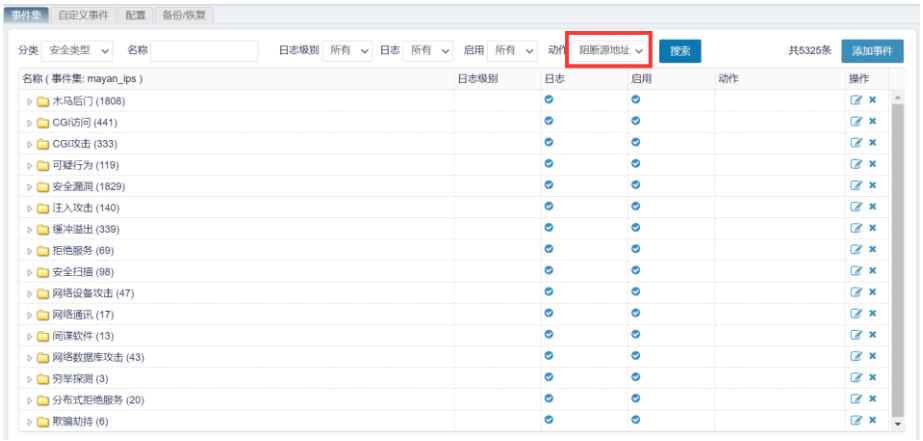
组，如下图：

3. 设置需要临时阻断的生效时间，点击**提交**，完成配置，进入**策略>安全防护>IP 黑名单**页面进行查看，如下图：

54.6.3 案例3：创建入侵防护阻断IP黑名单

配置步骤：

1. 进入**策略>安全防护>入侵防护**，将 ALL 事件集的动作改为阻断源 IP。如下图：



2. 配置防护策略，引用 ALL 入侵防护，配置如下：

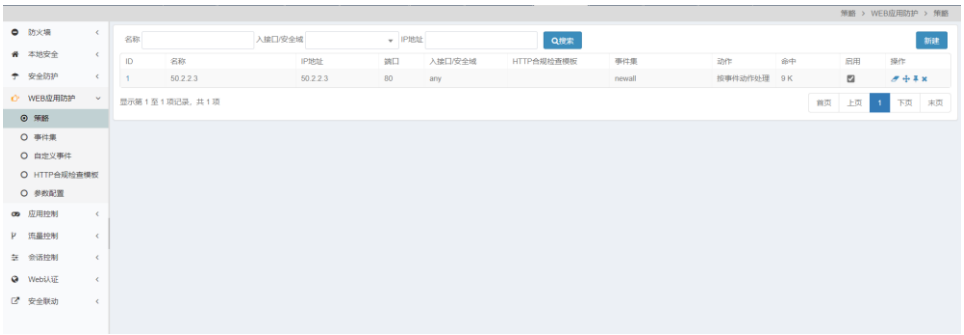
3. 有流量匹配到防护策略中入侵防护模块，源 IP 自动加入的 IP 黑名单中，如下图：

54.6.4 案例4：创建WEB应用防护阻断IP黑名单

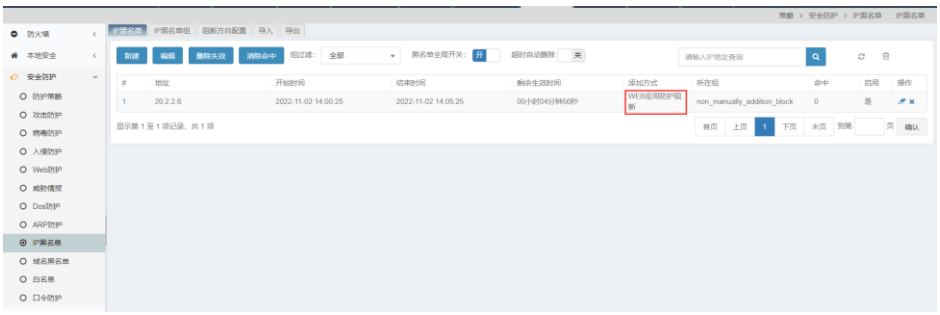
配置步骤：

1. 进入**策略>WEB 应用防护>自定义事件**，新建阻断源 IP 的自定义事件，如下图：

2. 将自定义事件加入到新建事件集 newall 中，然后策略引用事件集 newall，配置如下图：



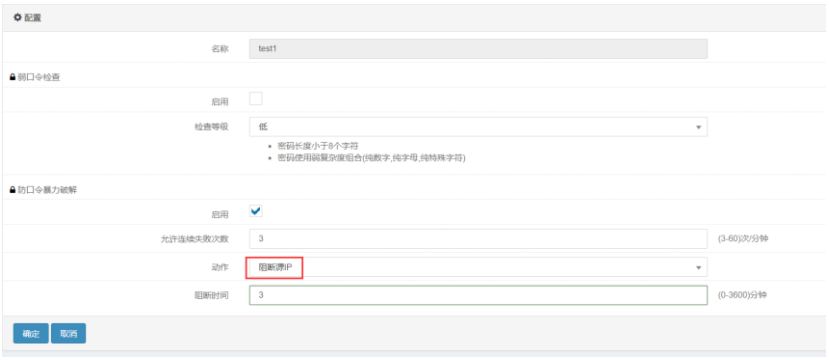
3. 匹配应用防护策略流量的源 IP 自动加入到 IP 黑名单中，如下图：



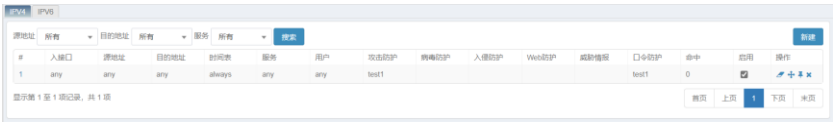
54.6.5 案例5：创建口令防护IP黑名单

配置步骤：

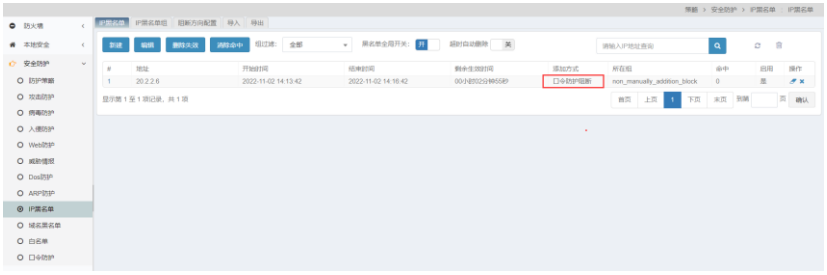
1. 配置口令防护模版 test1。防口令暴力破解部分中 动作：阻断源 IP



2. 配置防护策略，引用口令防护模版 test1，配置如下：



3. 有流量匹配到防护策略中口令防护模块，源 IP 自动加入的 IP 黑名单中，如下图：



55 第55章 域名黑名单防护

55.1 域名黑名单概述

用户发现有对可疑站点的请求流量时，可在防火墙中配置域名黑名单来进行防护。流经防火墙的 DNS 请求报文命中域名黑名单配置的过滤条件时，在设定时间表内可以精确阻断该 DNS 请求。

域名黑名单支持两种类型的域名格式，一种是带点的域名格式（如：qq.com、www.baidu.com），另一种是不带点的格式（如：google、github），所配置的域名长度不应超过 255，且对大小写不敏感。

域名黑名单支持导入、导出以及编辑创建，方便对大量的域名地址进行配置和备份操作。

域名黑名单首页会根据未超时域名黑名单的命中数从大到小进行展示。

55.2 配置域名黑名单

55.2.1 配置域名黑名单

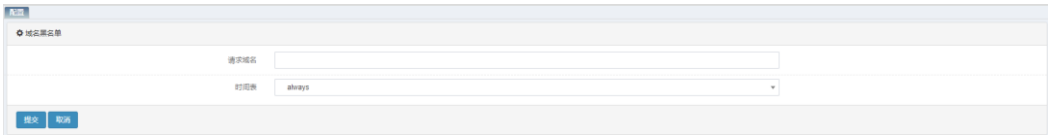
1. 进入**策略>安全防护>域名黑名单**，如下图：

请求域名：域名黑名单所阻断的请求域名。

时间表：域名黑名单生效的时间。

命中：匹配域名黑名单的命中数。

2. 点击**新建按钮**创建域名黑名单，如下图：



参数说明：

请求域名：域名黑名单所阻断的请求域名。

时间表：域名黑名单生效的时间。

3. 配置完毕后，点击**提交**。

提示

配置域名黑名单的时间表时需要引用时间对象，默认为always，表示所有时间。

55.2.2 编辑创建域名黑名单

配置步骤：

1. 进入**策略>安全防护>域名黑名单**，点**编辑**批量创建域名黑名单，如下图：

参数说明：

编辑窗口：输入域名地址，支持批量粘贴操作。

重置：清空编辑窗口已有内容。

关闭 ：取消域名黑名单编辑创建操作。

2. 编辑完毕后，点击**确定，**域名黑名单创建并提示成功编辑添加的条数，如下图：

3. **点击关闭，**完成域名黑名单编辑创建。

提示

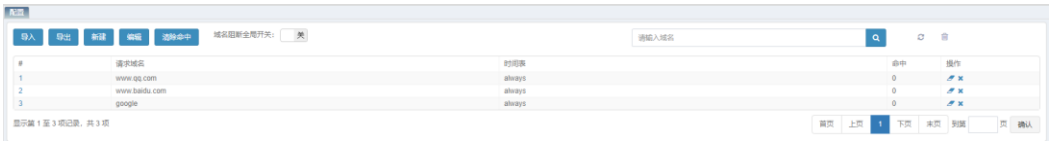
通过编辑创建的域名黑名单时间表均为 always。

编辑窗口的域名黑名单规格为 2048 条。

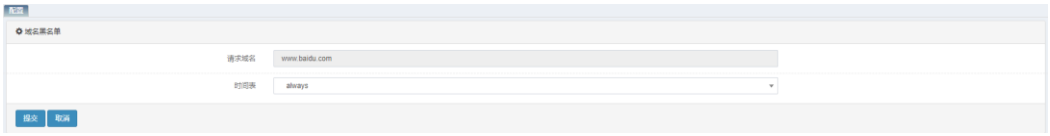
55.2.3 修改域名黑名单

配置步骤：

1. 进入**策略>安全防护>域名黑名单**，对于某条域名黑名单，点击域名黑名单前面的序号进入修改界面。



2. 可以对域名黑名单里面的内容进行修改，修改完毕后点击**提交**。

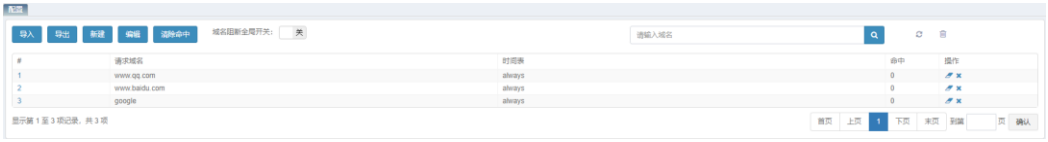


注意 编辑修改域名黑名单时，请求域名不能改变。

55.2.4 删除黑名单

配置步骤：

1. 进入**策略>安全防护>域名黑名单**，如下图：

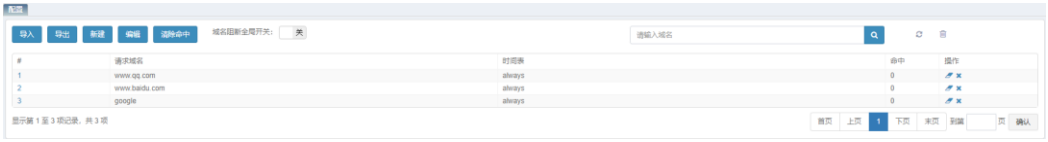


2. 点击 删除某条域名黑名单配置或者点击 删除全部域名黑名单配置。

55.2.5 重置域名黑名单命中数

配置步骤：

1. 进入**策略>安全防护>域名黑名单**，如下图：



2. 点击 重置某条域名黑名单已有命中数或者点击**清除命中**重置全部域名黑名单命中数。

注意

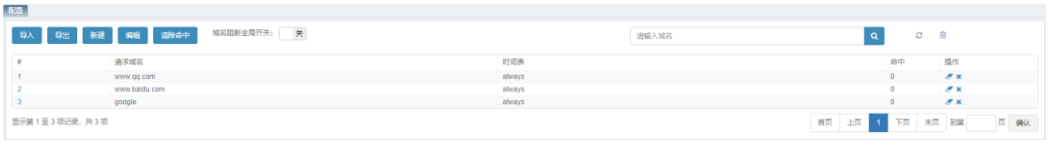
设备重启后域名黑名单命中数均重置。

域名黑名单超时后，已有命中数统计值保留。

55.2.6 刷新域名黑名单

配置步骤：

1. 进入**策略>安全防护>域名黑名单**，如下图：



3. 点击 按钮刷新域名黑名单页面。

55.3 查询域名黑名单配置

进入**策略>安全防护>域名黑名单**，如下图：

输入需要查找的域名地址，点击 进行搜索。

注意

搜索到的结果是此时此刻能够阻断该域名的黑名单列表。

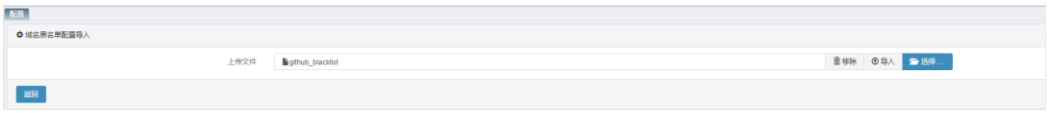
55.4 域名黑名单配置导入导出

进入**策略>安全防护>域名黑名单**，如下图：

55.4.1 域名黑名单导入

导入：可导入包含域名黑名单配置的文本文件，系统会读取文件中的配置并执行下发。

点击**选择**，选择需要导入的域名黑名单配置文件，如下图：



注意

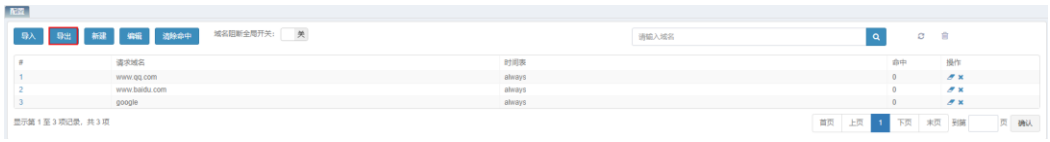
导入的域名黑名单时间表均为 always。

导入的域名黑名单若超过规格，则剩余部分不再被导入。

55.4.2 域名黑名单导出

导出：可将域名黑名单的配置导出至一个文本文件中。

点击**导出**，如下图：



注意

导出的文件中只有域名信息，没有时间表信息。

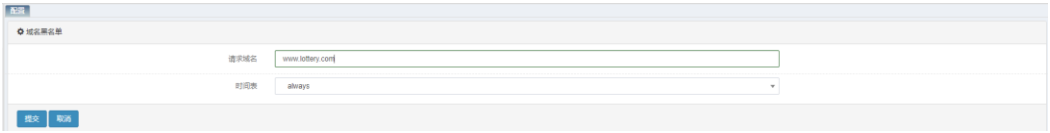
55.5 配置案例

55.5.1 案例1：禁止员工访问博彩站点

案例描述：某博彩站点（www.lottery.com）可能会有挂马行为，为了公司内部网络安全，可以通过配置域名黑名单来阻断对该站点的访问。

配置步骤：

1. 进入**策略>安全防护>域名黑名单**，点击**新建**按钮进入配置页面，配置请求域名为 www.lottery.com、时间表为 always 的黑名单，如下图：



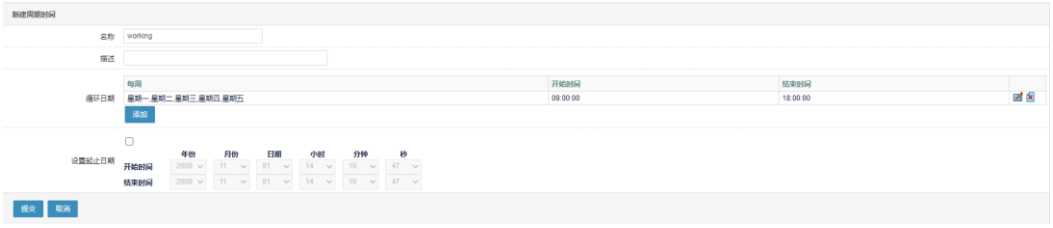
2. 点击**提交**，完成配置。

55.5.2 案例2：禁止员工在上班期间访问游戏站点

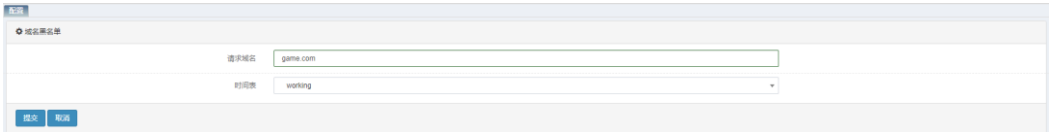
案例描述：公司上班时间为早九晚六，在这期间不希望员工访问 game.com 站点来玩游戏，可以通过配置域名黑名单来阻断对该站点的访问。

配置步骤：

1. 进入**对象>时间对象>周期时间**，点击**新建**按钮进入配置页面，配置循环时间每周为星期一、星期二、星期三、星期四、星期五，开始时间为 09:00:00，结束时间为 18:00:00，如下图：



2. 进入**策略>安全防护>域名黑名单**，点击**新建**按钮进入配置页面，配置域名为 game.com、时间表为 working 的黑名单，如下图：

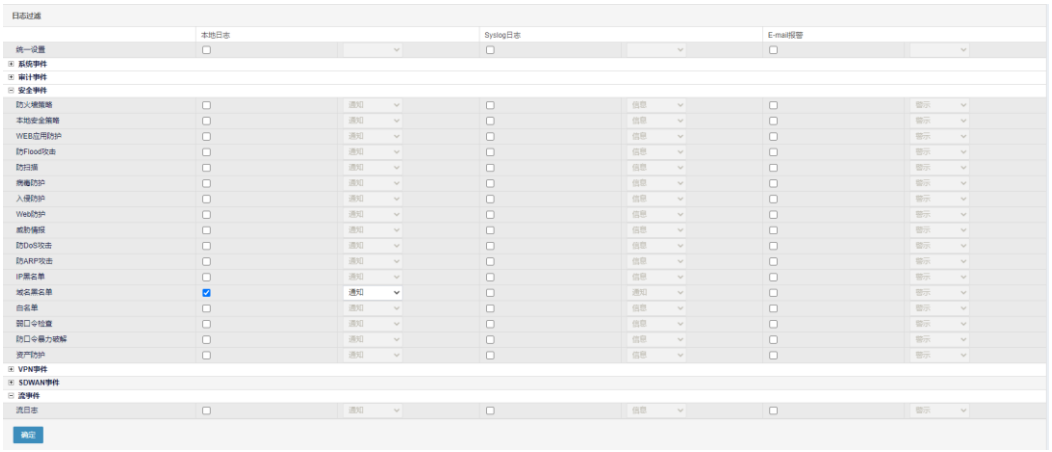


3. 点击**提交**，完成配置。

55.6 域名黑名单防护监控与维护

55.6.1 查看域名黑名单防护日志

1. 进入**日志>日志管理>日志过滤**，勾选域名黑名单的相关日志，并设置日志的级别，点击**确定**。



2. 进入**日志>安全日志>域名黑名单**里查看域名黑名单防护安全日志。

56 第56章 白名单防护

56.1 白名单概述

开启白名单功能后，流经 T 系列防火墙的流量在匹配到白名单配置的过滤条件后，在设定时间内会将该流量绕过防火墙策略、IP 黑名单等安全策略检查，做放行处理。

白名单仅对 IP 地址进行匹配，匹配方向可为源 IP、源或目的 IP。白名单支持 IPv4、IPv6、用户区域及 ISP 类型的地址配置。在 web 页面中，支持对白名单进行手动添加、编辑添加等添加方式。导入和导出功能，方便对大量的白名单地址进行配置和备份操作。白名单首页根据未超时白名单的命中数从大到小进行 TOP100 展示。

56.2 配置白名单匹配方向

进入**策略>安全防护>白名单**，选择**匹配方向配置**，设置白名单的放行方向，如下图：

源 IP：选择流经报文的源 IP 进行白名单匹配命中。

源或目的 IP：对流经报文先进行源 IP 的白名单匹配，若未命中，再进行目的 IP 的白名单匹配。

56.3 配置白名单

56.3.1 配置白名单

1. 进入**策略>安全防护>白名单**，选择**配置**，如下图：

地址：白名单所放行的 IP 地址或用户区域、ISP 名称所包含的 IP 地址。

配置添加时间 ：白名单配置创建时的系统时间。

生效时间：白名单生效的时间，单位为分钟。

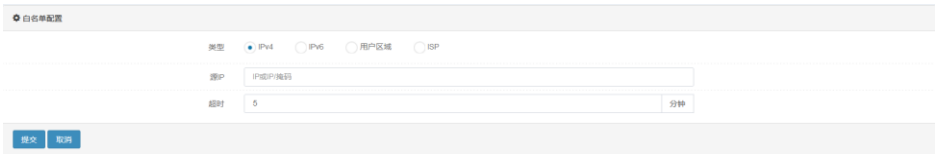
剩余放行时长：白名单剩余的生效时间，单位为秒。

添加方式：白名单的添加方式。

命中：流经设备流量匹配到白名单地址的命中计数

配置步骤：

2. 点击**新建**按钮创建白名单，如下图：

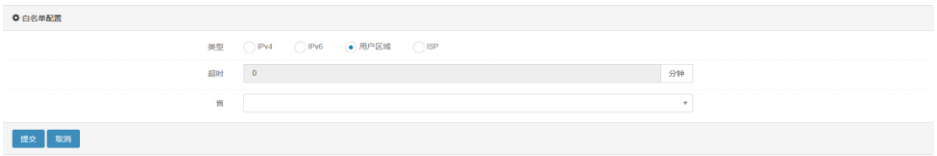


参数说明：

类型：白名单有 IPv4、IPv6、用户区域和 ISP 四种类型，新建的时候任选其一。

源 IP：白名单所放行的 ipv4 或者 ipv6 地址。

超时：配置白名单超时时间，允许配置范围为 0-9999，单位为分钟。默认为 5 分钟，配置成‘0’表示永久生效。

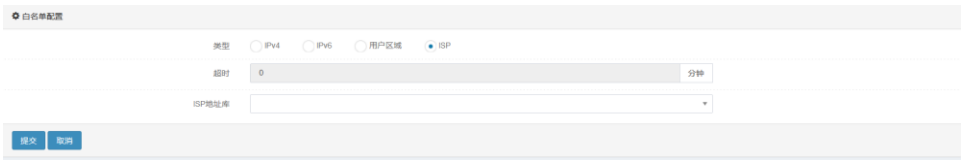


参数说明：

类型：用户区域类型。

超时：用户区域类型白名单超时时间设定为永久生效。

省：以 34 个中国省级行政区域名称区分不同的 IP 归属。



参数说明：

类型：ISP 类型。

超时：ISP 类型白名单超时时间设定为永久生效。

ISP 地址库：以 ISP 地址库名称区分不同的 IP 归属。

3. 配置完毕后，点击**提交**。

提示

白名单规格为 10000 条。

配置白名单放行的 IP 时要与白名单的类型对应上。

白名单放行的 IP 地址不能配置成广播地址和全 0 地址。

白名单 Pv4 类型配置子网地址时支持掩码为 1~32，IPv6 类型仅支持 64、80、96、112、128 位掩码配置。

56.3.2 编辑创建白名单

配置步骤：

1. 进入**策略>安全防护>白名单**，点击**编辑**批量创建白名单，如下图：

参数说明：

编辑窗口：输入 IPv4 或 IPv4/掩码，支持批量粘贴操作。

重置：清空编辑窗口已有内容。

关闭 ：取消白名单编辑创建操作。

2. 编辑完毕后，点击**确定，**白名单创建并提示成功编辑添加的条数，如下图：

3. 点击**关闭，**完成白名单编辑创建。

提示

通过编辑创建的白名单生效时间均为永久。

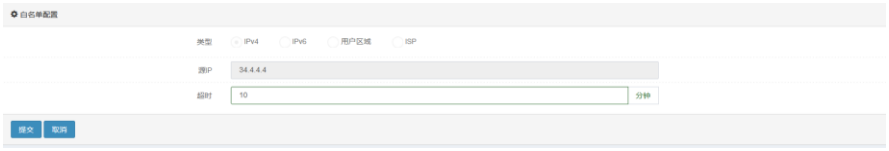
编辑窗口的白名单规格为 2048 条。

56.3.3 修改白名单

配置步骤：

1. 进入**策略>安全防护>白名单**，对于某条白名单，点击白名单前面的序号进入修改界面。

2. 可以对白名单表项内可修改时间进行修改，修改完毕后点击**提交**。



注意

编辑修改白名单时，类型和 IP 不能改变。
用户区域及 ISP 类型白名单无可修改内容。

56.3.4 删除白名单

配置步骤：

1. 进入**策略>安全防护>白名单**，选择**配置**，如下图：

2. 点击 删除某条白名单配置或者点击 删除全部白名单配置。

56.3.5 重置白名单命中数

配置步骤：

1. 进入**策略>安全防护>白名单**，选择**配置**，如下图：

2. 点击 重置某条白名单已有命中数。

注意

设备重启后白名单命中数均重置。

白名单超时后，已有命中数统计值保留。

56.3.6 全局开关白名单

配置步骤：

1. 进入**策略>安全防护>白名单**，选择**配置**，如下图：

2. 打开 白名单全局开关: 开 开关按钮，白名单**模块**对流经设备流量进行匹配放行处理。

注意

系统默认白名单全局开关状态为关闭。

56.3.7 查询白名单

配置步骤：

1. 进入**策略>安全防护>白名单**，选择**配置**，如下图：

2. 输入需要查找的白名单 IP 地址，点击进行查找，如下图：

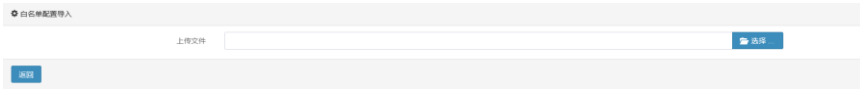
56.4 白名单配置导入导出

进入**策略>安全防护>白名单**，选择**配置**，如下图：

56.4.1 白名单导入

导入：可导入包含白名单配置的文本文件，系统会读取文件中的配置并执行下发。

点击选择，选择需要导入的白名单配置文件，如下图：



白名单导入配置须如下：

- **IPv4 类型**

whitelist-ip (x.x.x.x|x.x.x.x/x|x.x.x.0-x.x.x.255) timeout x configtime x-x-x x:x:x

x.x.x.x|x.x.x.x/x|x.x.x.0-x.x.x.255 ： IPv4 或 IPv4/掩码类型地址或 IP 范围，掩码可取(1~32)；

x：生效时间（分钟）；

x-x-x x:x:x ：配置起始的年-月-日 时：分：秒。

- **纯 IPv4**

x.x.x.x

x.x.x.x/x

纯 IPv4 或 IPv4/掩码类型地址，掩码可取值 1~32；

- **IPv6 类型**

whitelist-ipv6 (x:x::x:x|x:x::x:x/x) timeout x configtime x-x-x x:x:x

x:x::x:x|x:x::x:x/x ： IPv6 或 IPv6/掩码类型地址或 IP 范围，掩码可取(128|112|96|80|64)；

x ： 生效时间（分钟）；

x-x-x x:x:x ：配置生效时的年-月-日 时：分：秒。

- **用户区域类型**

whitelist-region province NAME timeout 0 configtime x-x-x x:x:x

NAME：区域名称，34个区域名称之一；

x-x-x x:x:x ：配置生效时的年-月-日 时：分：秒。

- **ISP 类型**

whitelist-isp NAME timeout 0 configtime x-x-x x:x:x

NAME：ISP 地址库名称；

x-x-x x:x:x ：配置生效时的年-月-日 时：分：秒。

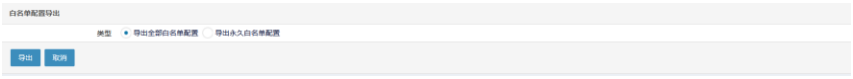
注意

导入文件如果有用户区域白名单类型，导入文档需使用 GB2312 编码。

56.4.2 白名单导出

导出：可将白名单的配置导出至一个文本文件中。

点击**导出**，如下图：



参数说明：

类型：支持两种白名单导出方式：导出全部白名单配置和只导出永久白名单配置。

选择类型点击**导出**按钮，设备根据导出类型及导出时间生成已命名的文档后，可操作页面弹窗保存至本地路径。

注意

导出文件如果有用户区域白名单类型，导出文档需用 GB2312 编码显示。

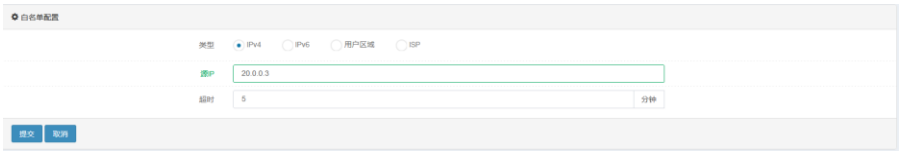
白名单导出前需先对当前配置进行保存。

56.5 配置案例

56.5.1 案例1：创建白名单

配置步骤：

1. 进入**策略>安全防护>白名单**，选择**配置**，点击**新建**按钮进入配置页面，配置源 IP 为 20.0.0.3 的白名单，如下图：



2. 点击**提交**，完成配置。

57 第57章 口令防护

57.1 口令防护概述

口令防护分为两个模块：弱口令检查、防口令暴力破解。

弱口令(weak password) 没有严格和准确的定义，通常认为容易被别人猜测到或被破解工具破解的口令均为弱口令。弱口令指的是仅包含简单数字和字母的口令，例如“123”、“abc”等，因为这样的口令很容易被别人破解，从而使用户的互联网账号受到他人控制，因此不推荐用户使用。

弱口令检查通过审计报文中的用户名和密码以及登陆状态，利用规则匹配的方式对密码进行检查，将检测到的弱口令进行日志上报。

口令暴力破解的意思是利用所有可能的字符组密码，尝试破解登录口令。这是最原始，粗暴的破解方法，根据运算能力，如果能够承受的起时间成本的话，最终一定会爆破出密码。而防口令暴力破解就是对此种攻击方式进行预防。

防口令暴力破解通过统计登录失败次数，来判断某个 IP 是否进行了口令暴力破解。一旦某个 IP 被认为是进行了暴力破解，则可以针对这个 IP 进行告警、阻断、精准阻断。

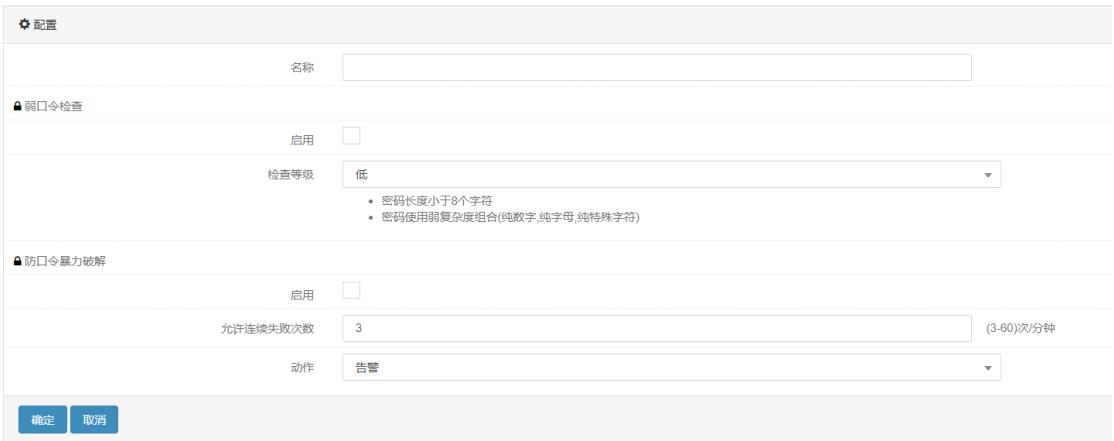
口令防护功能目前支持的协议有 FTP，POP3，IMAP，SMTP，HTTP，TELNET。

57.2 配置口令防护

57.2.1 新建口令防护模板

配置步骤：

1. 进入**策略>安全防护>口令防护**，如下图：



参数说明：

名称：口令防护模板名称。

弱口令检查：

启用：是否开启弱口令检查功能。

检查等级 ：弱口令检查的等级有高、中、低三种，选定某个检查等级之后会在 web 页面展示该等级弱口令判定的规则。

防口令暴力破解：

启用：是否开启防口令暴力破解功能。

允许连续失败次数：1 分钟内连续认证失败的次数。

动作：动作分为告警、阻断、精准阻断。

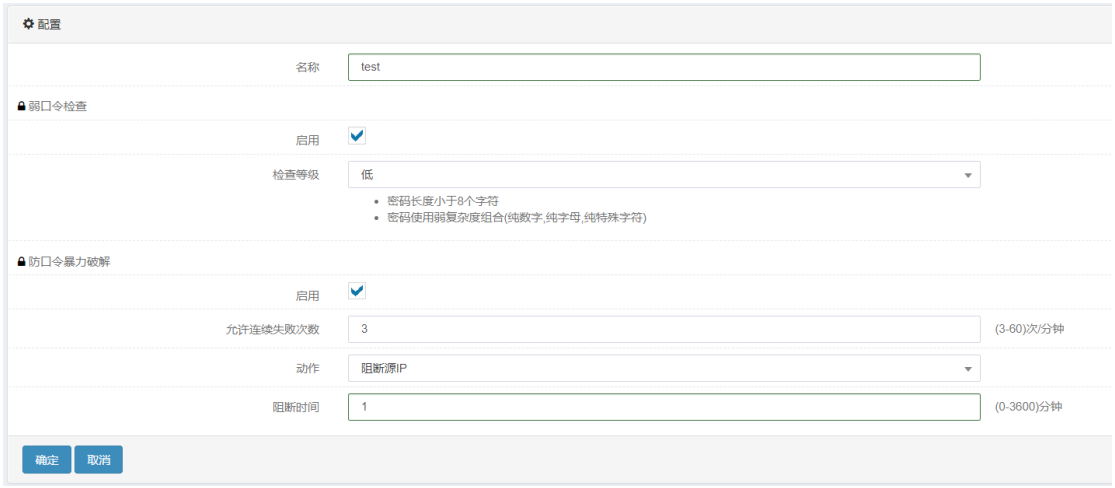
告警：发送告警日志

阻断：将该源 IP 加入黑名单

精准阻断：阻断三元组，源 IP、目的 IP、目的端口。

阻断时间：当动作为阻断时，该阻断时间代表源 IP 加入黑名单的时间。当动作为精准阻断时，该阻断时间代表阻断三元组的时间。

2. 配置完毕后，点击**确定**。



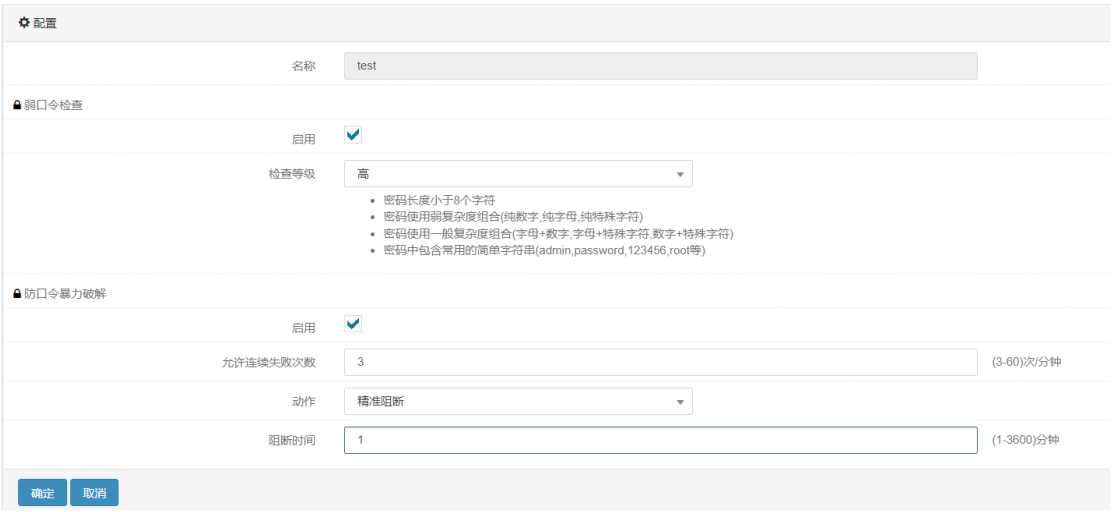
3. 点击**提交**，完成对口令防护的配置，显示如下页面：

57.2.2 编辑口令防护模板

已经创建的口令防护可以编辑修改。

1. 进入策略>安全防护>口令防护，如下图：

2. 单击需要修改的口令防护名称，进行修改编辑。



可以对口令防护进行配置修改，其中名称不能修改。

3. 点击更新完成修改的配置。

57.2.3 删除口令防护

1. 进入策略>安全防护>口令防护，如下图：

2. 单击需要删除的口令防护名称，点击进行删除。

3. 点击确定，完成口令防护的删除。

注意

正在被安全防护策略引用的口令防护，其删除按钮为灰色，不能被删除。

57.2.1 在安全防护策略中引用口令防护

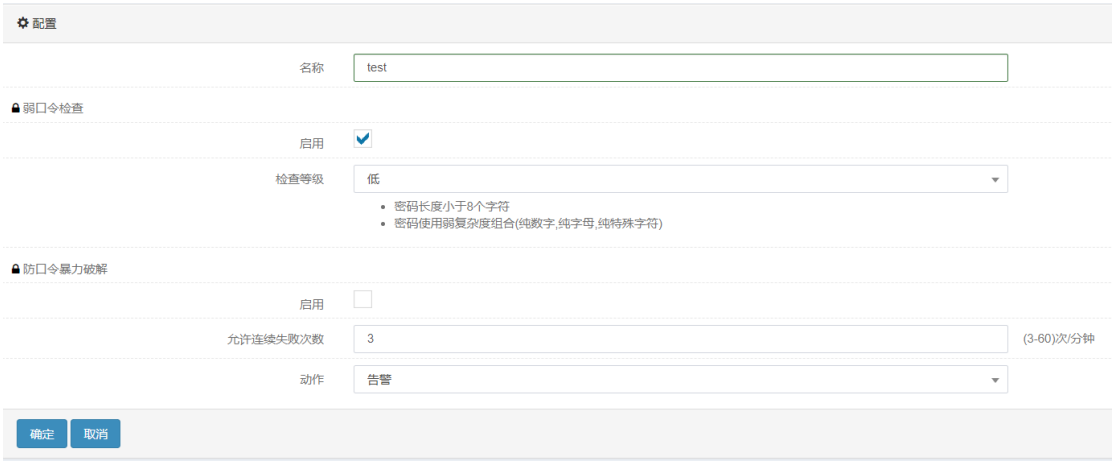
口令防护只有在安全防护策略中被引用才能生效，符合安全防护策略的报文才能受该口令防护的保护。

57.3 配置案例

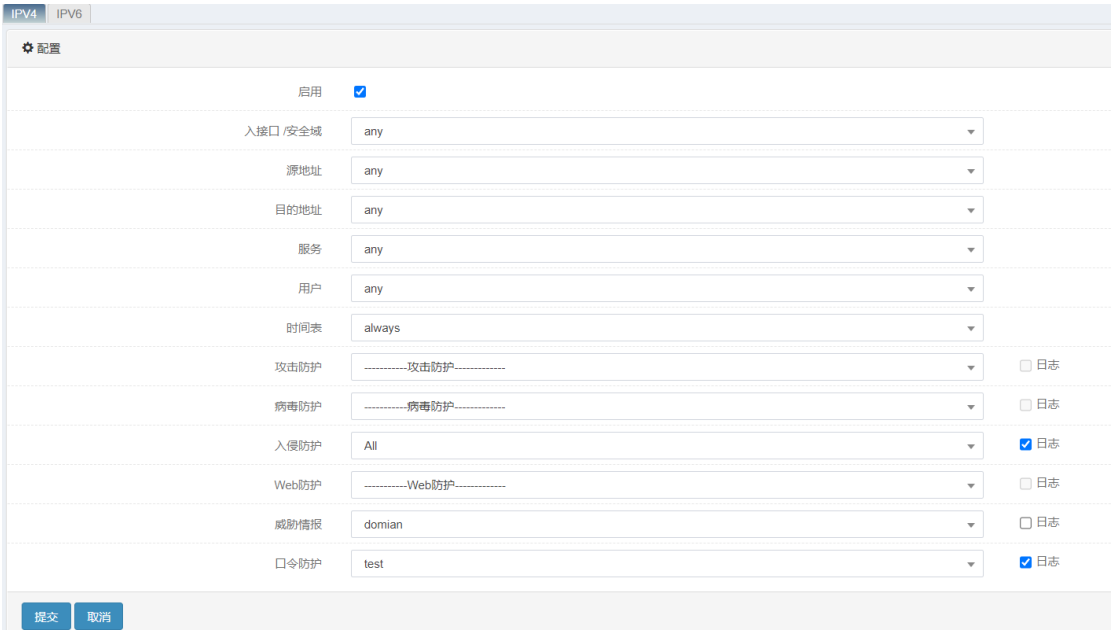
57.3.1 案例1：创建安全防护弱口令检查策略

配置步骤：

1. 进入**策略>安全防护>口令防护**，点击**新建**。选择启用弱口令检查功能，检查等级选择“低”，如下图：



2. 进入**策略>安全防护>防护策略**，点击**新建**，选择对应的参数，如下图：



3. 点击**提交**，完成配置。
4. 进入**策略>安全防护>防护策略**，勾选**启用**完成配置，如下图：

注意

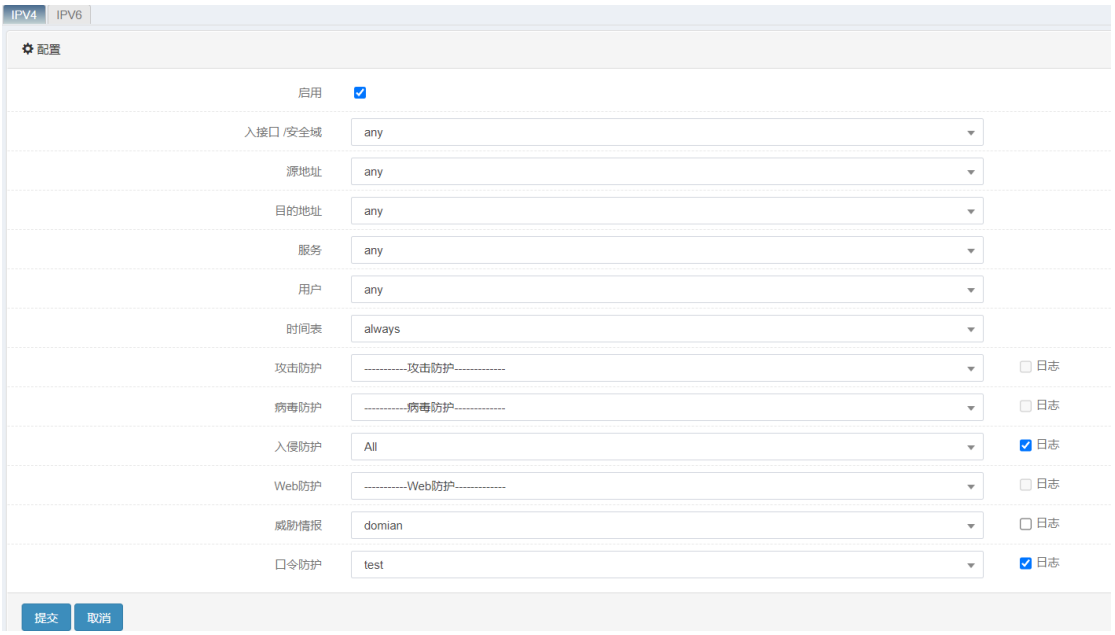
弱口令检查功能目前支持的协议有 FTP，POP3，IMAP，SMTP，HTTP，TELNET。

57.3.2 案例2：创建安全防护防口令暴力破解策略

配置步骤：

1. 进入**策略>安全防护>口令防护**，点击**新建**。选择启用防口令暴力破解功能，允许连续失败次数为 3 次，动作选择精准阻断，阻断时间为 1 分钟，如下图：

2. 进入**策略>安全防护>防护策略**，点击**新建**，选择对应的参数，如下图：



3. 点击**提交**，完成配置。
4. 进入**策略>安全防护>防护策略**，勾选**启用**完成配置，如下图：

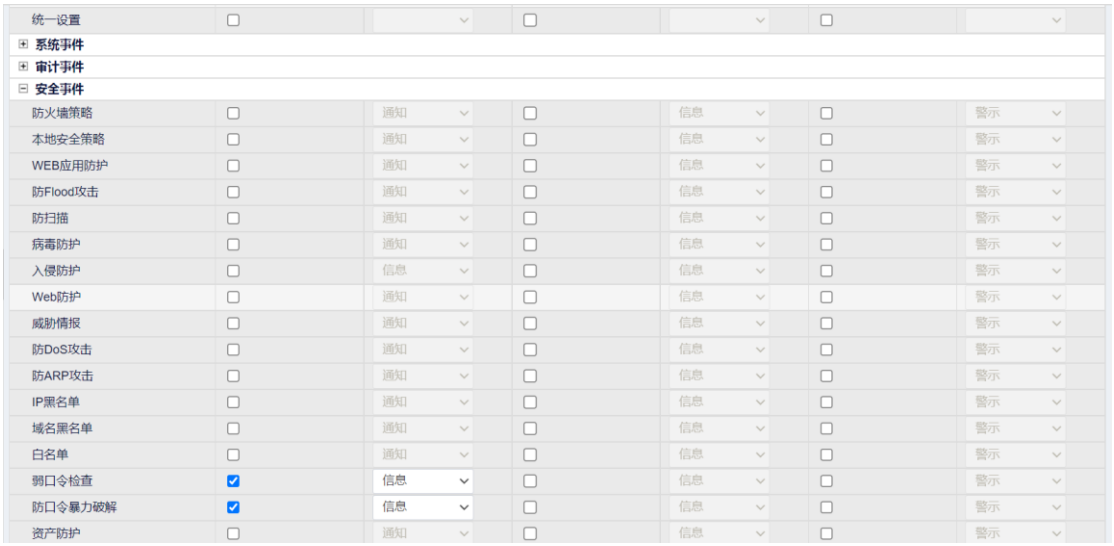
注意

防口令暴力破解功能目前支持的协议有 FTP，POP3，IMAP，SMTP，HTTP，TELNET。

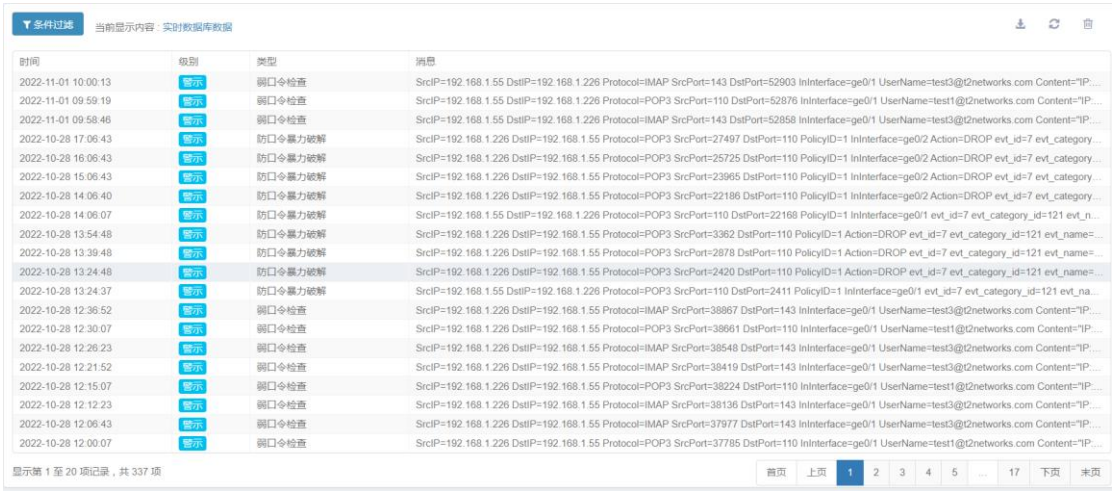
57.4 口令防护监控与维护

57.4.1 查看口令防护日志

1. 进入**日志>日志管理>日志过滤**，勾选防弱口令检查及防口令暴力破解的**相关**日志，并设置日志的级别，点击**确定**。



2. 进入**日志>安全日志>口令防护**里查看相关的口令防护安全日志。



58 第58章 Web 应用防护

58.1 概述

Web 应用防护可以防止 web 应用免受各种常见攻击，如 SQL 注入，跨站脚本攻击(XSS)，能够监测并过滤掉让应用遭受攻击的流量。它会在 HTTP 流量抵达应用服务器之前检测可疑访问，同时也能防止从 Web 应用获取某些未经授权的数据。

58.2 配置策略

58.2.1 策略的基本要素

web 应用防护策略的基本要素是匹配条件和动作。当站点地址，端口，入接口/安全域匹配成功时，则认为 web 应用防护策略命中。策略命中后，按照配置依次进行 HTTP 合规检查模板(如果有配置)、事件集(如果有配置)的检测。检测完成后，执行设置的动作。

当动作配置为“只检测不阻断”时，经过 HTTP 合规检查模板/事件集检测后，仅会上报检测的结果，不会对流量进行任何处理。

当动作配置为“按事件动作处理”时，经过 HTTP 合规检查模板/事件集检测侯，会根据 HTTP 合规模板或者事件的动作进行处理，如放行或阻断等。

58.2.2 新建策略

配置步骤：

1. 进入**策略>WEB 应用防护>策略**，点击新建，如下图。

参数说明：

启用：是否启用该策略。

名称：WEB 应用防护策略的名称。

站点地址：受保护 Web 服务器的 IP 地址。

端口：受保护 Web 服务器的端口。

入接口/安全域： 流量进入的接口或者安全域。

HTTP 合规检查模板：引用系统中配置好的 HTTP 合规模板，非必选项，可以不进行配置。

事件集：引用系统种存在的事件集，非必选项，可以不进行配置。

动作： 配置为“只检测不阻断”时，仅上报检测的结果，不会对流量进行其他处理。配置为“按事件动作处理”时，会根据匹配的合规检查模板/事件集中的动作进行处理，如放行或阻断等。

请求体： 是否检查客户端发往 Web 服务器的 http request body。

回应头：是否检查 Web 服务器发往客户端的 http response header。

回应体：是否检查 Web 服务器发往客户端的 http response body。

日志：日志开关，该日志开关和日志模块的日志开关都开启后才生效。

58.2.3 编辑策略

配置步骤：

1. 进入**策略>WEB 应用防护>策略**。
2. 点击策略 ID，进入编辑界面，如下图：

58.2.4 删除策略

配置步骤：

1. 进入**策略>WEB 应用防护>策略**。

2. 点击 ，可以删除一条策略，如下图。

58.2.5 移动策略

配置步骤：

1. 进入**策略>WEB 应用防护>策略**。

2. 点击 ，可以移动一条策略，如下图。

可以将策略移动到已有策略的之前或者之后，如下图所示。

58.2.6 插入策略

配置步骤：

1. 进入**策略>WEB 应用防护>策略**。

2. 点击 ，可以插入一条策略，如下图。

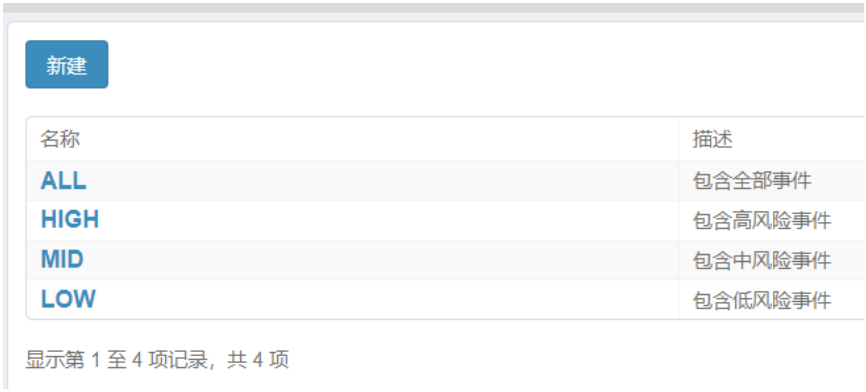
提交后会在该策略之上插入一条策略。

58.3 配置事件集

58.3.1 新建事件集

配置步骤：

1. 进入**策略>WEB 应用防护>事件集**，如下图。



由粗体显示的事件集名称，是系统预定义的事件集，不能被删除。

2. 点击**新建**，创建事件集，如下图：

参数说明：

名称：事件集名称。

描述：事件集的描述。

58.3.2 编辑事件集

配置步骤：

1. 进入**策略>WEB 应用防护>事件集**，如下图。

2. 对于某条存在的事件集，点击  按钮对事件集进行编辑。

58.3.3 删除事件集

配置步骤：

1. 进入**策略>WEB 应用防护>事件集**，如下图。

2. 对于某条存在的事件集，点击 按钮删除。

注意

预定义的事件集不能被删除，被策略引用的事件集也不能被删除。

58.3.4 复制事件集

配置步骤：

1. 进入**策略>WEB 应用防护>事件集**，如下图所示。

2. 对于某条存在的事件集，点击 按钮进行复制事件集操作。

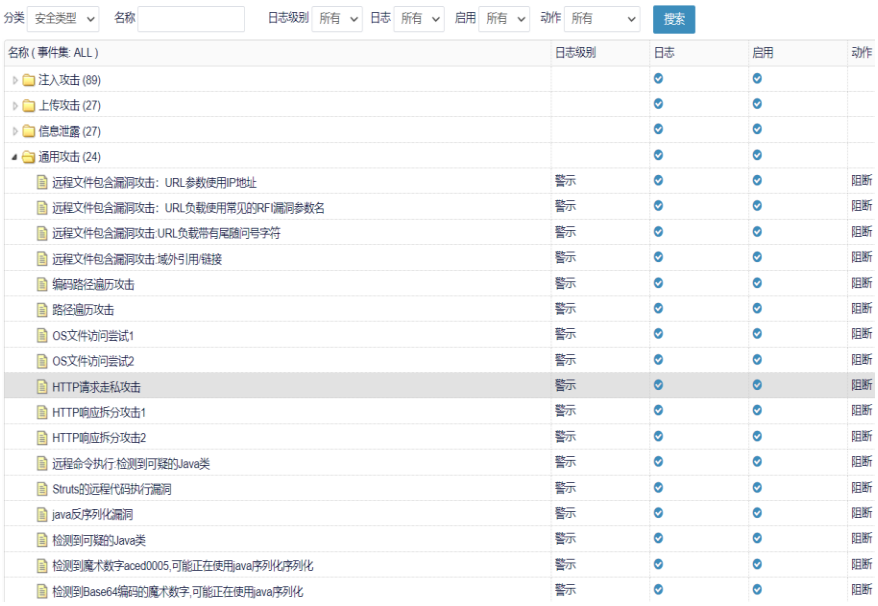
58.4 配置事件集中事件

58.4.1 查看事件

配置步骤：

1. 进入**策略>WEB 应用防护>事件集**，点击事件集名称或者 按钮，如下图。

2. 事件展示如下图：



58.4.2 添加事件

配置步骤：

1. 进入**策略>WEB 应用防护>事件集**，点击自定义事件集名称或者 。

2. 点击**添加事件**，如下图。

可以添加事件如下图。

3. 勾选要添加的事件，或者是要添加的事件大类，点击**提交**。

注意

1. 一个事件被添加到事件集后，再次点击添加事件按钮，这个事件将不再显示。
2. 只有自定义事件集才能添加事件。

58.4.3 编辑事件

配置步骤：

1. 进入**策略>WEB 应用防护>事件集**，点击自定义事件集名称或者 。

2. 点击 ，修改事件配置，可以修改单个事件，也可以修改一类事件，如下图。

修改完成后，点击**提交**。

注意

1. 编辑一类事件时，这类事件下所有事件配置都会被修改。
2. 只有自定义事件集才能添加事件。

58.4.4 删除事件

1. 进入**策略>WEB 应用防护>事件集**，点击自定义事件集名称或者 。

2. 点击 ，可以删除一个事件。

注意

只有有自定义事件集才能删除事件。

58.5 配置自定义事件

58.5.1 添加自定义事件

配置步骤：

1. 进入**策略>WEB 应用防护>自定义事件**，
2. 点击**新建**，如下图所示：

参数说明：

名称：自定义事件的名称。

描述：自定义的事件的描述。

检查字段：对 http 报文检测的字段。

匹配正则：对检查字段进行检查的正则表达式。

解码类型：对检查字段的内容进行相应的解码方式。

日志级别：该自定义事件上报日志时的级别。

日志：该自定义事件是否开启日志。

启用：是否启用该自定义事件。

动作：自定义事件的动作。当动作为“阻断源地址”时，会将报文的源 ip 地址加入到系统黑名单中。在黑名单模块添加方式展示为“WEB 应用防护阻断”。详见第 51 章 “黑名单防护”。

58.5.2 编辑自定义事件

配置步骤：

1. 进入**策略>WEB 应用防护>自定义事件**，
2. 点击事件名称，进入编辑界面，如下图：

58.5.3 删除自定义事件

配置步骤：

1. 进入**策略>WEB 应用防护>自定义事件**，

2. 点击 ，删除单个自定义事件，如下图

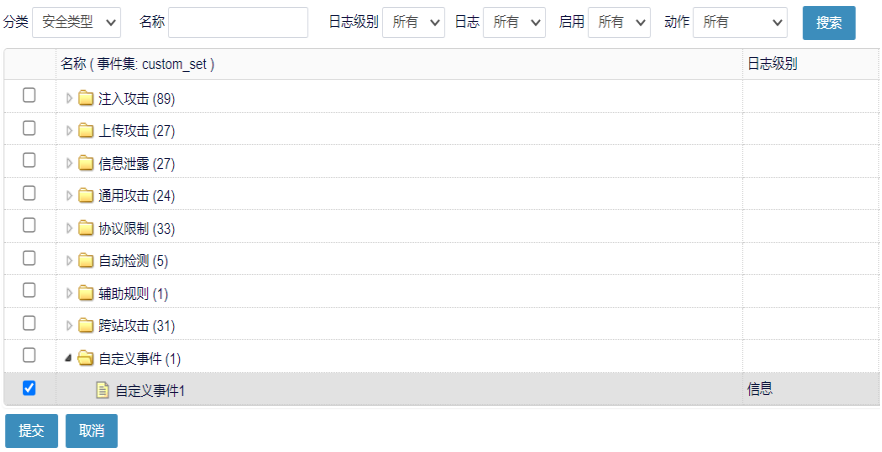
注意

当有自定义事件被事件集引用时，不能执行删除操作。

58.5.4 引用自定义事件

配置步骤：

1. 进入**策略>WEB 应用防护>事件集**，点击自定义事件集名称或者 。
2. 点击**添加事件**，选择自定义事件（可选一个，也可选多个），如下图。



58.6 配置合规检查模板

58.6.1 添加合规检查模板

配置步骤：

1. 进入**策略>WEB 应用防护>HTTP 合规检查模板**，
2. 点击**新建**，如下图。

参数说明：

名称：HTTP 合规检查模板的名称。

描述：HTTP 合规检查模板的描述。

HTTP 方法：检查 HTTP 报文中 HTTP 方法字段。如果预定义方法中没有出现时，可通过自定义 HTTP 方法的形式添加，动作可选择允许或禁止。

HTTP 协议版本号：检查 HTTP 报文中 HTTP 协议版本号字段。如果预定义版本号没有出现时，可通过自定义 HTTP 协议版本号的方式添加。动作可选择允许或禁止。

Content-type 类型：检查 HTTP 报文中 HTTP 头体里面 content-type 字段。如果预定义类型不满足需求时，可通过自定义 content-type 类型的方式添加。动作可选择允许或禁止。

Content-type 字符集：检查 HTTP 报文中 HTTP 头体里面 content 字段。如果预定义字符集不满足需求时，可自定义 content-type 字符集的方式添加。动作可选择允许或禁止。

文件名后缀：检查 HTTP 请求报文中传输文件的扩展名称。动作可选择允许或禁止。

HTTP 请求头：检查头 HTTP 报文中 HTTP 头域名称。动作可选择允许或禁止。

58.6.2 编辑合规检查模板

配置步骤：

1. 进入**策略>WEB 应用防护>HTTP 合规检查模板**，
2. 点击合规检查模板名称，进入编辑界面，如下图：

58.6.3 删除合规检查模板

配置步骤：

1. 进入**策略>WEB 应用防护>HTTP 合规检查模板**，

2. 点击 ，可以删除一个模板。

注意

当合规检查模板被策略引用时，不能执行删除操作。

58.7 配置参数

配置步骤：

1. 进入**策略>WEB 应用防护>参数配置**，如下图。

当事件动作为“阻断源 ip”时，报文源 ip 将被添加到系统黑名单模块，这个配置是源 ip 被添加到“黑名单”功能中被阻断的时间。详见第 51 章“黑名单防护”。

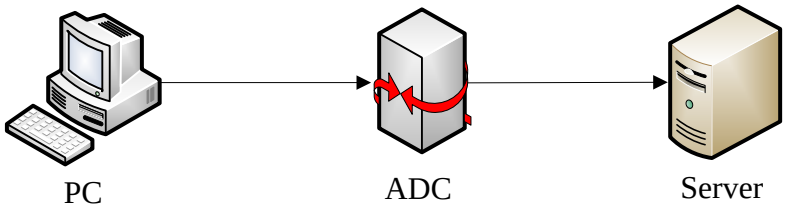
58.8 配置案例

58.8.1 阻断POST方法

案例描述

PC 通过防火墙设备访问 Web 服务器，阻断 POST 方法。

网络拓扑：



配置步骤：

1. 进入**策略>WEB 应用防护>合规检查模板**，如下图配置。

2. 进入**策略>WEB 应用防护>策略**，如下图配置。

3. PC 通过防火墙设备访问 Web 服务器，使用 POST 方法被阻断。

58.9 常见故障分析

58.9.1 自定义事件不能匹配

现象	自定义事件配置看似没有错误却没有被命中
分析	1. 如果http报文传输过程中编码了，配置时没有勾选解码类型，或者选择了错误的解码类型，会导致检查字段匹配错误。 2. 如果是检查请求体的内容，需要在WEB应用策略中将请求体打钩。
解决	1. 提前获知编码方式，选择正确的解码类型。 2. 确认是否需要检查请求体，需要的话要在策略中打钩。

59 第59章 应用控制策略

59.1 应用控制策略概述

应用控制策略，是在安全策略基础上的进一步扩展，也是防火墙的核心模块。该模块不再局限于简单地对 IP、端口的分析控制，进一步对报文的数据内容进行协议分析、特征识别，识别出流量所属的具体应用，进而完成对某些具体应用流量的过滤、审计等功能。如对 P2P 下载、在线视频的流量控制，就可以通过该模块完成。

应用控制模块的核心配置，即是应用参数的配置，主要包括：

- 应用，用来审计的目标应用。详细参照“应用对象”一章，目前防火墙可以识别的应用有 1000 多种，覆盖了当前流行的绝大多数应用。
- 应用行为，应用支持审计的动作，如登录、注销、下载文件等等。
- 应用行为参数，该应用行为支持的审计参数。如登录的用户名，下载的文件名等等。

应用控制策略通过定义以上参数，去匹配流量中的数据，一旦命中，即执行控制策略的动作：放行或者阻断，以及是否记录日志。

59.2 配置应用控制策略

59.2.1 配置策略的基本要素

应用控制策略的基本要素是匹配条件和动作。匹配条件包括地址对象、应用对象、应用行为、行为参数、关键字匹配、策略生效的时间范围。其中，地址对象、时间范围对象、关键字对象都都需要先建立好模板，策略的动作有“允许”，“拒绝”。

配置步骤：

1.进入**策略>应用控制>应用控制策略**，点击新建。

参数说明：

启用：是否启用该策略。

源地址：源地址对象或源地址对象组（目前只适用于 IPv4）。

用户：用户或用户组。

应用：应用分为 3 类，自定义应用、预定义应用组和单个的预定义应用，any 表示所有应用。引用下拉框支持模糊搜索

应用行为：应用特征库库可以识别的动作，如登录、注销、下载文件等等，any 表示所有应用行为。

时间表：策略生效的时间，可以引用已配置的时间对象，always 表示所有时间。

内容匹配：没有启用则匹配内容列表不生效，启用则匹配内容列表生效。

行为参数：以上配置的应用行为所支持审计的参数。如登录的用户名，下载的文件名等等。any 表示应用行为的所有参数。

关键字：引用建立好的关键字模板。当行为参数获取到的内容包含关键字内容(大小写敏感)，则匹配成功。any 代表匹配任何内容。

匹配类型：匹配类型分别包含和不包含两种。

匹配内容列表：根据行为参数+关键字+匹配类型的组合为一组，最多可以配置十组，匹配时只有都满足这些组合才算匹配成功

处理动作：对符合匹配条件的数据流执行的动作。

日志：日志开关，该日志开关和日志模块的日志开关都开启后才生效。

3. 配置完毕后，点击**提交**。


提示

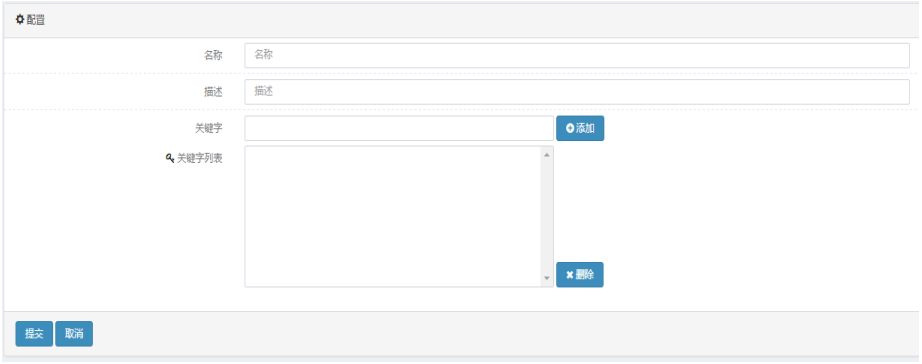
创建一条新的应用控制策略时，系统会自动生成该策略的 ID 号，策略 ID 是应用控制策略的唯一标识；匹配内容列表中所有组合全部匹配成功策略才算被命中。

59.2.2 关键字配置

关键字模板可以在应用控制模板里的关键字下拉菜单里直接新建引用，也可以在关键字模块优先创建。

配置步骤：

1. 进入**策略>应用控制>关键字**，如下图：



参数说明：

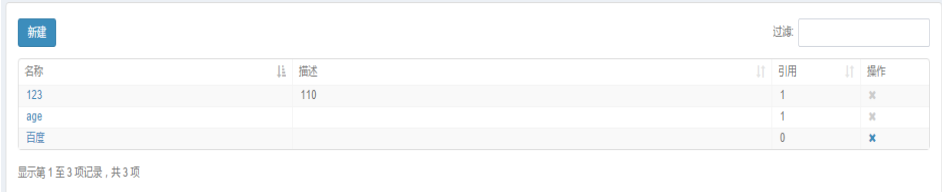
名称：关键字模板的名字。

描述：用户可以配置对关键字的描述信息。

关键字：要进行匹配的关键字，大小写敏感。

关键字列表：最多可配置 128 条关键字，匹配时只要满足一条关键字即算匹配成功。

2. 配置完毕后，点击**提交**。



59.2.3 启用应用控制策略

配置好的应用控制策略必须启用才能使其生效。

配置步骤：

1. 进入**策略>应用控制>应用控制策略**，如下图：

2. 勾选**启用**可以启用一条策略。

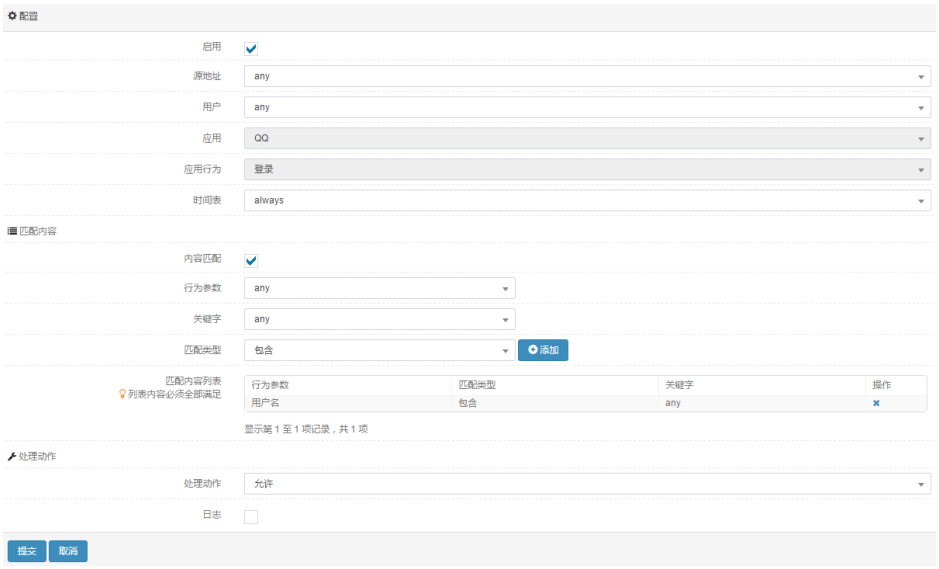
59.2.4 编辑应用控制策略

配置步骤：

3. 进入**策略>应用控制>应用控制策略**，对某条存在的应用控制策略点击策略 ID 号进入编辑界面。

4. 可以对应用控制策略里面的内容进行编辑修改，修改完毕后点击**提交。**

命中为命中该应用控制策略的计数，修改策略计数会清 0。



注意

编辑策略时，应用和应用行为都不能改变。

59.2.5 删除应用控制策略

配置步骤：

3. 进入**策略>应用控制>应用控制策略**，如下图：

4. 点击 删除策略。

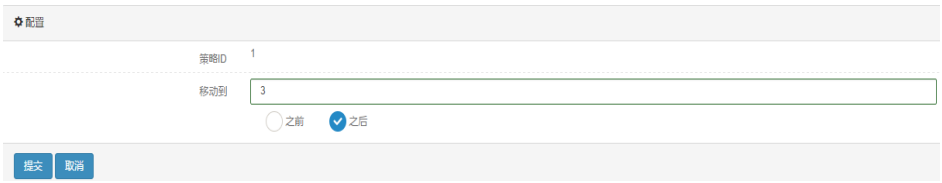
59.2.6 调整应用控制策略的顺序

通过移动策略可以调整应用控制策略的顺序，从而使位置在前的策略优先匹配。

配置步骤：

1. 进入**策略>应用控制>应用控制策略**，如下图：

2. 点击 移动策略。



策略 ID：需要被移动的策略的 ID 号。

移动到（策略 ID）：参考策略的 ID 号。

之前：移动策略到参考策略之前。

之后：移动策略到参考策略之后。

3. 点击**提交**。

注意

因为进行数据匹配时是根据策略的顺序至上而下进行匹配，命中成功后不再进行后续策略的匹配。

59.2.7 查询应用控制策略

查询步骤：

1. 进入**策略>应用控制>应用控制策略**，如下图：

2. 右上角的过滤框

过滤框可以根据页面配置的任何信息过滤。

例如：过滤 http

例如：过滤策略 ID

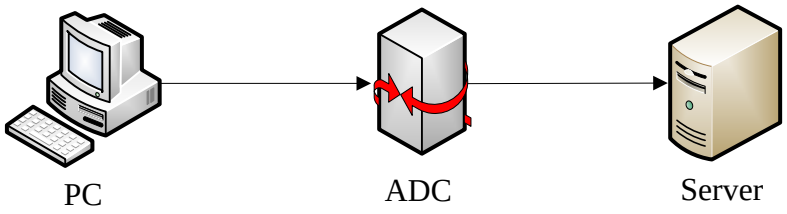
59.3 配置案例

59.3.1 案例1：阻断QQ号中包含“12456”的用户登陆

案例描述

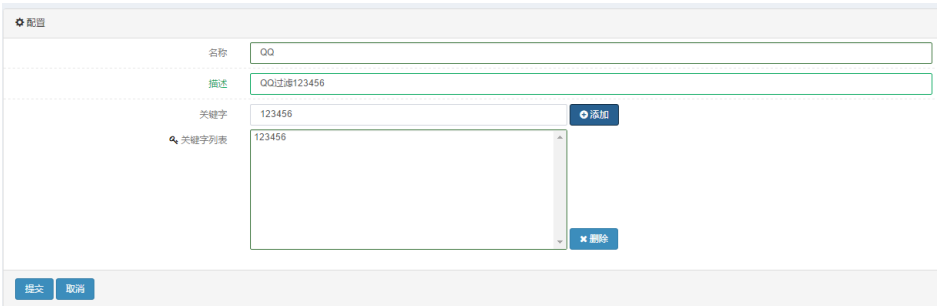
PC 通过防火墙设备访问外网。配置应用控制规则阻断 QQ 号中包含“123456”的用户登陆。

网络拓扑：



配置步骤：

1. 进入**策略>应用控制>关键字**，如下图：



2. 进入**策略>应用控制>应用控制策略**，如下图：

3. 点击**提交**，提交后如下图：

4. 配置完成

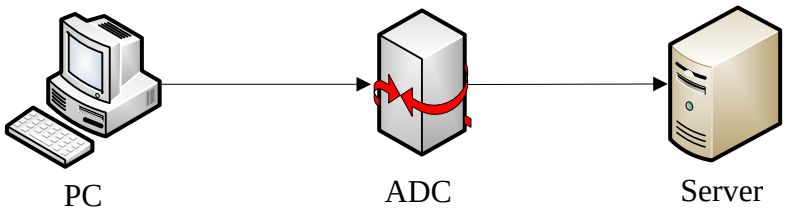
5. PC 上使用包含”123456”的 QQ 号登录，登陆被阻断。

59.3.2 案例2：拒绝接收所有电子邮件

案例描述

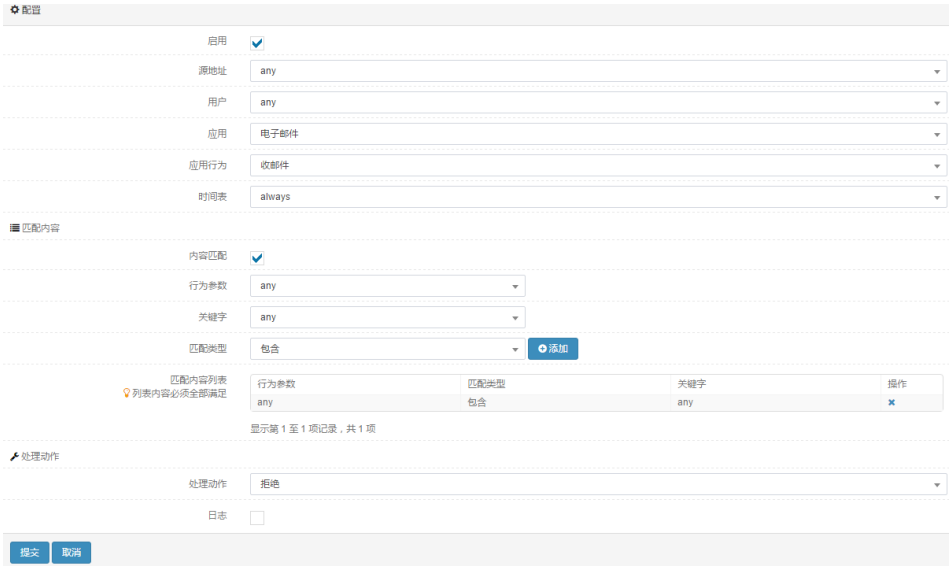
PC 通过防火墙设备访问外网。配置应用控制规则拒绝接收所有电子邮件。

网络拓扑：



配置步骤：

1. 进入**策略>应用控制>应用控制策略**，如下图：



2. 点击**提交**，提交后如下图：

3. 配置完成

4. PC 上登录邮箱后，收不到任何邮件。

59.4 常见故障分析

59.4.1 常见故障：策略没有命中

现象	策略配置看似没有错误却没有被命中
分析	一方面由于流量应用本身具有复杂和混合的特点，用户的一个访问可能有多种特征；另一方面，流量在传输过程中，特征会发生改变。比如HTTP访问，最开始是识别成HTTP，打开页面，应用引擎识别到新浪的特征后，流量应用标识被改变，HTTP的应用控制策略就匹配不了。正是因为复杂和变化的特点，导致应用控制策略配置起来难免会遇到流量无法匹配到策略的情况，主要有以下一些原因： ➢ ➢ 策略顺序。策略查找顺序和页面显示顺序一致。配置策略的时候，精确的应用（比如说新浪就比HTTP-网页浏览要精确）放在前面。 ➢ 多条关键字匹配为“与”的关系不要太复杂。 ➢ 加密流量不能审计到内容。很多网站现在都陆续迁移成HTTPS方式访问，如果要控制，只能通过证书识别了，比如说淘宝/天猫； ➢ 有防火墙策略冲突。防火墙策略和应用控制策略配置冲突时，假如都是阻断，应用控制策略就匹配不到了；（只要有一个策略阻断，就是可以阻断的）； ➢ 流量被识别成自定义的应用了：自定义应用优先级最高； ➢ 关键字能匹配的数据超过应用引擎审计长度。为了保证性能，应用引擎默认只审计20个数据包，后台有识别所有流量的开关，不建议打开； ➢ 应用特征更新了。请升级到最新的应用特征库版本。
解决	结合以上的分析，提出以下建议： ➢ 升级到最新的特征库版本； ➢ 配置较粗粒度的策略看是否可以命中，确认应用引擎确实生效； ➢ 调整策略顺序，确认页面上的策略顺序逻辑合理； ➢ 对于加密的访问，搜索是否有通行证的应用（通行证为证书特征），比如淘宝为阿里通行证；网易有网易通行证； ➢ 检查如果有配置特别粗的自定义应用，请删除； ➢ 缩小范围后可以稳定复现，收集好环境和操作步骤等信息反馈到售后支持；

60 第60章 Web 控制策略

60.1 Web控制策略概述

Web 访问控制审计功能可以对用户在某网站发布信息或者发布含有特定关键字信息的行为进行控制，并能对发布行为进行日志记录。例如，阻止用户在社区论坛类网站发布含有关键字“暴力”的信息，并记录发布行为日志。网络管理员可以针对不同用户、不同时间、不同信息发布行为制定适合的 Web 外发信息规则，系统将会对与规则相匹配的网络流量根据配置进行处理。

60.2 配置Web控制策略

60.2.1 配置策略的基本要素

Web 控制策略的基本要素是匹配条件和动作。匹配条件包括源地址、入接口、用户、URL 分类、文件类型、行为参数、关键字匹配、策略生效的时间范围。其中，地址对象、时间范围对象、关键字对象都需要先建立好。模板策略的动作有“允许”，“拒绝”。

配置步骤：

1.进入**策略>应用控制>Web 控制策略**，点击新建。

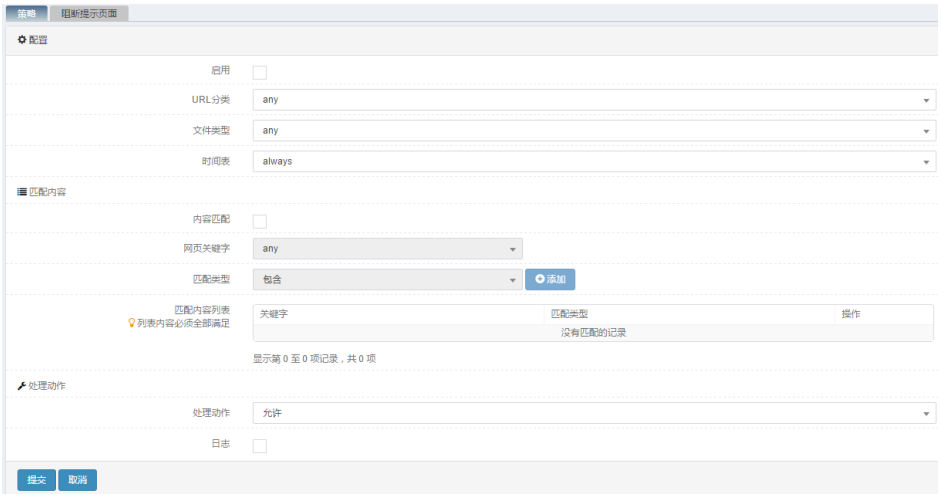
参数说明：

启用：是否启用该策略。

源地址：源地址对象或源地址对象组（目前只适用于 IPv4）。

用户：用户或用户组。

2.进入**策略>应用控制>Web 控制策略>控制规则列表**，点击新建。



参数说明：

启用：是否启用该策略的规则。

URL 分类：URL 分类分为 3 类，预定义 URL 分类、自定义 URL 分类、预定义 URL 分类组，any 表示所有 URL 分类。引用下拉框支持模糊搜索。

文件类型：引用建立好的关键字模板。当行为参数获取到的内容包含关键字内容(大小写敏感)，则匹配成功。any 代表匹配任何内容。

时间表：策略生效的时间，可以引用已配置的时间对象，always 表示所有时间。

内容匹配：没有启用则匹配内容列表不生效，启用则匹配内容列表生效。

网页关键字：引用建立好的关键字模板。当行为参数获取到的内容包含关键字内容(大小写敏感)，则匹配成功。any 代表匹配任何内容。

匹配类型：匹配类型分别包含和不包含两种。

匹配内容列表：根据行为参数+关键字+匹配类型的组合为一组，最多可以配置十组，匹配时只有都满足这些组合才算匹配成功

处理动作：对符合匹配条件的数据流执行的动作，允许或拒绝。

日志：日志开关，该日志开关和日志模块的日志开关都开启后才生效。

3.配置完毕后，点击**提交**。


提示

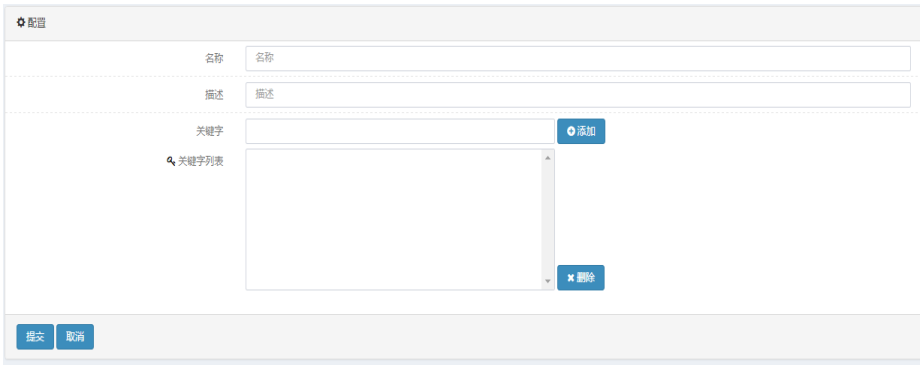
创建一条新的 Web 控制策略时，系统会自动生成该策略的 ID 号，策略 ID 是 Web 控制策略的唯一标识；匹配内容列表中所有组合全部匹配成功策略才算被命中。

60.2.2 关键字配置

关键字模板可以在应用控制模板里的关键字下拉菜单里直接新建引用，也可以在关键字模块优先创建。

配置步骤：

2. 进入**策略>应用控制>关键字**，如下图：



参数说明：

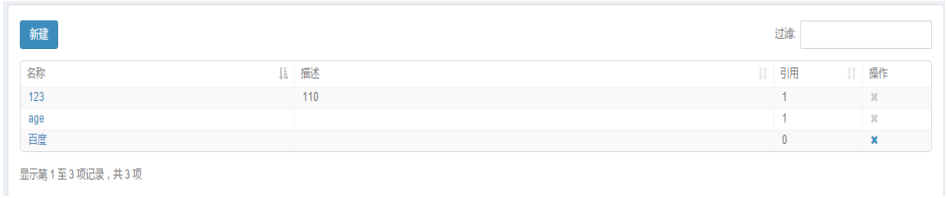
名称：关键字模板的名字。

描述：用户可以配置对关键字的描述信息。

关键字：要进行匹配的关键字，大小写敏感。

关键字列表：最多可配置 128 条关键字，匹配时只要满足一条关键字即算匹配成功。

2. 配置完毕后，点击**提交**。



60.2.3 启用Web控制策略

配置好的 Web 控制策略必须启用才能使其生效。

配置步骤：

3. 进入**策略>应用控制>Web 控制策略**，如下图：

4. 勾选**启用**可以启用一条策略。

60.2.4 编辑Web控制策略

配置步骤：

5. 进入**策略>应用控制>Web 控制策略**，对某条存在的 Web 控制策略点击策略 ID 号进入编辑界面。

6. 可以对 Web 控制策略里面的内容进行编辑修改，修改完毕后点击**提交。**

提示

命中为命中该 Web 控制策略的计数，修改策略计数会清零。

注意

编辑策略时，控制规则列表里的规则需要启用才会生效。控制规则列表的优先级是至上而下。

60.2.5 删除Web控制策略

配置步骤：

5. 进入**策略>应用控制>Web 控制策略**，如下图：

6. 点击 删除策略。

60.2.6 调整Web控制策略的顺序

通过移动策略可以调整 Web 控制策略的顺序，从而使位置在前的策略优先匹配。

配置步骤：

4. 进入**策略>应用控制>Web 控制策略**，如下图：

5. 点击 移动策略。

策略 ID：需要被移动的策略的 ID 号。

移动到（策略 ID）：参考策略的 ID 号。

之前：移动策略到参考策略之前。

之后：移动策略到参考策略之后。

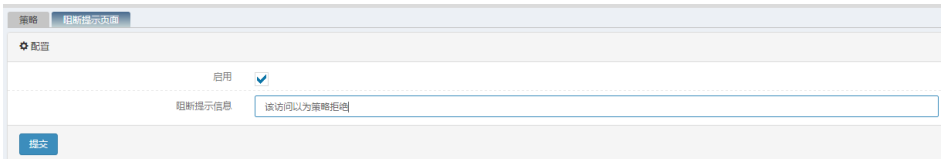
6. 点击**提交**。

因为进行数据匹配时是根据策略的顺序至上而下进行匹配，命中成功后不再进行后续策略的匹配。

60.2.7 阻断提示页面

查询步骤：

1.进入**策略>应用控制>Web 控制策略**，如下图：



参数说明：

启用：是否启用阻断提示页面。

阻断提示信息：用户自定义该策略处理动作为拒绝时在页面上提示的内容。

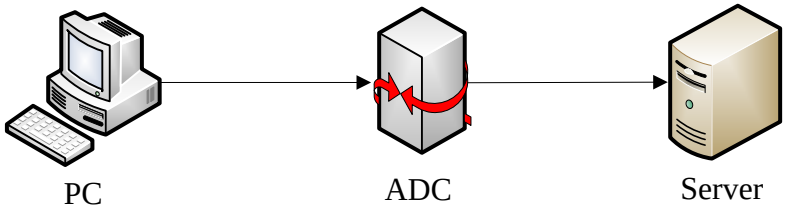
60.3 配置案例

60.3.1 案例1：阻断所有新闻网页并提示该网络禁止访问新闻

案例描述

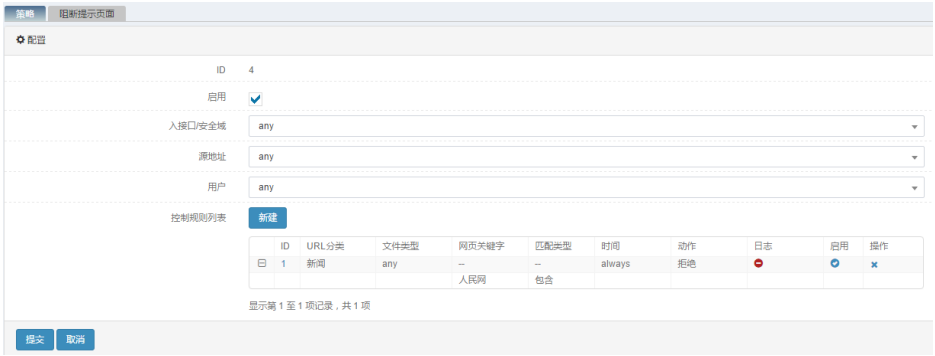
PC 通过防火墙设备访问外网。配置阻断所有新闻网页并提示该网络禁止访问新闻。

网络拓扑：



配置步骤：

1.进入**策略>应用控制>Web 控制策略**，如下图：



2.点击**提交**，提交后如下图：

3.配置完成

4.PC 上禁止访问新闻网页。

60.4 常见故障分析

60.4.1 常见故障：策略没有命中

现象	策略配置看似没有错误却没有被命中
分析	➢ 多条关键字匹配逻辑错误。 ➢ 加密流量不能审计到内容。很多网站现在都陆续迁移成HTTPS方式访问，比如说淘宝/天猫； ➢ 有防火墙策略冲突。防火墙策略和Web控制策略配置冲突时，假如都是阻断，Web控制策略就匹配不到了；（只要有一个策略阻断，就是可以阻断的）； ➢ 关键字能匹配的数据超过应用引擎审计长度。为了保证性能，应用引擎默认只审计20个数据包，后台有识别所有流量的开关，不建议打开； ➢ URL特征库过期。
解决	结合以上的分析，提出以下建议： ➢ 升级到最新的URL特征库版本； ➢ 配置较粗粒度的策略看是否可以命中，确认应用引擎确实生效； ➢ 调整策略顺序，确认页面上的策略顺序逻辑合理； ➢

61 第61章 APT 联动

61.1 APT联动概述

APT 产品用于检测网络中传输的文件是否有恶意行为。防火墙设备的 APT 联动功能，主要是对流经设备的网络数据进行文件还原，发送给 APT 设备进行检测，对恶意文件溯源、记录，以及提供 APT 文件检测结果的快速查询。

防火墙设备的 APT 联动模块目前只支持与启明星辰的 APT 产品进行联动。

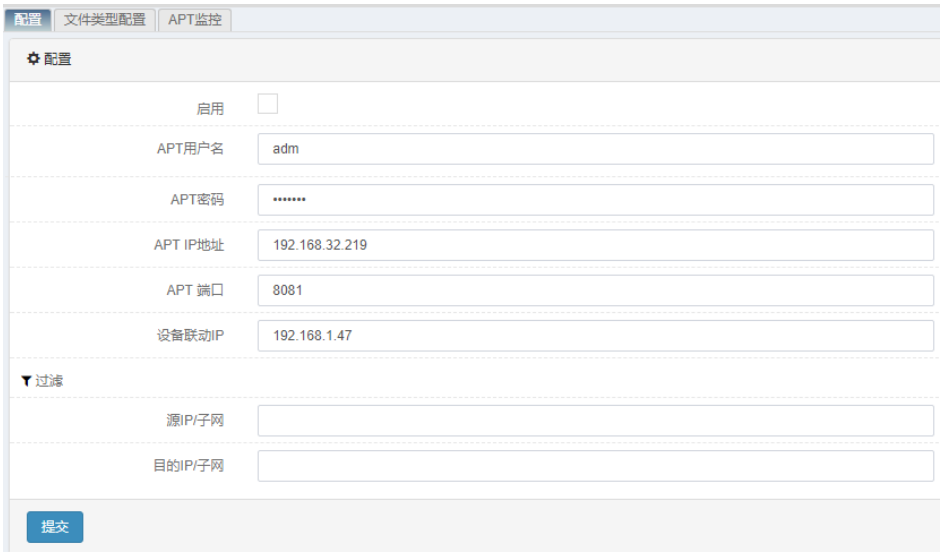
61.2 配置APT联动

61.2.1 配置联动的基本要素

APT 联动的基本要素是对端 APT 设备的用户名、密码、IP 地址、端口和本地设备的 IP 地址。

配置步骤：

1. 进入**安全联动>APT 联动**，配置。



参数说明：

启用：是否启用该联动。

APT 用户名：对端的 APT 设备的用户名

APT 密码：对端的 APT 设备的密码

APT IP 地址：对端的 APT 设备的 IP 地址

APT 端口：对端的 APT 设备的端口号

设备联动 IP：本地设备与 APT 设备通信的 IP 地址

过滤：

源 IP/子网：进行文件检测的源 IP 地址过滤

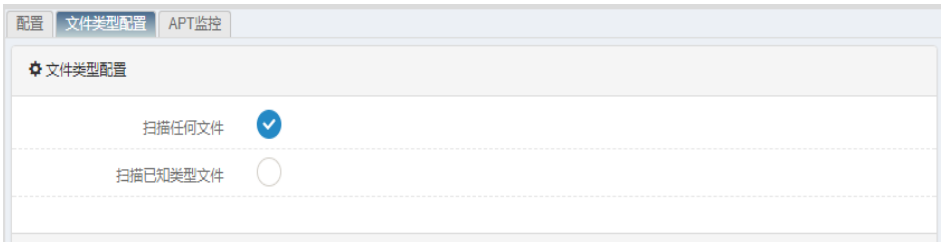
目的 IP/子网：进行文件检测的目的 IP 地址过滤

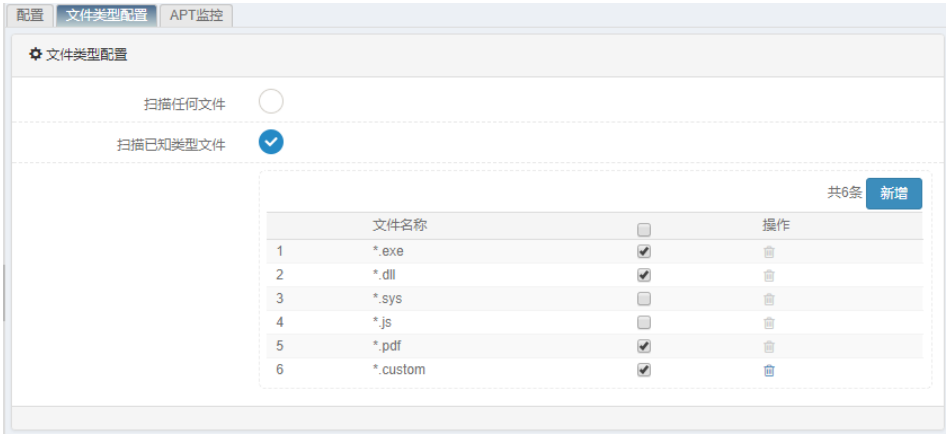
2. 配置完毕后，点击**提交**。

过滤部分如果没有配置，代表任意 IP 均做文件检测

61.2.2 APT文件类型过滤

配置步骤：





参数说明：

扫描任何文件：不做类型过滤，检测所有文件。

扫描已知类型文件：对配置且启用的类型进行文件检测。可以增加或删除

自定义的文件类型。

文件过滤类型只有启用了才有效果。

61.2.3 APT监控

APT 监控用来显示检测出的恶意文件信息。

参数说明：

威胁文件数/检测文件数：检测出的恶意文件数/上传进行检测的文件总数

文件名称：检测出的恶意文件名称

源 IP：恶意文件的源 IP

源端口：恶意文件的源端口

目的 IP：恶意文件的目的 IP

目的端口：恶意文件的目的端口

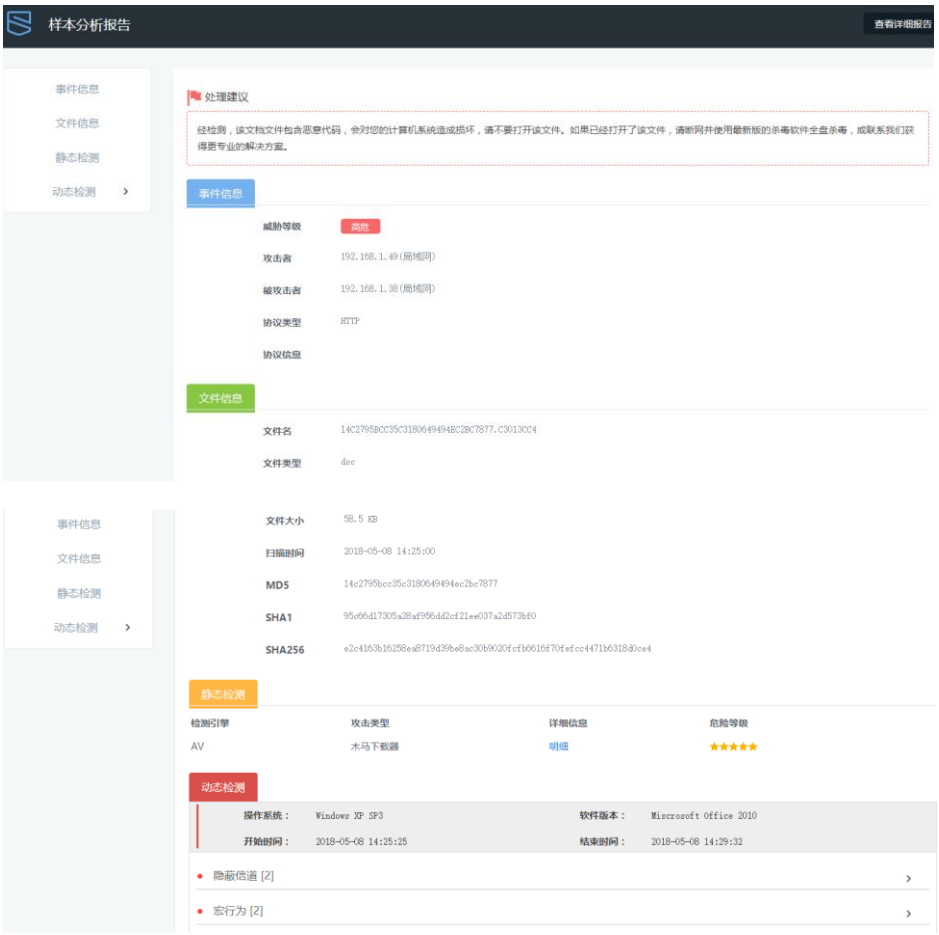
级别：恶意文件的危险级别(高危、中危、低危)，对应着红黄蓝三个颜色。

时间：恶意文件的检测时间

操作：分为阻断和详细信息

61.2.4 APT检测结果详细信息

对检测出的威胁文件结果可以查看病毒的详细信息。



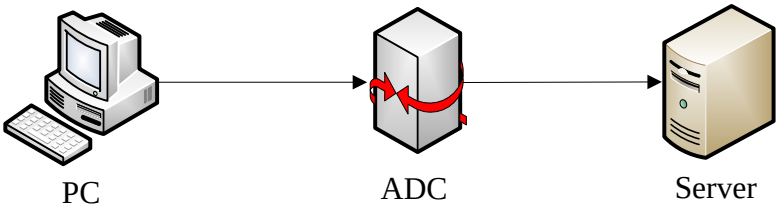
61.3 配置案例

61.3.1 案例：PC通过防火墙设备访问外网下载病毒文件APT联动可以检测并报警

案例描述

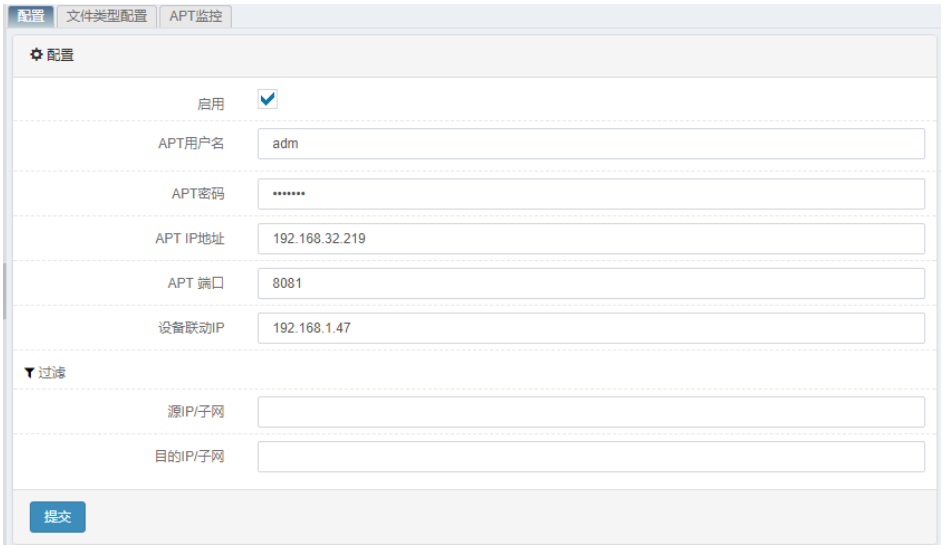
PC 通过防火墙设备访问外网下载病毒文件 APT 联动可以检测并报警。

网络拓扑：

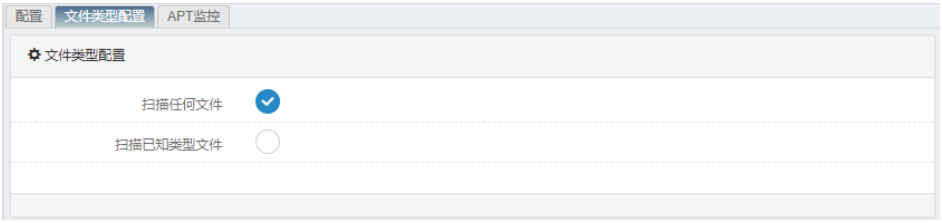


配置步骤：

1. 进入**安全联动>APT 联动>配置**，如下图：

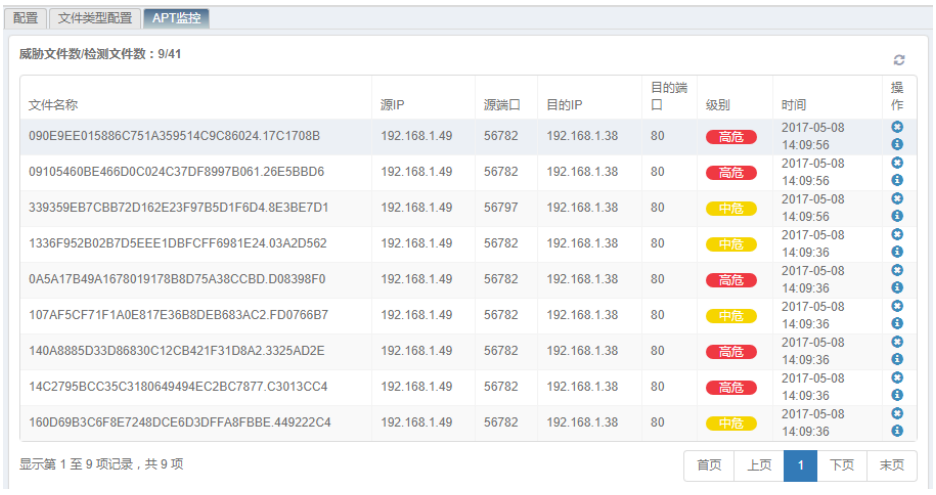


2. 进入**安全联动>APT 联动>文件类型配置**，如下图：



3. 配置完成

4. 检测结果



61.4 常见故障分析

61.4.1 常见故障：匹配不到想要检测的文件

现象	匹配不到想要检测的文件
分析	APT检测默认检测协议是HTTP，有可能是没有相对应的协议设置，或者是没有相对应的文件类型设置
解决	通过命令行将对应的协议(http.imap.smtp.pop3)设置上（命令行命令：apt-file protocol http.imap.smtp.pop3），检查文件要匹配的类型是否启用

62 第62章 IDS 联动

62.1 IDS联动概述

防火墙设备通过接收 IDS 产品发送来的动态过滤规则，从而为网络提供动态的安全防护特性。

防火墙设备的 IDS 联动模块支持同时接收多个 IDS 设备发送的过滤规则，目前只支持与启明星辰的 IDS 产品进行联动。

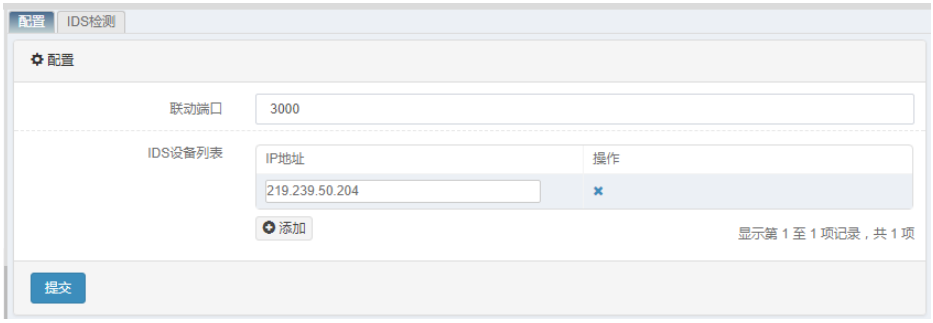
62.2 配置IDS联动

62.2.1 配置联动的基本要素

IDS 联动的基本要素是 IDS 设备的端口和 IP。

配置步骤：

1. 进入**安全联动>IDS 联动**，配置。



参数说明：

联动端口：默认为 3000，可配置的范围为<1—65535>，不输入参数时，使用默认值

IP 地址：填写需要联动的 IDS 设备的 IP 地址。最多可以添加 100 个 IDS 地址。

2. 正确输入各参数
3. 配置完成后，点击**提交**以使配置生效

62.2.2 IDS监控

配置步骤：

进入**安全联动>IDS 联动>IDS 监控**

页面上根据动态规则的生成次序显示防火墙设备中的动态规则；

可以根据协议或者 IDS 设备的 IP 进行过滤；

点击 可以单独删除一条规则，或者点击 按钮删除所有的规则。

62.3 配置案例

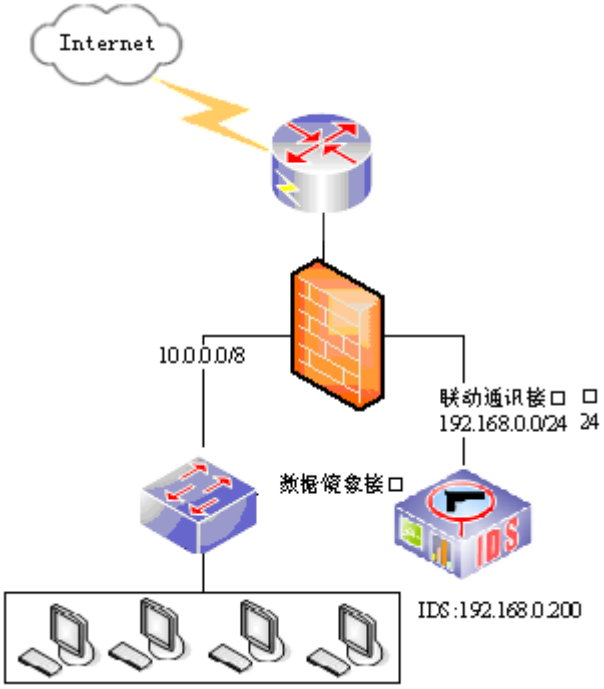
62.3.1 案例：低流量网络的防火墙设备与IDS实施方案

案例描述：

由于网络流量比较低，使用一个 IDS 来对网络内所有通讯数据进行监控并向防火墙设备发送联动规则。

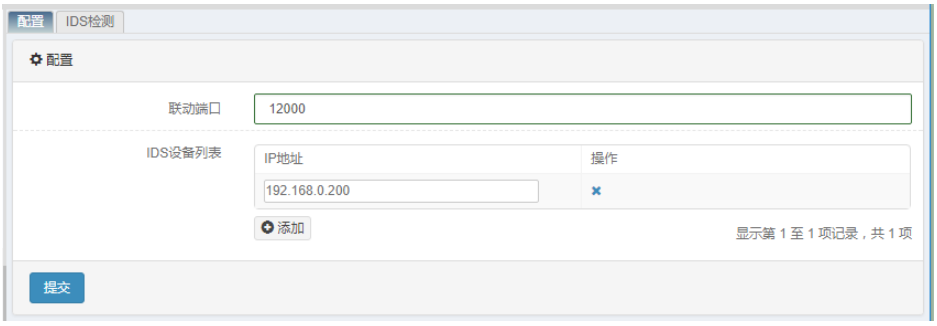
基本原则是：IDS 处于防火墙设备的保护网络中，对被保护网络内的数据进行监控。

用户使用 10.0.0.0/8 网络地址工作，IDS 与防火墙设备使用 192.168.0.0/16 网络地址进行控制和协同工作。建议 IDS 与防火墙设备控制和协同工作网络与实际业务网络分离，以确保安全和实时性，但其与业务网络可以处于同一网络中。



配置步骤：

1. 进入**安全联动>IDS 联动>配置**



2. 如图输入合理的参数。

3. 点击**提交**按钮使配置生效。

62.4 常见故障分析

62.4.1 常见故障：IDS发出动态规则，但NG-FW未阻断

现象	IDS设备报告已发送联动规则，但NG-FW未阻断相关数据报文。
分析	有以下几个可能的原因：

	1)IDS设备和NG-FW之间的数据加密认证状态不一致； 2)IDS设备和NG-FW通讯端口设置不一致； 3)未将IDS设备IP添加到NG-FW中的IDS设备IP列表中；
解决	1) 先查看设备相关配置，保证配置一致性； 2) 使用debug ids-interaction命令，查看NG-FW和IDS的交互信息； 3) 操作IDS设备，要求其重新与NG-FW进行加密认证。

63 第63章 CSP 联动

63.1 CSP联动概述

防火墙设备通过接收 CSP 设备发送来的动态过滤规则，从而为网络提供动态的安全防护特性。

防火墙设备的 CSP 联动模块支持同时接收多个 CSP 设备发送的过滤规则，目前只支持与启明星辰的 CSP 设备进行联动。

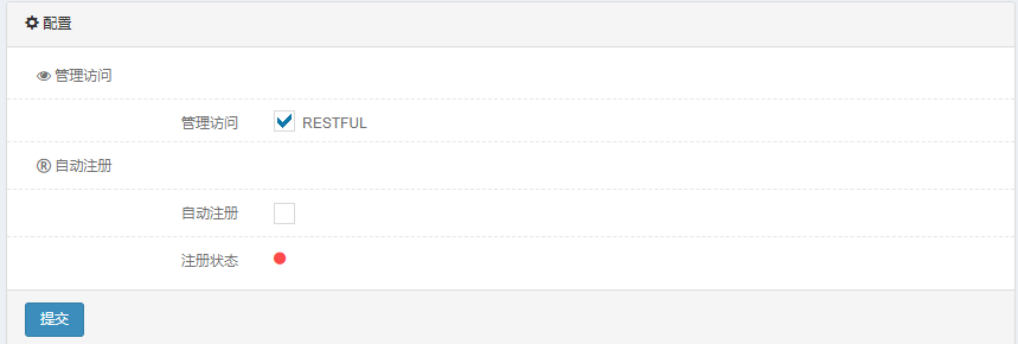
63.2 配置CSP联动

63.2.1 配置联动的基本要素

CSP 联动需要开启集中管理管理访问

配置步骤：

4. 进入**系统>配置>集中管理**，配置。



63.2.2 CSP监控

配置步骤：

进入**安全联动>CSP 联动**

页面上根据动态规则的生成次序显示防火墙设备中的动态规则；

可以根据协议或者 CSP 设备的 IP 进行过滤；

点击 可以单独删除一条规则，或者点击 按钮删除所有的规则。

64 第64章 天珣联动

64.1 天珣联动概述

天珣内网安全管理系统是启明星辰公司的一款内网安全管理与审计系统，通过天珣客户端、策略服务器、策略网关、策略网关代理，以及和交换机、防火墙等设备的配合，能实现准入控制、主动防御、桌面管理、防泄密、终端审计等功能。

防火墙设备可以作为天珣策略网关与天珣系统进行联动。天珣策略网关代理向防火墙下发管理网段，对管理网段内的主机，防火墙通过天珣策略网关代理查询内网主机的状态信息，并根据状态信息，拒绝或允许内网主机通过防火墙设备。

主机的状态分为：符合策略(SATISFIED)、不符合策略(UNSATISFIED)、未知(UNKNOWN)这 3 种。符合策略表示主机安装了天珣准入控制客户端，并且安全状态符合策略服务器的配置要求；不符合策略表示主机安装了天珣准入控制客户端，但安全状态不符合策略服务器的配置要求；未知表示主机未安装天珣准入控制客户端，或其他原因导致策略网关代理无法获取客户端的状态信息。只有主机状态为符合策略时，才允许该内网主机通过 FW 设备进行网络访问。

用户可以实时查看内网主机的状态信息，也可以删除全部或者指定主机的状态信息。

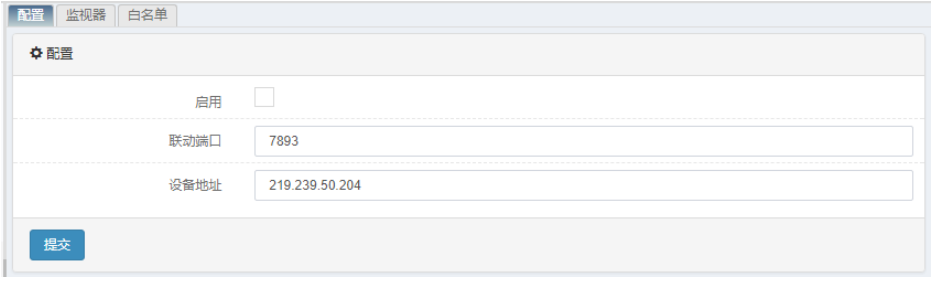
64.2 配置天珣联动

64.2.1 配置联动的基本要素

天珣联动的基本要素是天珣设备的端口和 IP。

配置步骤：

1. 进入**安全联动>天珣联动**，配置。



参数说明：

启用：是否启用联动。

联动端口：默认为 7893，可配置的范围为<1—65535>，不输入参数时，使用默认值

设备地址：天珣服务器的 IP 地址

2. 正确输入各参数

3. 配置完成后，点击**提交**以使配置生效

64.2.2 配置白名单

天珣联动白名单功能：匹配白名单列表（五元组匹配）的流不再进行天珣联动策略检查。

配置步骤：

进入**安全联动>天珣联动>白名单**

参数说明：

协议：白名单的协议类型，有 **ANY/TCP/UDP/ICMP/OTHER** 五种，根据选择的协议不同，随后的配置页面也会有变化，默认为 **ANY**

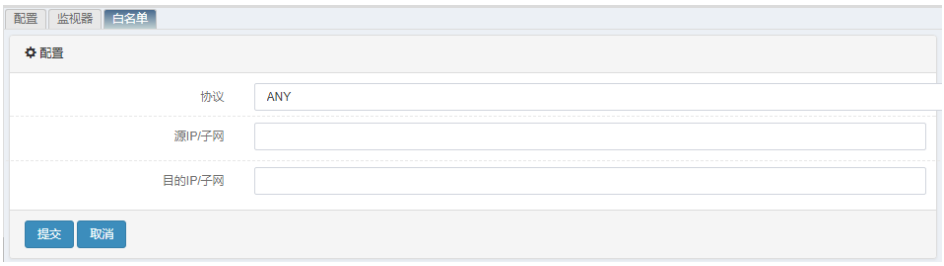
源 IP/子网：流的源 IP 地址，可以输入地址/子网掩码

目的 IP/子网：流的目的 IP 地址，可以输入地址/子网掩码

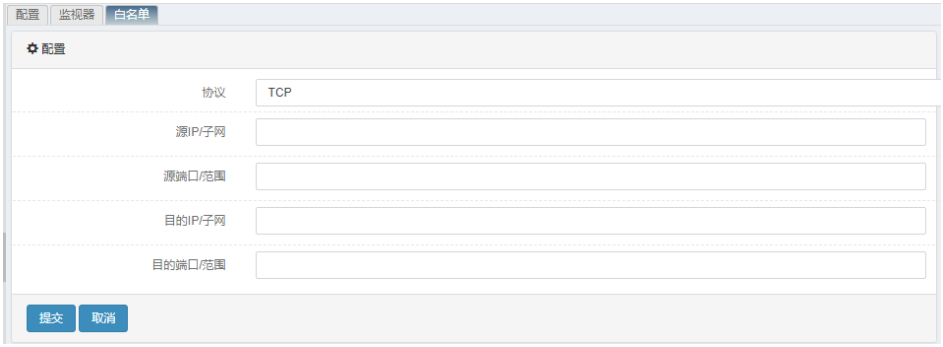
源端口/范围：流的源端口，可以输入端口/端口范围

目的端口/范围：流的目的端口，可以输入端口/端口范围

点击**新建**按钮，创建白名单。



当**协议**选择 **TCP/UDP** 时：

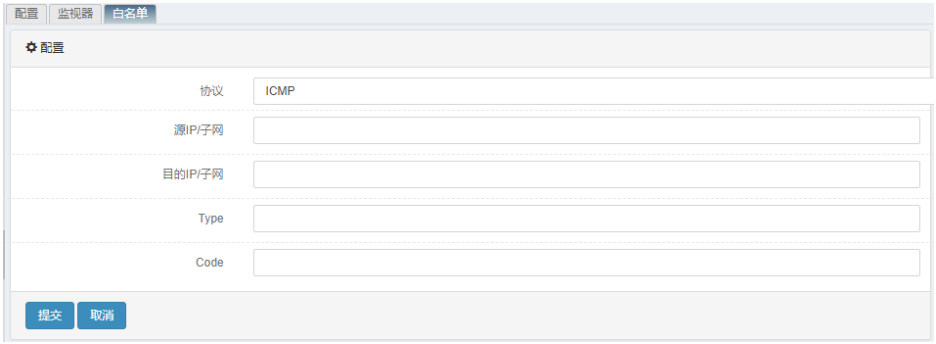


参数说明：

源端口/范围：流的源端口，可以输入端口/端口范围；

目的端口/范围：流的目的端口，可以输入端口/端口范围；

当**协议**选择 **ICMP** 时：

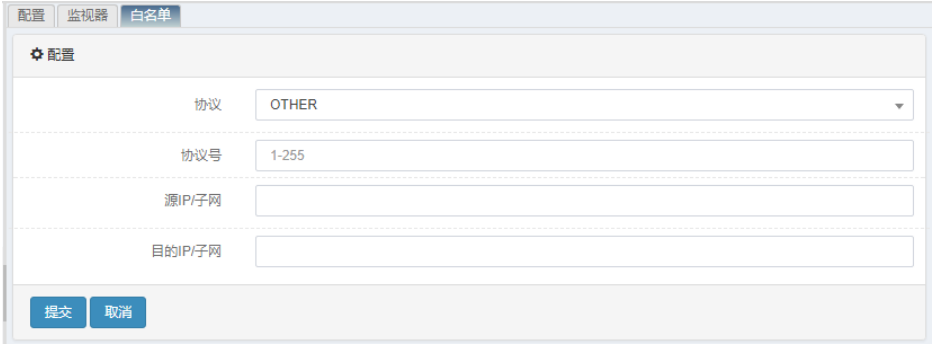


参数说明：

Type： ICMP 流的 Type 值

Code： ICMP 流的 Code 值

当**协议**选择 **OTHER** 时，配置界面如下：



参数说明：

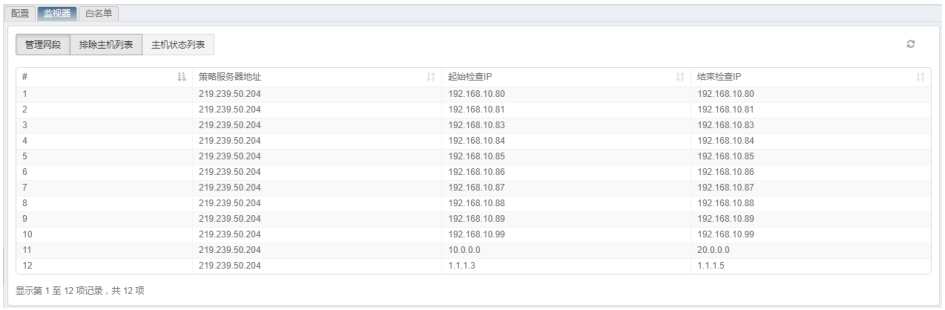
协议号：流的协议号，范围 1-255，不能输入 ICMP、TCP 和 UDP 对应的协议号（ICMP:1、TCP:6、UDP:17），不设值时默认为所有其它协议

点击 可以单独删除一条白名单列表。

64.2.3 天珣监控

配置步骤：

进入**安全联动>天珣联动>监视器**



监视器中的信息由 3 部分组成：

管理网段：由天珣策略网关代理下发给防火墙，表明哪些范围内的主机需要进行状态检查；

排除主机列表：管理网段中的某些 IP 地址不需要状态检查，允许他们通过防火墙设备。

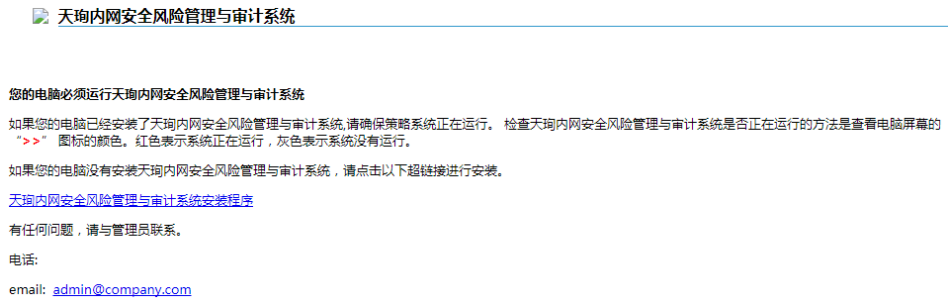
主机状态列表：列出了每个主机及对应的状态信息。

点击 可以单独删除一条主机状态列表，或者点击 删除所有的主机状态列表。

64.2.4 天珣提示安装页面

配置步骤：

进入**安全联动>天珣联动**



天珣页面是 ip 如果没有检测成功，返回给用户的一个天珣客户端下载的提示页面，管理员、电话、email 等配置均是在天珣服务器端进行配置。点击“天珣内网安全风险管理与审计系统安装程序”可以安装天珣客户端，此

超链接地址也是由天珣服务器端所填写。

如果天珣服务器配置了提示 url，则返回给用户由天珣服务器配置的自定义 url 页面。

64.3 配置案例

64.3.1 案例：允许符合安全策略的内部主机访问外网

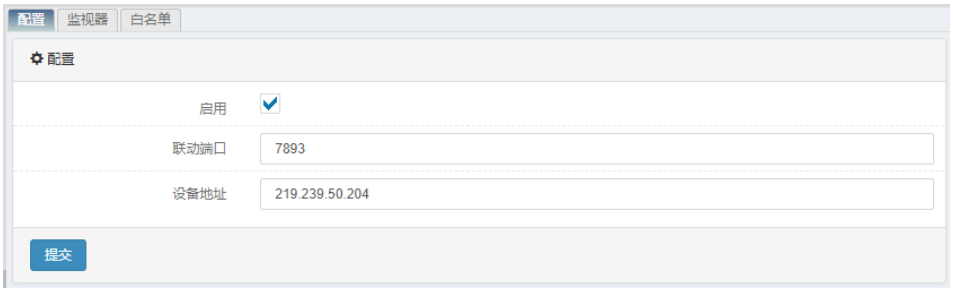
案例描述

某公司部署有天珣系统，防火墙设备作为网关。公司希望只有安装了天珣客户端软件，并且符合安全策略的内部主机，才允许通过防火墙设备访问外网。

可以通过防火墙和天珣的联动来实现。

配置步骤：

1. 进入**安全联动>天珣联动>配置**，如下图：



2. 配置完成
3. 检测结果

只有在主机状态列表中状态符合安全策略的内部主机才可以访问外网。

64.4 常见故障分析

64.4.1 常见故障：FW上没有管理网段

	FW设备上没有看到管理网段，所有的内部主机都能通过FW设备。

		有以下几个可能的原因： 1) FW上未启用天珣联动或策略网关代理的IP/Port配置不正确； 2) 天珣策略服务器或策略网关代理配置不正确； 3) FW和天珣策略网关代理之间的通信有问题。
		1) 先查看设备相关配置，保证配置正确并且和天珣策略网关代理的配置一致； 2) 使用 debug tianxun-interaction 命令，查看FW和天珣策略网关代理的交互信息；

65 第65章 漏扫联动

65.1 漏扫联动概述

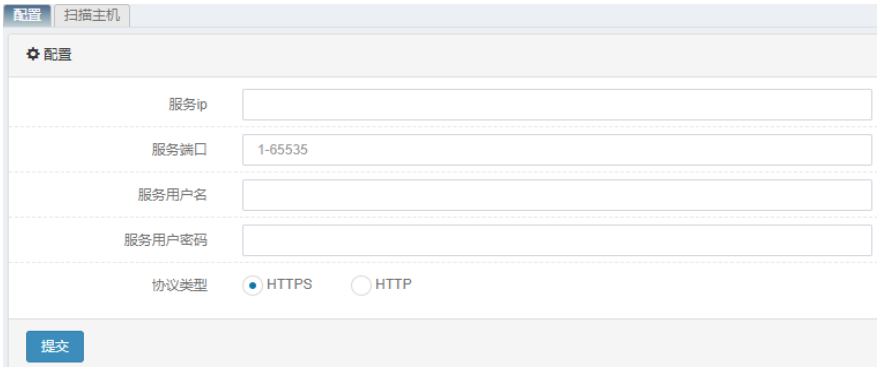
通过防火墙与漏洞扫描服务器联动，由防火墙统一对被保护的主机进行管控，通过防火墙访问网络的主机可以在防火墙威胁统计的基础上，由防火墙控制漏洞扫描服务器对威胁主机进行漏洞扫描。

防火墙同时做漏洞扫描服务器的代理，用户通过防火墙直接对关心的主机进行扫描操作。

65.2 漏扫服务器配置

65.2.1 配置漏扫服务器

进入**策略>漏扫联动>配置**，如下图：



服务 IP：漏扫服务器的 IP 地址，必选项。

服务端口：漏扫服务器的端口号，非必选项。

服务用户名：漏扫服务器的接口类型用户名，必选项。

服务用户名密码：漏扫服务器的接口类型用户对应密码，必选项。

协议类型：和漏扫服务器交互的协议类型，可选项是 https 或者 http，默认是 https。

点击**提交**提交配置


注意

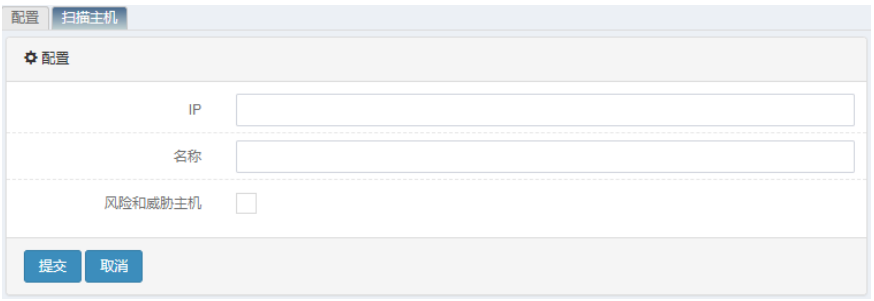
漏扫联动配置必须与漏扫服务器端开放的 ip、端口号、用户权限、用户密码、restful 协议类型完全一致，否则将与漏扫服务器端联动失败。

65.3 扫描主机配置

65.3.1 添加扫描主机

进入**策略>漏扫联动>扫描主机**，如下图：

点击**新建**添加扫描主机，如下图：



IP：要扫描的主机 IP 地址，必选项。

名称：要扫描的主机名称，非必选项。

风险和威胁主机：要扫描的主机是否是风险/威胁主机

点击**提交**添加扫描主机

65.3.2 管理扫描主机

进入**策略>漏扫联动>扫描主机**，进入扫描主机列表，如下图：

点击**刷新进度**，刷新被扫描主机的状态、扫描进度

点击▶按钮，开始请求漏扫服务器对主机进行扫描

点击按钮，下载主机的 PDF 扫描结果文件

点击按钮，删除扫描主机

对已完成漏洞扫描的主机进行重新扫描，将会删除上次的扫描结果。

66 第66章 流量控制策略

66.1 流量控制概述

随着网络技术的快速发展，基于网络的应用越来越多、越来越复杂。种类繁多的应用正在吞噬着越来越多的网络资源. 网络中的流量急剧上升，造成了网络阻塞，带宽利用率下降。

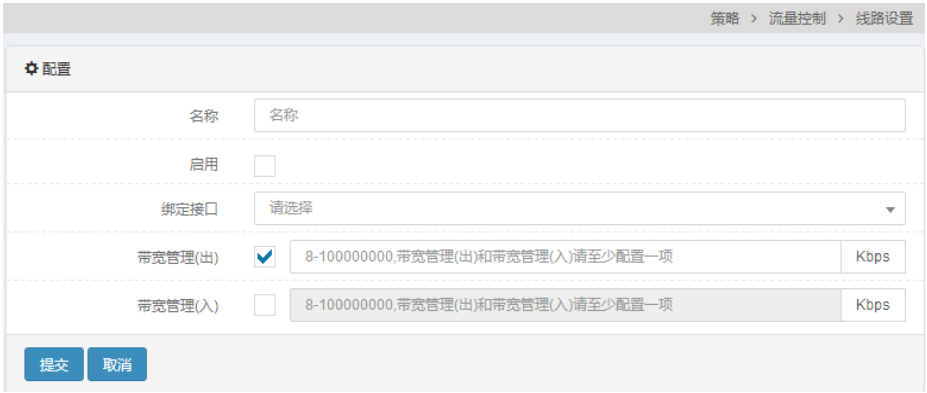
流量控制可以对数据流进行分类，利用类别和子类别的包含关系可以实现灵活的带宽共享和独占模式。带宽保障，满足关键业务与重要员工的带宽保障需求，动态保障这些业务与员工所需的带宽，在其需要使用网络时得到带宽的保障，优先使用网络，在其空闲的时候，带宽可以被其他业务或者员工使用。在不增加带宽的前提下，提升被保障业务与员工访问互联网的质量与速度。带宽控制，指定主机或服务预留带宽、限制最高带宽，也能实现平均分配带宽，并进行优先级管理，有效提高带宽利用率并提高用户体验。

66.2 配置线路策略

66.2.1 配置线路策略

配置步骤：

1. 进入**策略>流量控制>线路设置**，点击**新建**。



名称：线路策略的名称。

启用：是否启用该线路，只有启用的情况下，该线路策略才会参与调度。

绑定接口：指定线路策略匹配接口，只有从该接口进入或者发出的报文，才会匹配到这条线路策略。

带宽管理（出）：设定匹配该策略的流量出方向的最大带宽限制，范围为 8-100000000Kbps。

带宽管理（入）：设定匹配该策略的流量入方向的最大带宽限制，范围为 8-100000000Kbps。

2. 配置完毕后，点击**提交**。


注意

1、出和入方向至少配置一个方向。
2、一个接口只能被一条线路策略绑定。
3、新建一条线路策略，会生成一条默认管道策略。
4、如果带宽不配置，系统会设置成默认值（10000000kbps）。

66.2.2 编辑线路策略

配置步骤：

1. 进入**策略>流量控制>线路设置**，对某条存在的线路策略点击线路名策略称进入编辑界面。

2. 可以对线路策略里面的内容进行编辑修改，修改完毕后点击**提交**。

66.2.3 删除线路策略

配置步骤：

1. 进入**策略>流量控制>线路设置**，如下图：

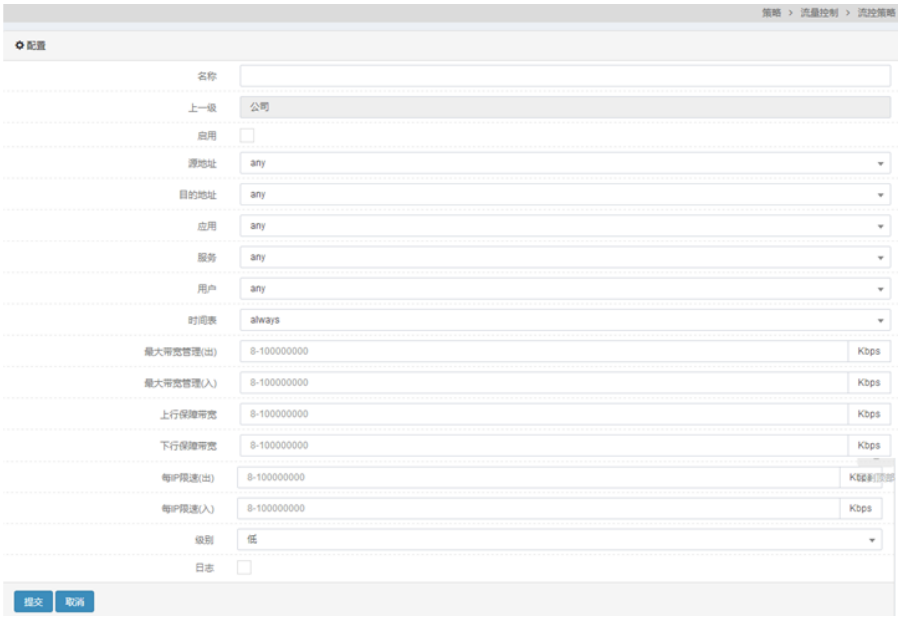
2. 点击 ✖ 删除策略。

66.3 配置管道策略

66.3.1 配置管道策略

配置步骤：

1. 进入**策略>流量控制>流控策略**，选中一条线路策略，点击**新建**。



名称：管道策略的名称。

上一级：该管道策略的父策略。

启用：是否启用该策略，只有启用的情况下，该策略才能够被调度。

源地址：数据流的源地址，可以引用已定义的某个地址对象或地址对象组，any 表示源地址为任意。

目的地址：数据流的目的地址，可以引用已定义的某个地址对象或地址对象组，any 表示目的地址为任意。

应用：数据流的应用属性，可以引用已定义的某个应用对象或应用对象组，

any 表示应用为任意。

服务：数据流的服务属性，包括协议、源端口和目的端口，可以引用系统预定义服务、自定义的服务对象或服务对象组，any 表示服务为任意。

用户：数据流的用户属性，可以引用用户对象或用户对象组，any 表示用户为任意。

时间表：策略生效的时间，可以引用已配置的时间对象，always 表示所有时间。

最大带宽管理（出）：设定匹配该策略的流量出方向的最大带宽限制，范围为 8-100000000Kbps。

最大带宽管理（入）：设定匹配该策略的流量入方向的最大带宽限制，范围为 8-100000000Kbps。

上行保证带宽：设定匹配该策略的流量出方向的保证带宽，范围为 8-100000000Kbps。

下行保证带宽：设定匹配该策略的流量入方向的保证带宽，范围为 8-100000000Kbps。

每 ip 限速（出）：设定匹配该策略的每个主机的出方向流量的最大带宽（以 IP 作为不同主机的区分），范围为 8-100000000Kbps。

每 ip 限速（入）：设定匹配该策略的每个主机的入方向流量的最大带宽（以 IP 作为不同主机的区分），范围为 8-100000000Kbps。

优先级：指定符合该策略匹配条件的流量的优先级，优先级分为高、中、低，缺省设置为低。

日志：是否开启 qos 日志。

2. 配置完毕后，点击**提交**


注意

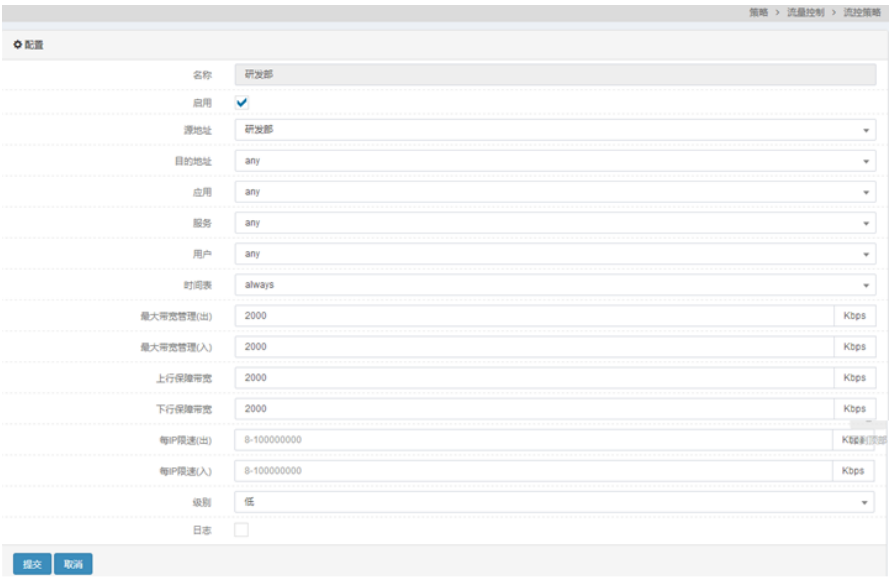
1. 新建一条管道策略时，必须先选中一条父策略，在父策略的基础上，新建子策略。
2. 配置带宽时，子策略的最大带宽和保证带宽不能大于父策略的最大带宽和保证带宽；自身的保证带宽不能大于最大带宽。
3. 最多可以配置 32 条线路策略，256 条管道策略（不包括默认策略）。
4. 每条线路策略下最多支持 4 级管道策略。
5. 管道策略勾选启用选项，但不一定参与调度，只有它的父策略及以上的策略都启用的时候，才会参与调度。
6. 出和入方向指接口的出和入方向。

66.3.2 编辑管道策略

配置步骤：

1. 进入**策略>流量控制>流控策略**，对某条存在的管道策略，点击，进入编辑界面。

2. 可以对管道策略里面的内容进行编辑修改，修改完毕后点击**提交**。



66.3.3 删除管道策略

1. 进入**策略>流量控制>流控策略**，如下图：

2. 点击 ✖，删除管道策略。

注意

1、默认管道策略不可以被删除。

2、删除一条管道策略，它以及它以下的策略都会被删除。

66.3.4 移动管道策略

通过移动策略可以调整策略的顺序，从而使位置在前的策略优先匹配。

1. 进入**策略>流量控制>流控策略**，如下图：

2. 选中一条策略，点击 上移 或者 下移 。

注意

1、只有同级的管道策略之间才可以移动顺序。

2、默认管道策略不能被移动。

66.4 流量监控

进入**策略>流量控制>流控监控**，可以查看流量控制的结果，如下图：

点 ，刷新统计结果。

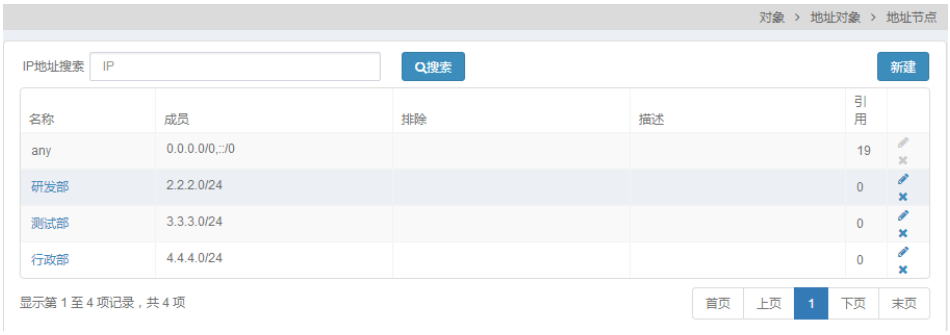
66.5 配置案例

案例描述：

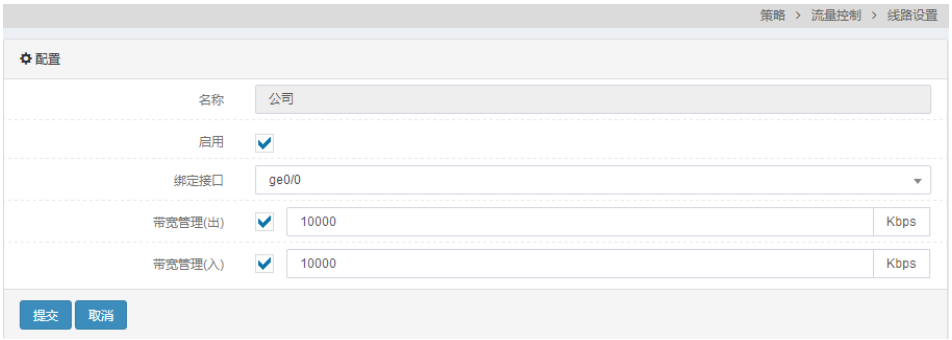
一个公司，共有 10M 带宽，都通过网卡 eth0 连接到 internet，现在想给各个部门分配一定的带宽：研发-2M，测试-5M，行政-3M，在部门内部，为了保障关键应用的稳定运行，确保重要员工顺畅地使用网络，限制与工作无关的流量，防止对带宽的滥用，又根据业务类型对流量进行限制和保证，在研发部，聊天限制为 0.5M，给邮件保证 1 M，下载限制为 0.5 M。

配置步骤：

1. 进入**对象>地址对象>地址节点**，配置地址对象“研发部”，”测试部”，”行政部”，如下图：



2. 进入**策略>流量控制>线路设置，**点击**新建，**输入参数，如下图：



3. 进入**策略>流量控制>流控策略，**在线路策略”公司”下，配置流控策略

“研发部”，”测试部”，”行政部”，如下图：

4. 进入**策略>流量控制>流控策略**，在流控策略”研发部”下，配置流控策略“下载”，”聊天”，”邮件”，如下图：

5. 配置完成，可以进入**策略>流量控制>流控监控**，查看流控效果。

67 第67章 会话控制策略

67.1 会话控制策略概述

为了对数据流进行会话控制，T 系列防火墙引入了会话控制策略的概念。

用户可以针对连接会话，进行新建或者并发的控制，从而保护连接表不被攻击填满，并且能够在一定程度上限制一些服务或应用的带宽。

会话控制支持根据入接口、源地址、目的地址、时间、服务或应用的组合去进行控制。会话控制功能包括了源主机连接限制、源主机连接速率限制、目的主机连接限制、目的主机连接速率限制、总连接限制和总连接速率限制六种限制方式。

通过配置会话控制策略可以对经过设备的数据流进行有效的控制。当设备收到数据报文时，把该报文的源地址、目的地址、服务等信息和用户配置的会话控制策略匹配，决定是否对这条数据流进行限制，并且把这条流和匹配的会话控制策略关联起来，从而确定如何处理该流的后续报文。

会话控制策略按 IPv4 或 IPv6 从上往下匹配的原则，只对通过 T 系列防火墙的数据包进行处理，对于设备本身发出的数据包不进行限制。

67.2 配置会话控制策略

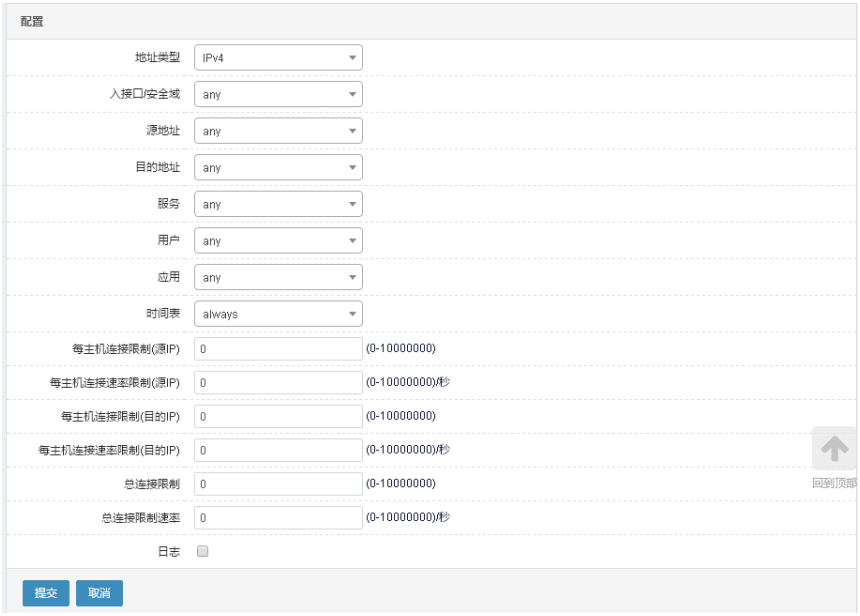
67.2.1 配置策略的基本要素

会话控制策略有两个基本要素分别是匹配条件部分和会话限制部分。匹配条件部分包括数据流的入接口、源地址、目的地址、服务、应用和策略生效的时间范围。其中，数据流的入接口、源地址、目的地址、服务、应用和时间范围都可以直接引用已定义的对象。

会话控制策略的限制有源主机连接限制、源主机连接速率限制、目的主机连接限制、目的主机连接速率限制、总连接限制和总连接速率限制六种可配置的限制方式。

配置步骤：

1. 进入**策略>会话控制**，点击新建。



参数说明：

地址类型：会话控制策略分为 IPv4 和 IPv6 两种类型，数据包匹配相应协议类型的会话控制策略。

入接口：数据流的流入方向，可以指定某个特定接口，any 表示所有接口。

源地址：数据流的源地址，可以引用已定义的某个地址对象或地址对象组，any 表示源地址为任意。

目的地址：数据流的目的地址，可以引用已定义的某个地址对象或地址对象组，any 表示目的地址为任意。

服务：数据流的服务属性，包括协议、源端口和目的端口，可以引用系统预定义服务、自定义的服务对象或服务对象组，any 表示服务为任意。

用户：数据流的用户属性，可以引用已定义的某个用户对象或 用户组，any 表示用户为任意。

应用：数据流的应用属性，引用系统预定义应用，any 表示应用为任意。

时间表：策略生效的时间，可以引用已配置的时间对象，always 表示所有时间。

每主机连接限制（源 IP）：对匹配该条策略的流，根据源地址连接数进行限制，配置为 0 表示不限制。

每主机连接速率限制（源 IP）：对匹配该策略的流，根据源地址连接速率进行限制，配置为 0 表示不限制。

每主机连接限制(目的 IP）：对匹配该条策略的流，根据目的地址连接数进行限制，配置为 0 表示不限制。

每主机连接速率限制（目的 IP）：对匹配该策略的流，根据目的地址连接速率进行限制，配置为 0 表示不限制。

总连接控制：对匹配该条策略的流，根据总连接数进行限制，配置为 0 表示不限制。

总连接速率限制：对匹配该策略的流，根据总连接速率进行限制，配置为‘0’表示不限制。

日志：选中此复选框启用日志功能，匹配该会话控制策略的数据流被阻断的信息会被发往 syslog 服务器或者产生设备本地日志，日志的优先级为信息级别。

2. 配置完毕后，点击**提交**。

入接口不能引用被 trunk 引用的接口。

1，创建一条新的会话控制策略时，必须引用相同协议类型的地址对象。

2，系统会自动生成该策略的 ID 号，策略 ID 是会话控制策略的唯一标识。不同协议类型的会话控制策略的 ID 是相互独立的。

67.2.2 启用会话控制策略

配置好的会话控制策略必须启用才能使其生效。

配置步骤：

1. 进入**策略>会话控制**，如下图：

2. 勾选**启用**可以启用一条策略。

策略缺省为不启用，配置后必须手工启用才能使其生效。

67.2.3 编辑会话控制策略

配置步骤：

1. 进入**策略>会话控制**，对于某条存在的会话控制策略，点击策略 ID 号进入编辑界面。
2. 可以对会话控制策略里面的内容进行编辑修改，修改完毕后点击**更新**。

注意

编辑策略时，地址类型不能改变。

67.2.4 删除会话控制策略

配置步骤：

1. 进入**策略>会话控制**，如下图：

2. 点击删除策略。

67.2.5 调整会话控制策略的顺序

通过移动策略可以调整会话控制策略的顺序，从而使位置在前的策略优先匹配。

配置步骤：

1. 进入**策略>会话控制**，如下图：

2. 点击移动策略。

策略 ID：需要被移动的策略的 ID 号。

移动到（策略 ID）：参考策略的 ID 号。

之前：移动策略到参考策略之前。

之后：移动策略到参考策略之后。

3. 点击**提交**。

只有相同协议类型的策略，才能调整顺序。

67.2.6 查询会话控制策略

查询步骤：

1. 进入**策略>会话控制**，如下图：

2. 在下拉框中分别选择**源地址**、**目的地址**和**服务**，点击**搜索**查询配置中与关键字相符的所有会话控制策略。

67.3 会话控制策略监控与维护

67.3.1 查看会话控制策略

进入**策略>会话控制**，可以根据协议类型查看已经配置的会话控制策略。

67.4 配置案例

67.4.1 案例1：创建IPv4会话控制策略限制总连接速率

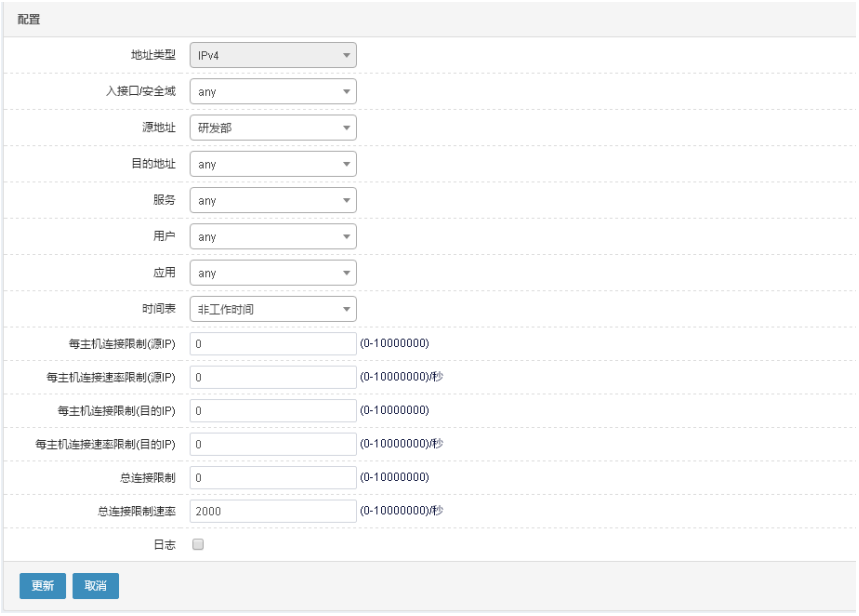
通过设备访问外网，对研发部某一时间段的会话进行总连接速率的限制。

配置步骤：

1. 进入**对象>地址对象>地址节点**，配置地址对象“研发部”，如下图：

2. 进入**对象>时间对象>绝对时间**，配置时间对象“非工作时间”，如下图：

4. 进入**策略>会话控制**，点击**新建**，输入参数，如下图：



5. 点击**提交**。

6. 进入**策略>会话控制**，如下图：

7. 勾选**启用**完成设置。

67.5 常见故障分析

67.5.1 故障现象：匹配上某条策略的某些数据流没有受到相应的限制

现象	匹配上某条策略的数据流没有受到相应的限制。
分析	有可能是以下几种情况导致该策略无法生效： ➢ 该策略没有启用，请检查策略状态是否为启用； ➢ 由于策略在IPv4或IPv6有相同入接口时按从上往下的原则进行匹配，数据流可能匹配到前面的某条策略，请检查配置是否冲突。
解决	启用该策略，如果和其他策略的配置冲突，可以根据需求修改策略或者改变策略的顺序。

68 第68章 Web 认证策略

68.1 Web认证策略概述

配置 Web 认证策略前需要先配置认证用户组和认证服务器。配置认证用户时，既可以选择配置单个用户，也可以选择配置用户组。但是在 Web 认证策略中只能配置用户组。Web 认证策略将过滤掉没有经过认证的用户报文，对应经通过认证的报文进行转发。

68.2 配置Web认证策略

68.2.1 配置用户

在配置用户时，既可以选择配置认证用户也可以选择配置静态绑定用户。

选择配置认证用户的步骤：

3. 进入**对象>用户对象>用户**，点击**新建。**

参数说明：

用户名：用户名称。

启用：是否启用该用户对象。

类型：用户类型可以是认证用户或者静态绑定。

认证用户：若类型选择的是认证用户则需要配置服务器类型，有三种类型选项：

LOCAL：本地认证。可以把用户名添加到天清汉马 T 系列防火墙用户数据库中，然后为用户设置一个密码以允许用户使用这个内部数据库进行认证。

RADIUS：服务器认证。可以添加一个 RADIUS 服务器并且选择 RADIUS，以允许用户使用选定的 RADIUS 服务器进行认证。

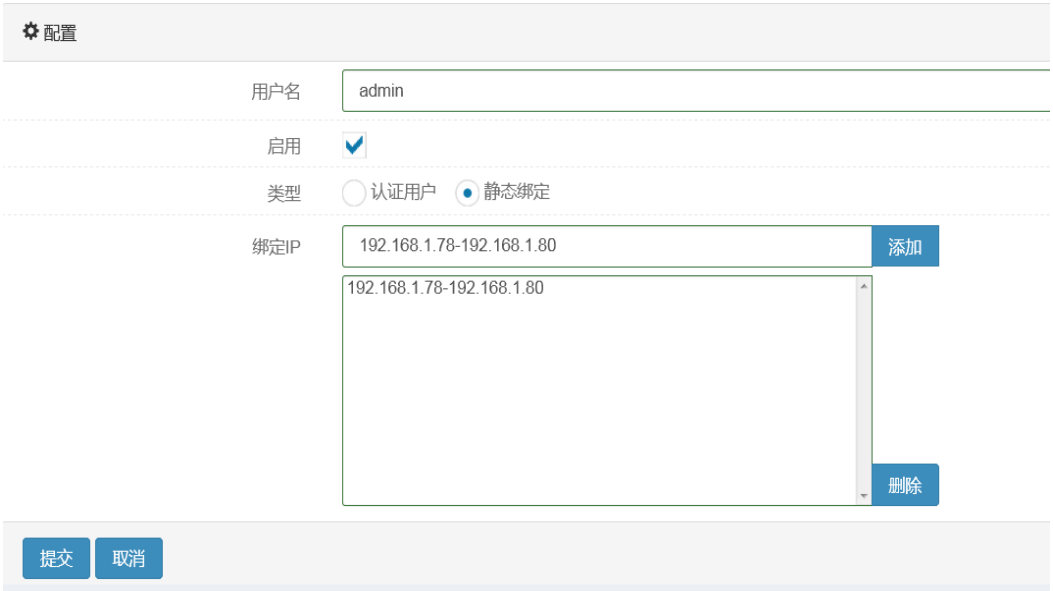
LDAP：服务器认证。可以添加一个 LDAP 服务器并且选择 LDAP，以允许用户使用选定的 LDAP 服务器进行认证。

密码：该用户名对应的密码。

确认密码：在输入一遍密码，以便确认密码是否输入错误。

选择配置静态绑定用户的步骤：

4. 进入**对象>用户对象>用户**，点击**新建。**



参数说明：

用户名：用户名称。

启用：是否启用该用户对象。

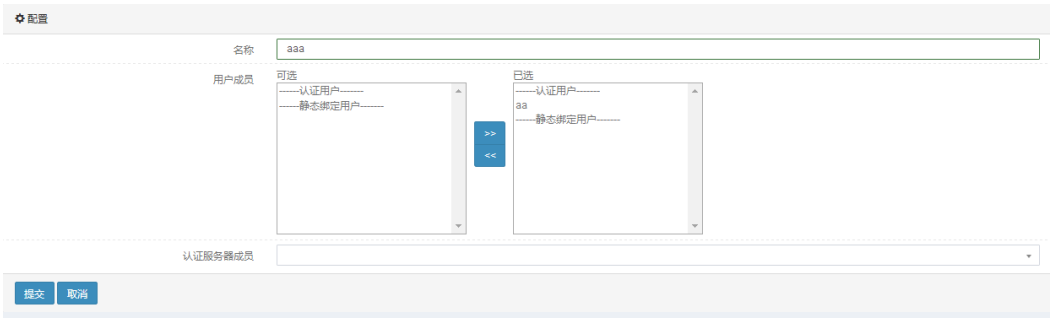
类型：用户类型可以是认证用户或者静态绑定。

绑定 IP：可以选择绑定单个 IP，也可以选择绑定一个 IP 段。

5. 点击**提交**，完成对用户对象的配置，显示如下页面：

68.2.2 配置用户组

1. 进入**对象>用户对象>用户组**，点击**新建**。



参数说明：

用户名：用户组名称。

描述：对该用户组的描述信息。

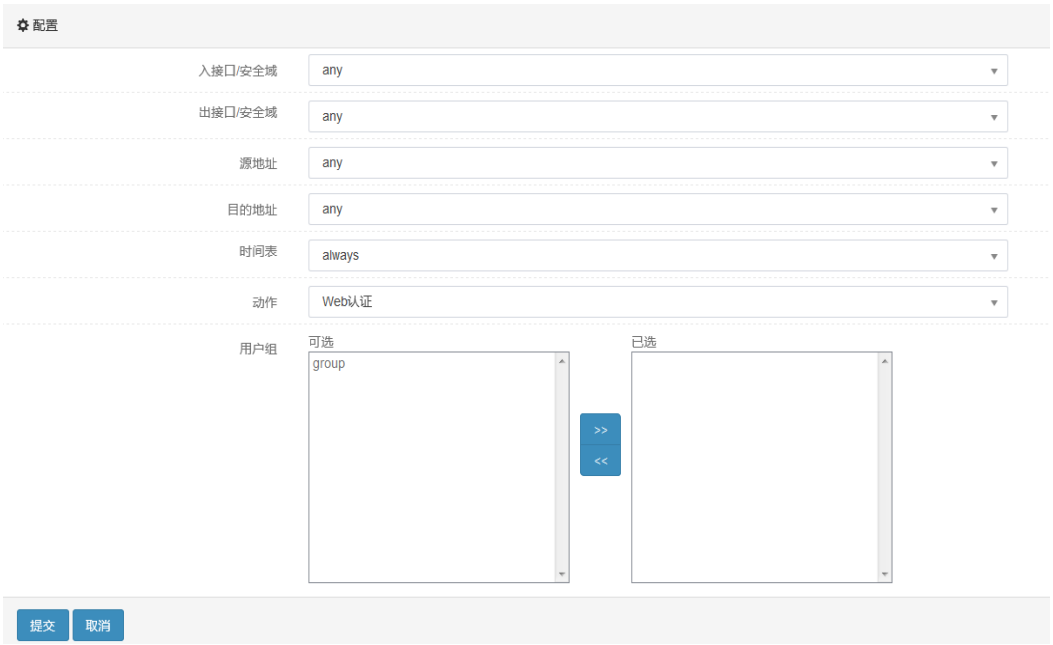
成员：在已存在的用户进行选择，组成用户组。

认证服务器成员：可选择认证服务器，默认本地认证。

2. 点击**提交**，完成对用户组的配置，显示如下页面：

68.2.3 配置Web认证策略

1. 进入**策略>Web 认证>策略**，点击**新建**。



参数说明：

入接口/安全域：数据流的流入方向，可以指定某个特定接口，any 表示所有接口。

出接口/安全域：数据流的流出方向，可以指定某个特定接口，any 表示所有接口。

源地址：数据流的源地址，可以引用已定义的某个地址对象或地址对象组，any 表示源地址为任意。

目的地址：数据流的目的地址，可以引用已定义的某个地址对象或地址对象组，any 表示目的地址为任意。

时间表：策略生效的时间，可以引用已配置的时间对象，always 表示所有时间。

动作：该策略的动作类型。有两种类型可以选择：Web 认证、允许。

用户组：用户组对象，可以引用已定义的某些用户组对象。

注意

当动作选择的是 Web 认证时，用户组不能为空。

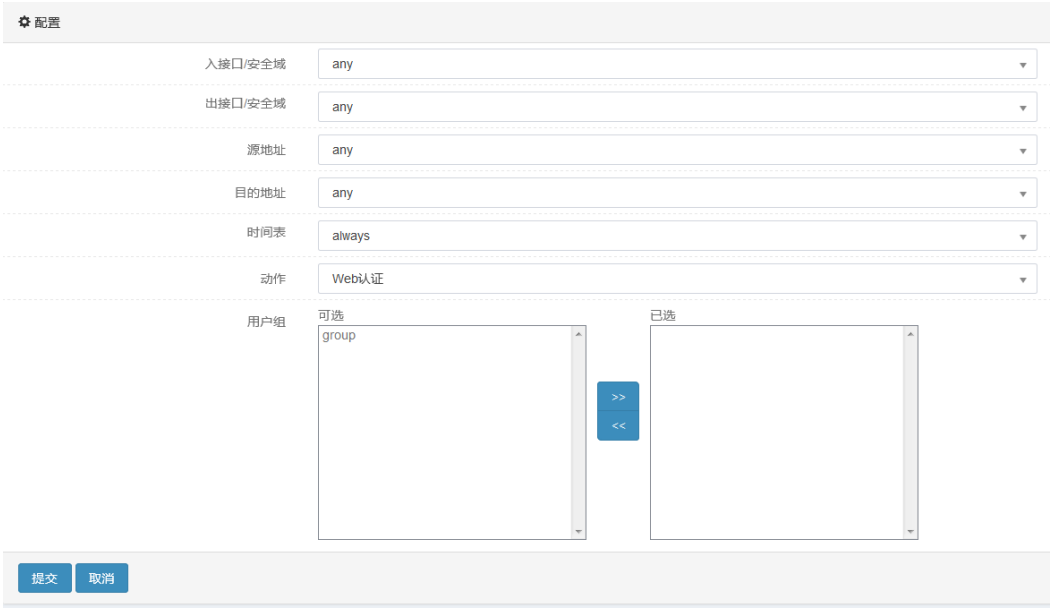
2.点击**提交**，完成对 web 认证策略的配置，显示如下页面：

68.2.4 编辑Web认证策略

已经创建的 Web 认证策略可以编辑修改。

1.进入**策略>Web 认证>策略**，如下图：

2.单击需要修改的 Web 认证策略**序号**，进行修改编辑。



可以对该 web 认证策略进行配置修改。

3.点击**提交**完成修改的配置。

68.2.5 删除Web认证策略

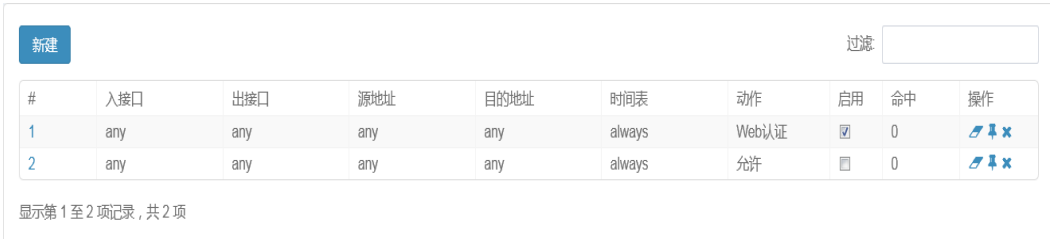
1.进入**策略>Web 认证>策略**，如下图：

2.选择需要删除的攻击防护，点击 ✖ 进行删除。

3.点击**确定**，完成 Web 认证策略的删除。

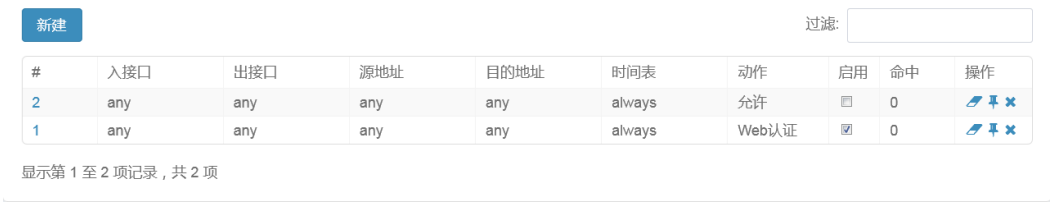
68.2.6 移动Web认证策略

1. 进入**策略>Web 认证>策略**，如下图：



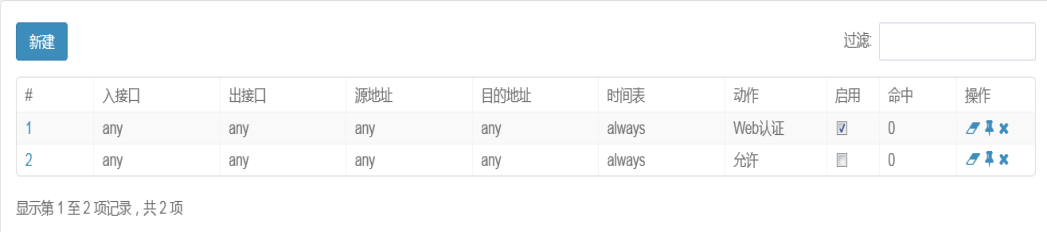
2. 选择需要移动的 Web 认证策略，点击 。

3. 点击提交，显示移动成功。

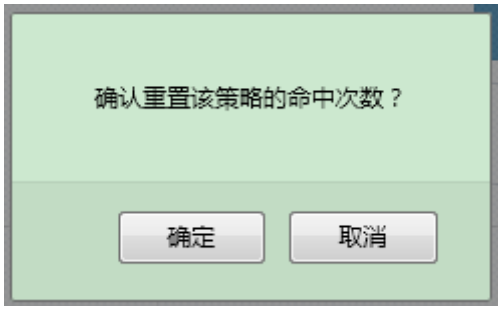


68.2.7 Web认证策略命中次数清零

1. 进入**策略>Web 认证>策略**，如下图：



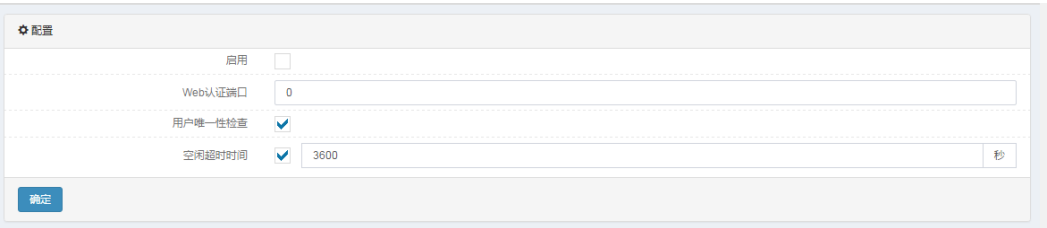
2. 选择需要移动的 Web 认证策略，点击 。



3. 点击确定。

68.2.8 修改Web认证配置

1. 进入**策略>Web 认证>配置**，如下图：



参数说明：

启用：是否开启 portal 认证页面。默认不开启。

Web 认证端口：认证服务的侦听的端口，默认为 0。

用户唯一性检查：勾选之后，不能多人使用同一个账号登陆。

空闲超时时间：若用户在空闲超时时间内没有流量产生，则会被强制下线。默认为 3600 秒。

2. 修改之后点击**确定**。

68.2.9 清除所有在线用户

1. 进入**策略>Web 认证>在线信息**，如下图：

2. 点击 清空所有，清除所有在线用户。

3. 点击 ，进行刷新。

68.3 配置案例

68.3.1 配置案例： 配置员工上网需要ladp认证

案例描述：要求所有员工在通过设备访问外网时，需要到 ldap 服务器上进行认证，配置认证策略已达到上述要求。外网口为 ge1/3，ldap 服务器地址为 11.11.11.2/24。

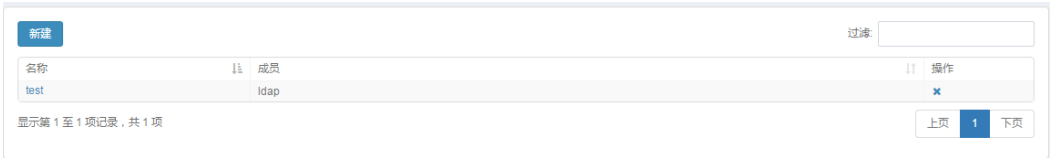
配置步骤：

步骤 1：配置 ldap 服务器：

进入 **对象 >> 认证服务器 >> LDAP** 节点下，配置 ldap 服务器

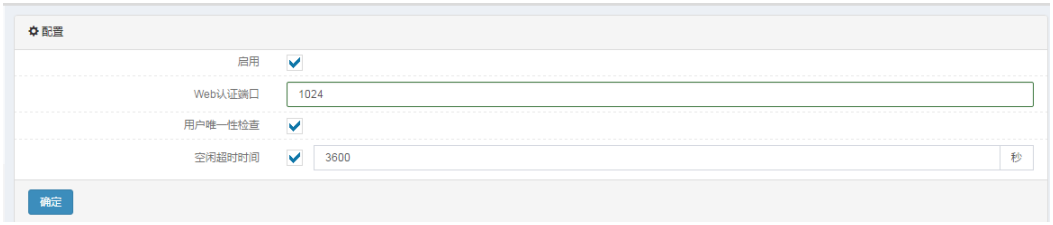
步骤 2：配置用户组，并引用 ldap 服务器

进入 **对象 >> 用户对象 >> 用户组** 节点下，新增用户组 test



步骤 3：开启 web 认证功能

进入 **策略 >> web 认证 >> 配置** 节点下，开启 web 认证功能



注意

开启用户唯一性检查后，不能多人使用同一个账号登录，一个用户名只对应一个 IP 地址

步骤 4：配置 web 认证策略

进入 **策略 >> web 认证 >> 策略** 节点下，配置 web 认证策略

步骤 5：勾选**启用**完成设置

68.4 常见故障分析

68.4.1 故障现象：认证用户进行认证时失败

现象	认证用户进行认证时失败。
分析	（1） 密码错误 （2） 用户已经禁用 （3） 本地不保存用户名的认证用户认证时所在的组没有加入RADIUS服务器 （4） RADIUS/LDAP服务器配置错误（比如：共享密钥，IP等） （5） RADIUS/LDAP服务器连接不上（比如：PING不通） （6） RADIUS/LDAP服务器上没有这个用户
解决	（1） 检查用户密码，输入正确的用户名和密码 （2） 解禁用户 （3） 为该用户认证时所在的组添加RADIUS/LDAP服务器 （4） 修改该RADIUS/LDAP服务器的配置 （5） 首先确保天清汉马USG和RADIUS/LDAP服务器能通讯，能PING通

（6） 为该RADIUS/LDAP服务器添加该用户

69 第69章 地址对象

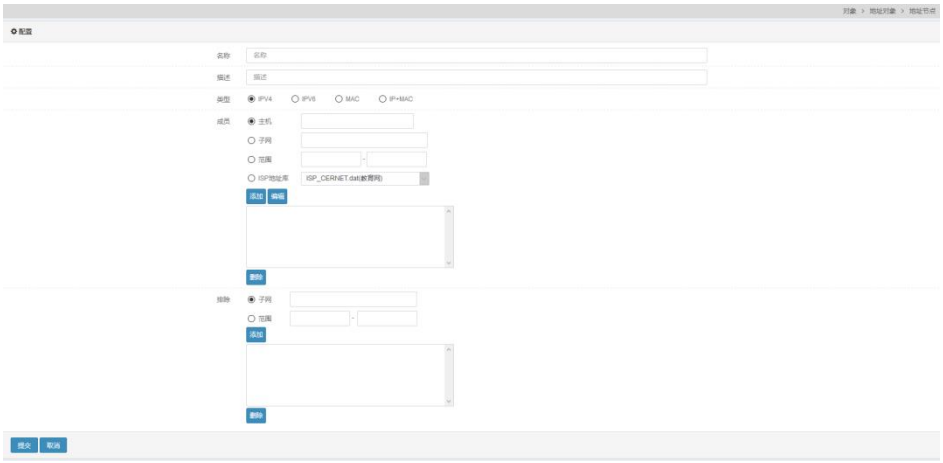
69.1 地址对象概述

为了方便用户的配置和管理，防火墙中引入了地址对象的概念。地址对象分为地址节点、地址组和域名地址，地址组是地址节点和域名地址的集合。在其它功能的配置中（如防火墙策略、NAT 规则，路由策略），可以引用地址对象来定义配置生效的条件。

69.2 配置地址节点

地址节点分为 IPv4 类型，IPv6 类型，MAC 类型以及 IP+MAC 类型。

1. 进入**对象->地址对象>地址节点**，点击**新建**，如下图：



名称：为新建地址节点设置名称，不得超过 63 个字符。

描述：对新建地址节点做描述，不得超过 127 个字符。

类型：地址节点可分为 IPv4 类型，IPv6 类型，MAC 类型以及 IP+MAC 类型。

地址节点：

成员：该地址节点中包含的成员。

IPv4 类型地址节点的内容包含：

- 主机：主机 IPv4 地址。
- 子网： IPv4 网段地址。
- 范围： IPv4 地址池范围。

- IPv4 的 ISP 地址库。

IPv6 类型地址节点的内容包括：

- 主机：主机 IPv6 地址。
- 子网：IPv6 网络地址。
- 范围：IPv6 地址范围。

MAC 类型的地址节点内容包括：

- MAC 地址。

IP+MAC 类型的地址节点内容包括：

- IPv4 地址和 MAC 地址的组合。

编辑：IPv4 类型地址节点可以批量复制粘贴主机地址进行成员新建。

排除：该地址节点中排除的成员。

IPv4 类型地址节点：

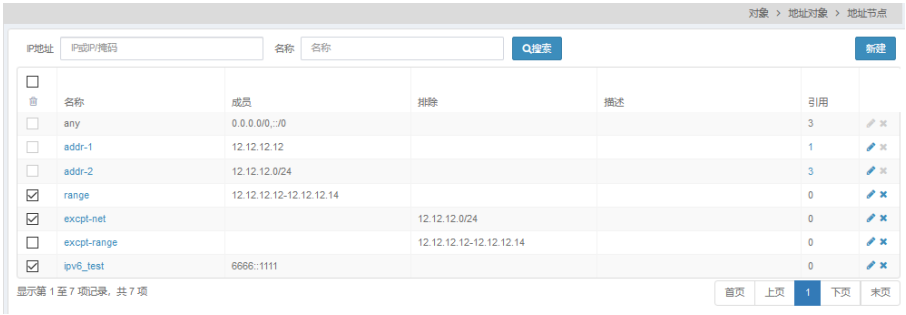
- 子网： IPv4 网段地址。
- 范围： IPv4 地址范围。

2. 点击**提交**。

69.3 批量删除地址节点

可对未被引用的地址节点进行批量删除操作。

1. 进入**对象->地址对象->地址节点**，在地址节点首列选中可勾选所要批量删除的地址节点，如下图：



2. 点击 ，批量删除完成。

69.4 配置地址组

地址组是地址节点的集合，可以使用地址组方便的管理和地址相关的规则。

配置步骤：

1. 进入**对象->地址对象->地址组**，点击新建，如下图：

名称：为新建地址组设置名称，不得超过 63 个字符。

描述：对新建地址组做描述，不得超过 127 个字符。

可选成员：已经定义好的地址节点和地址组信息。

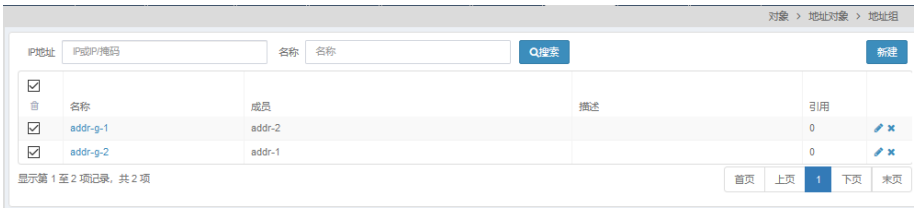
已选成员：已经选中的地址组成员。

2. 点击**提交**。

69.5 批量删除地址组

可对未被引用的地址组进行批量删除操作。

1. 进入**对象->地址对象->地址组**，在地址组首列选中可勾选所要批量删除的地址组，如下图：



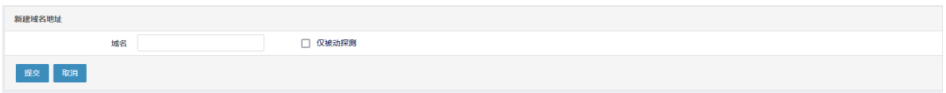
2. 点击 ，批量删除完成。

69.6 配置域名地址

域名地址是一种特殊的地址组，地址组名称定义为域名地址，地址组成员是由配置域名解析到的 IP 地址集合，解析分为主动探测及被动探测两种解析方式。

配置步骤：

1. 进入**对象->地址对象->域名地址**，点击新建，如下图：



域名：设置需要解析的域名，不得超过 63 个字符。

仅被动探测：域名地址解析默认为主动+被动探测方式解析。主动探测解析方式为获取系统从 DNS 服务器解析到的 IP 地址。可勾选改选项将解析方式设置为仅被动探测，即仅对流经设备的 dns 请求的回复报文中所含域名

与域名地址域名名称对比，决定是否将回复报文中的 IP 地址添加至解析成员中。

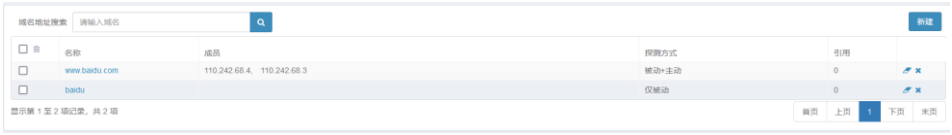
域名地址相关规格：

域名地址对象数量规格 2000 个；

单个域名地址对象解析成员数量规格 500 个；

全部域名地址对象解析生成总成员数量规格 50000 个；

2. 点击**提交**，如下图：



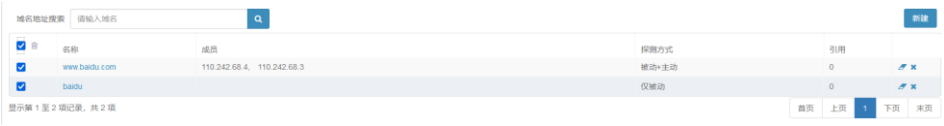
注意

主动探测解析方式须在系统->配置->DNS 中，配置好 DNS 服务器，域名地址才能解析到对应的 IP 地址，自动添加为该域名地址对象的成员。

69.7 批量删除域名地址

可对未被引用的域名地址进行批量删除操作。

1. 进入**对象->地址对象->域名地址**，在域名地址首列选中可勾选所要批量删除的域名地址，如下图：

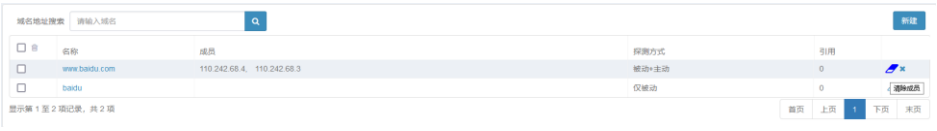


2. 点击 ，批量删除完成。

69.8 清除域名地址解析成员

可对指定域名地址下解析到的成员进行清除操作。

1. 进入**对象->地址对象->域名地址**，如下图：



2. 点击 ，删除对应域名地址已解析到的成员。

注意

对域名地址解析到的成员执行主动淘汰机制，即对域名地址对象在设定时间内(默认 3600 秒)没有再次解析到的成员结果，系统对该成员进行删除

69.9 配置案例

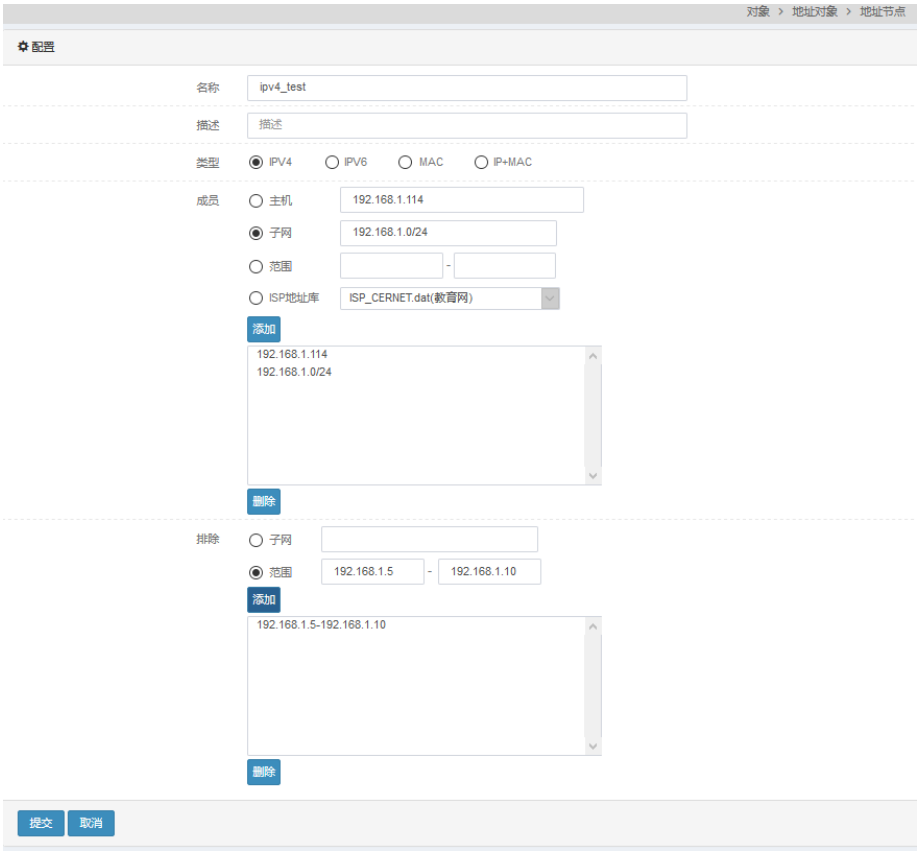
69.9.1 配置案例1：增加IPv4地址节点

案例描述

增加一个 IPv4 的地址对象，包含内网的某些网段，排除个别主机或者网段。

配置步骤：

1. 进入**对象->地址对象>地址节点**，点击**新建**，如下图：



2. 输入参数。

3. 点击 **提交** 完成设置。

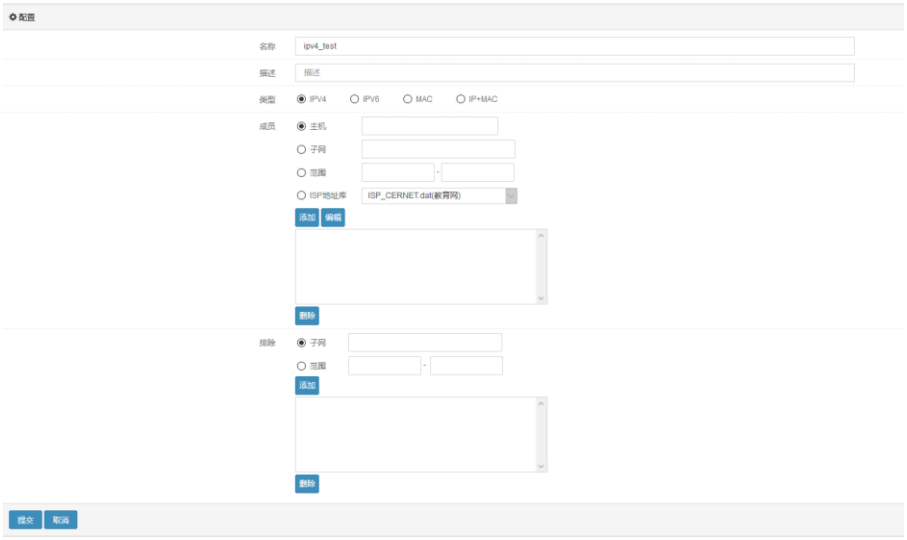
69.9.2 配置案例2：编辑增加IPv4地址节点

案例描述

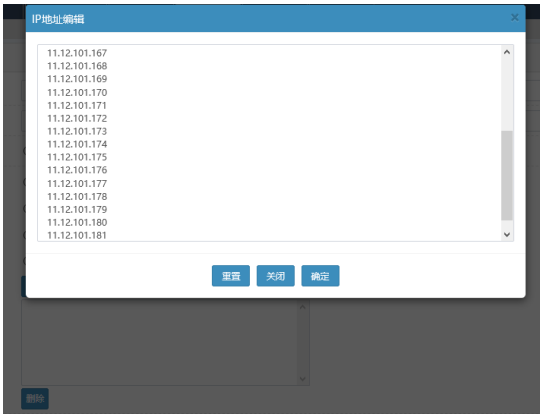
批量增加若干个 IPv4 类型的主机地址对象。

配置步骤：

1. 进入**对象->地址对象>地址节点**，点击**新建**，如下图：



2. 点击**编辑**。



3. 点击**确定**批量添加 IPv4 地址。

4. 点击**提交**完成配置。

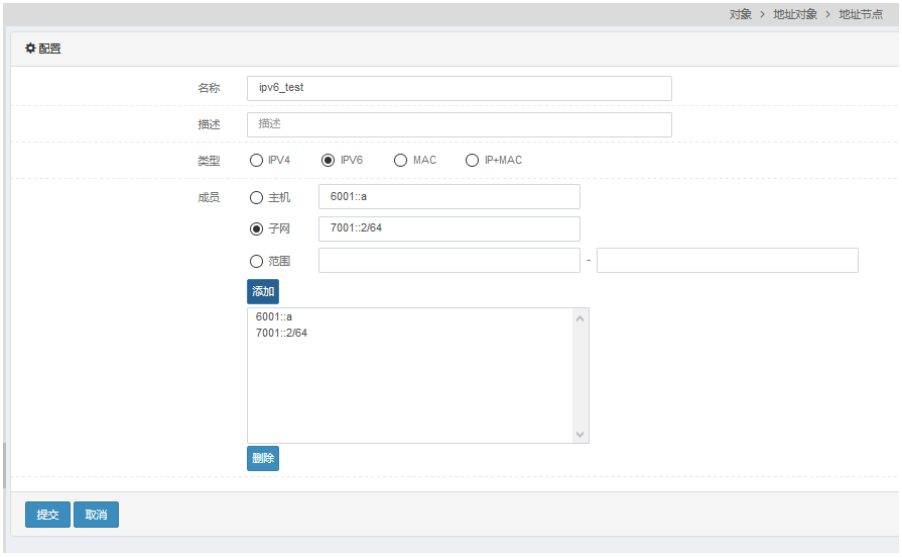
69.9.3 配置案例3：增加IPv6地址节点

案例描述

增加一个 IPv6 的地址对象，包含内网所在子网。

配置步骤：

1. 进入**对象->地址对象>地址节点**，点击**新建**，如下图：



2. 输入参数。

3. 点击**提交**完成设置。

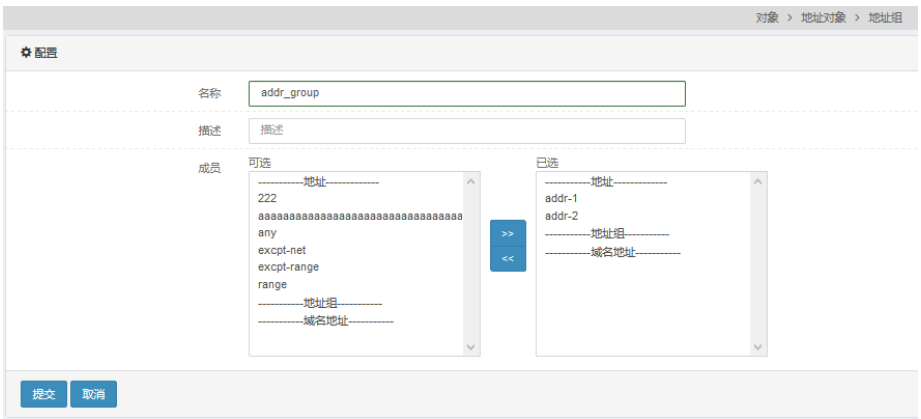
69.9.4 配置案例4：增加地址对象组

案例描述

增加地址对象到地址对象组。

配置步骤：

1. 进入**对象->地址对象>地址组**，点击**新建**，如下图：



2. 选择**可用地址和地址组**中的地址节点，点击 >> 添加到**成员**中。

3. 点击**提交**完成设置。

69.9.5 配置案例5：增加域名地址并在防火墙策略中引用

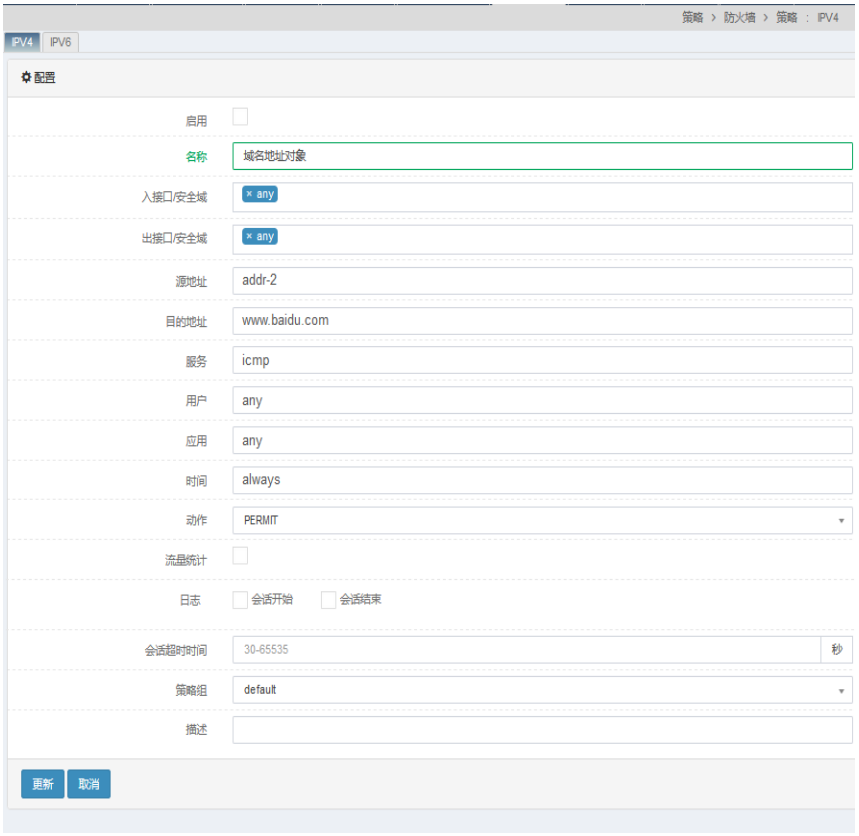
案例描述

增加一个域名地址，并查看域名地址中包含的成员，并在防火墙策略中引用这个域名地址对象。

配置步骤：

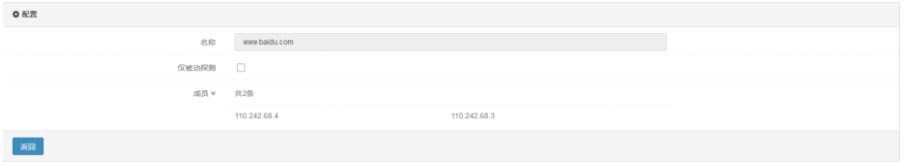
1. 进入**对象->地址对象>域名地址**，点击**新建**，如下图：

2. 在**域名**文本框中，输入需要解析的域名。
3. 点击**提交**完成设置。
4. 新建防火墙策略，目的地址为域名地址对象，如下图：



5. 查看域名地址中包含的成员。

点击要查看的域名，进入查看域名成员页面。



69.10 地址对象监控与维护

69.10.1 查看地址节点

1. 点击**对象->地址对象->地址节点**，如下图：

2. 通过 IP 或 IP 网段查找：

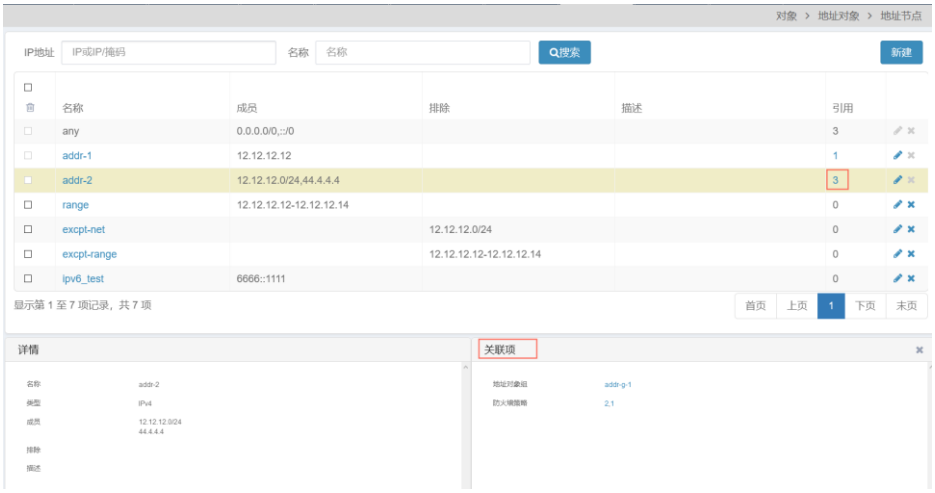
在 **IP 地址**输入 IP 或 IP/掩码后，点击 搜索 可以查看成员包含搜索 IP 的指定地址节点，如下图：

3. 通过名称查找：

在**名称**输入名称后，点击 搜索 可以查看地址对象名称包含搜索内容的指定地址节点，如下图：

4. 引用详情显示：

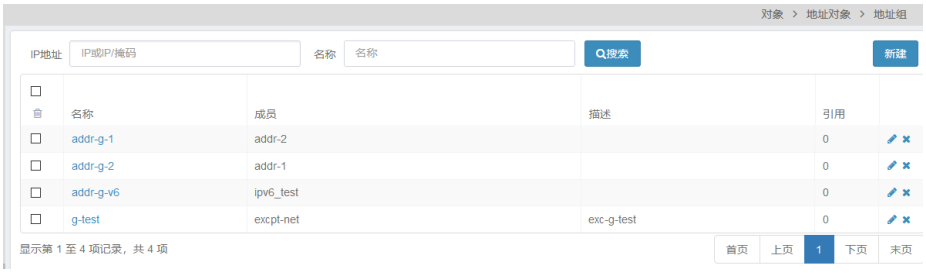
对除”any”的其他地址对象，点击非 0 引用数，可查看该地址对象被其他模块的关联项详情，如下图：



点击某个关联项，可跳转至对应模块进行解引用该地址对象编辑操作，当该地址对象引用数减少至 0 时，可对其进行删除操作。

69.10.2 查看地址组

1. 点击**对象->地址对象->地址组**，如下图：



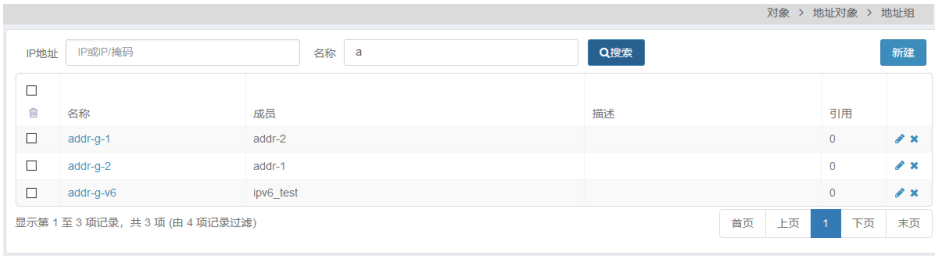
2. 通过 IP 或 IP 网段查找：

在 **IP 地址**输入 IP 或 IP/掩码后，点击 搜索 ，可以查看指定的地址组，如下图：

3. 通过名称查找：

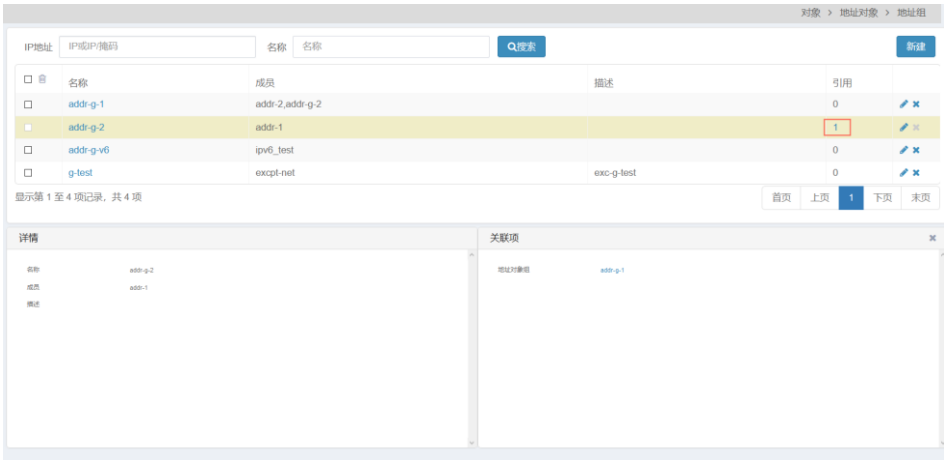
在**名称**输入名称后，点击 搜索 可以查看地址组名称包含搜索内容的指定地

址组，如下图：



4. 引用详情显示：

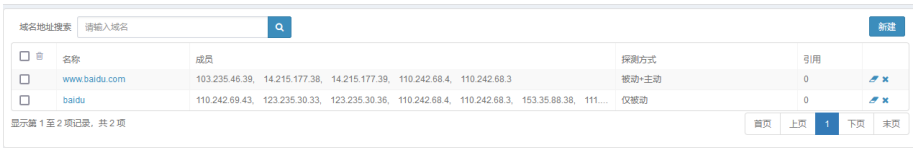
点击地址组中非 0 引用数，可查看该地址组被其他模块的关联项详情，如下图：



点击某个关联项，可跳转至对应模块进行解引用该地址组编辑操作，当该地址组引用数减少至 0 时，可对其进行删除操作。

69.10.3 查看域名地址

1. 点击**对象->地址对象->域名地址**，如下图：

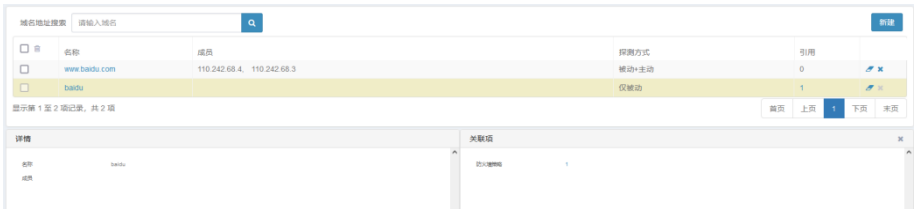


2. 名称搜索：

在**域名地址搜索**输入域名地址，可以查看指定的域名地址，如下图：

3. 引用详情显示：

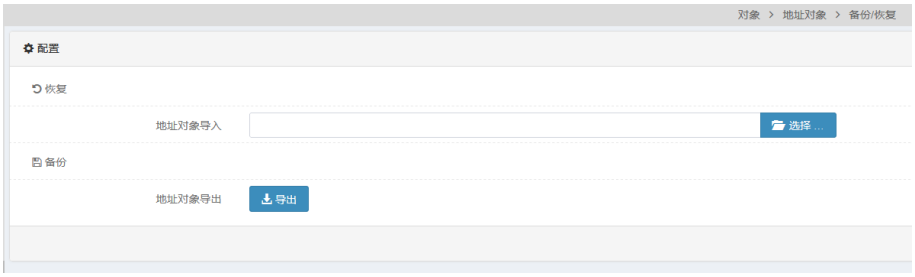
点击域名地址中非 0 引用数，可查看该域名地址对象被其他模块的关联项详情，如下图：



点击某个关联项，可跳转至对应模块进行解引用该域名地址编辑操作，当该域名地址引用数减少至 0 时，可对其进行删除操作。

69.10.4 地址对象的备份和恢复

点击**对象->地址对象>备份恢复**，如下图：



参数说明：

恢复：可导入包含地址对象配置的文本文件，系统会读取问题中的配置并执行下发。地址对象的配置格式必须如下：

- **地址对象配置文件首行**

！此行严禁修改或移除！

- **域名地址类型地址对象**

address-domain www.baidu.com

address-domain-passive baidu

- **IPv4 类型地址对象**

address NAME

host-address A.B.C.D

net-address A.B.C.D/M

range-address A.B.C.D E.F.G.H

isp-address NAME

net-address-exp A.B.C.D/M

range-address-exp A.B.C.D E.F.G.H

- **IPv6 类型地址对象**

address-v6 NAME

host-v6 X:X::X:X

net-v6 X:X::X:X/M

range-v6 X:X::X:X X:X::X:X

- **MAC 类型地址对象**

address-mac NAME

mac-host FF-FF-FF-FF-FF-FF

- **IP+MAC 类型地址对象**

address-ip-mac NAME

bind A.B.C.D FF-FF-FF-FF-FF-FF

- **地址组**

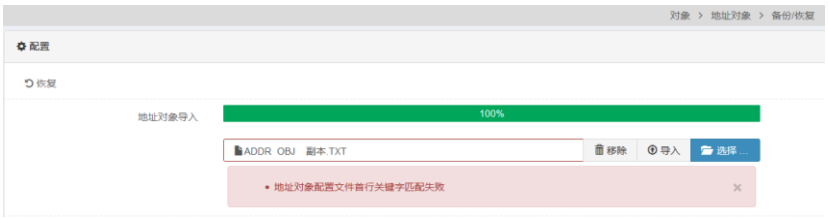
address-group NAME

address-object NAME

地址对象导入错误提示：

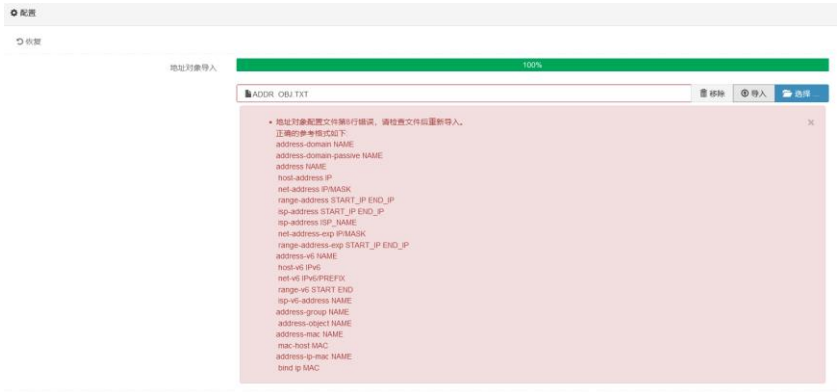
- **地址对象配置文件首行错误**

导入配置文件中未识别出正确的首行关键字，导入错误提示如下图：



- **地址对象的配置格式错误**

导入配置文件中发现地址对象的配置格式错误，提示信息显示出错行数及正确格式模板，如下图：



备份：可将地址对象的配置导出至一个文本文件中。

69.11 常见故障分析

69.11.1 故障现象：提交不成功

现象	当设置完毕后点击提交，显示提交失败。
分析	检查地址是否有效。
解决	修改为有效的地址。

69.11.2 故障现象：域名地址没有成员

现象	新建域名地址后，查看域名地址列表，成员为空。
分析	检查系统的DNS服务器是否已经配置并且能够正常访问。
解决	为系统配置有效的DNS服务器。

70 第70章 ISP 地址库

70.1 ISP地址库概述

ISP 地址库是运营商提供的公网地址的集合，该地址库可以被地址对象引用，地址对象被策略路由引用使用在出站链路负载均衡中。通过对出站流量的目的地址与 ISP 地址库的匹配，将流量引导到最合适的链路中去。

注意

1.ISP 地址库用于出站链路负载均衡的时候，不要将该地址库用于源地址对象。

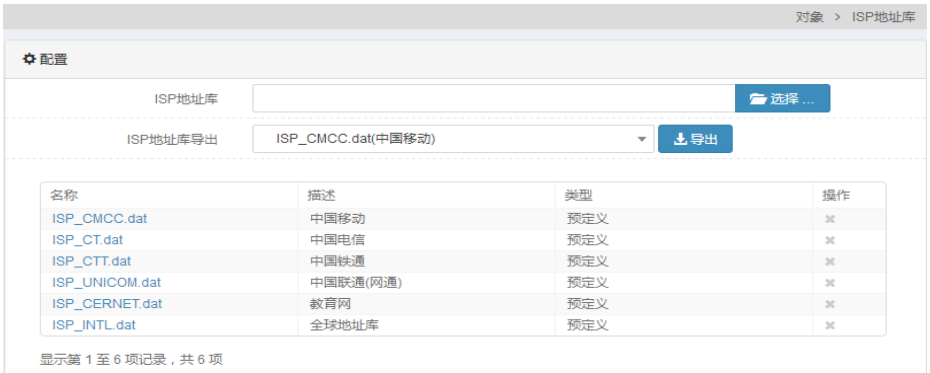
2.ISP 地址库的格式是唯一的，IPv4 只能是 A.B.C.D-A.B.C.D，IPv6 只能是 X:X::/M，其他的格式出现加载错误。

70.1 配置ISP地址库

ISP 地址库分为两类：预定义和自定义，预定义为系统自带，预定义 ISP 地址库不管有没有被地址对象引用都不能被删除；自定义为用户上传，自定义 ISP 地址库在没有被地址对象引用的情况下可以被删除。

70.1.1 配置ISP地址库

进入**对象> ISP 地址库**



名称：ISP 地址库的名称，不可以包含中文。

描述：对 ISP 地址库做描述，不得超过 127 个字符。

类型：ISP 地址库的类型。

ISP 地址库导入：导入 ISP 地址库。

ISP 地址库导出：导出 ISP 地址库。

70.1.2 ISP地址库导入

进入**对象> ISP 地址库->IPV4 或 IPV6**，如下图：

选择：选择合法的 ISP 地址库文件，如果文件名起始不是 ISP，则上传之后 IPv4 地址库会被自动加上 ISP_，IPv6 地址库会被自动加上 ISPV6_。

导入：上传文件到系统存储设备中。

移除：将选择的文件移除，重新选择。

注意

1.导入的 ISP 地址库文件最多支持 10M 大小，大于 10M 会导入失败。

2.导入的 ISP 地址库只有被地址对象引用时才会进行加载，ISP 地址库的行数如果超过 1 万行，则加载时只会加载前 1 万行，后面的 ISP 地址不会被加载，即，ISP 地址库中一万行之后的地址不会生效。

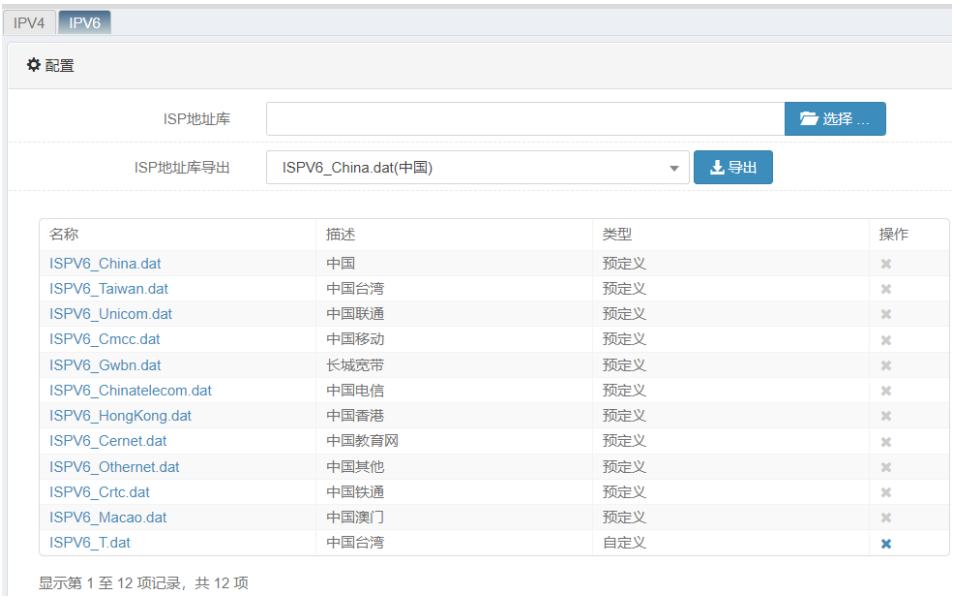
70.1.3 ISP地址库导出

进入**对象> ISP 地址库->IPV4 或 IPV6**，如下图：

导出：选择需要导出的 ISP 地址库文件，从设备导出到本地。

70.1.4 ISP地址库删除

进入**对象> ISP 地址库->IPV4 或 IPV6，如下图：**



点击 删除

注意

当删除按钮为灰色时，表明该 ISP 地址库正在被地址对象引用，或者为预定义 ISP 地址库，不能被删除。

70.2 常见故障分析

70.2.1 ISP地址加载不完整

故障现象	当ISP地址库被地址对象引用之后，会被解析加载到内存中，当查看ISP地址库的时候发现部分ISP地址不存在。
分析与解决	1)ISP地址库行数超过一万行，大于一万行的地址范围不会被解析加载，该情况建议将ISP地址库文件分拆。

71 第71章 服务对象

71.1 概述

为了方便用户的配置和管理，防火墙设备中引入了服务对象的概念。在其它功能(如防火墙策略、NAT 规则、路由策略)的配置中，可以引用服务对象来定义配置生效的条件。

服务对象里包括预定义服务，自定义服务，服务组。

预定义服务：系统预先添加服务，用户不可编辑或删除。

自定义服务：需要用户自行配置添加。

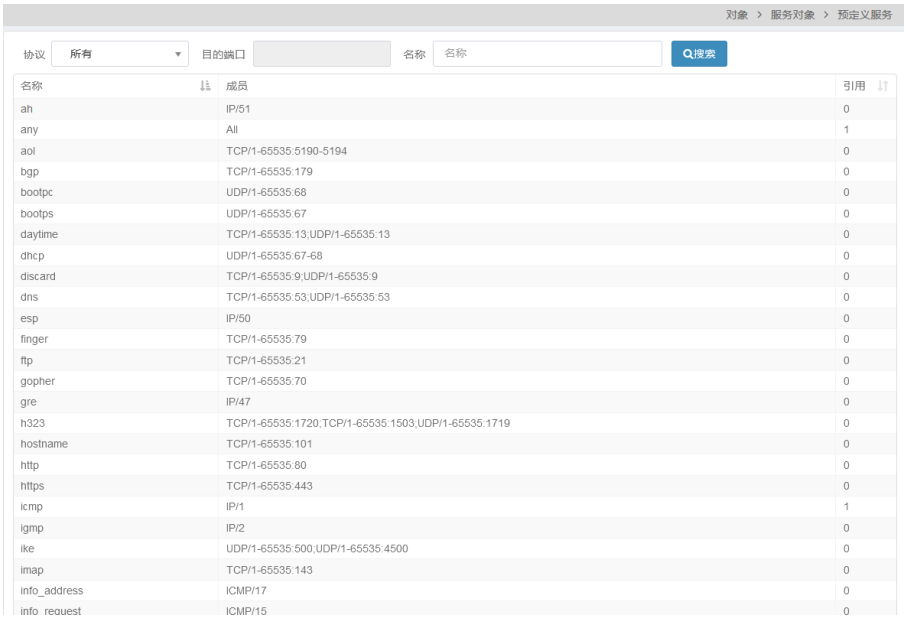
服务组：服务组是服务的集合。

71.2 配置服务对象

71.2.1 预定义服务

进入**对象->服务对象->预定义服务**，可查看预定义配置：

下图是部分系统预定义服务。

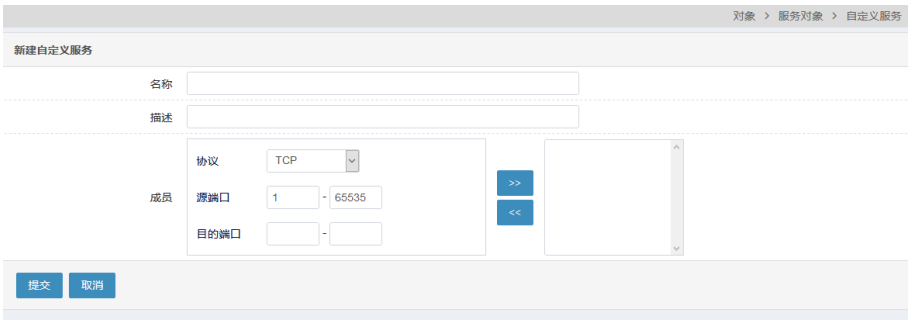


名称	成员	引用
ah	IP/51	0
any	All	1
aol	TCP/1-65535:5190-5194	0
bgp	TCP/1-65535:179	0
bootpc	UDP/1-65535:68	0
bootps	UDP/1-65535:67	0
daytime	TCP/1-65535:13;UDP/1-65535:13	0
dhcp	UDP/1-65535:67-68	0
discard	TCP/1-65535:9;UDP/1-65535:9	0
dns	TCP/1-65535:53;UDP/1-65535:53	0
esp	IP/50	0
finger	TCP/1-65535:79	0
ftp	TCP/1-65535:21	0
gopher	TCP/1-65535:70	0
gre	IP/47	0
h323	TCP/1-65535:1720;TCP/1-65535:1503;UDP/1-65535:1719	0
hostname	TCP/1-65535:101	0
http	TCP/1-65535:80	0
https	TCP/1-65535:443	0
icmp	IP/1	1
igmp	IP/2	0
ike	UDP/1-65535:500;UDP/1-65535:4500	0
imap	TCP/1-65535:143	0
info_address	ICMP/17	0
info_request	ICMP/15	0

71.2.2 配置自定义服务

配置步骤：

1.进入**对象->服务对象>自定义服务**，点击**新建**，如下图



名称：为新建自定义服务设置名称。

描述：对新建自定义服务做描述。

协议：可以自定义的服务协议（TCP,UDP,ICMP,IP）。

源端口：协议源端口号。

目的端口：协议目标端口号。

2.点击**提交**。

如果用户只想对某个协议填写特定端口，则“-”两边填写同样的端口号即可。

71.2.3 批量删除自定义服务

可对未被引用的自定义服务对象进行批量删除操作。

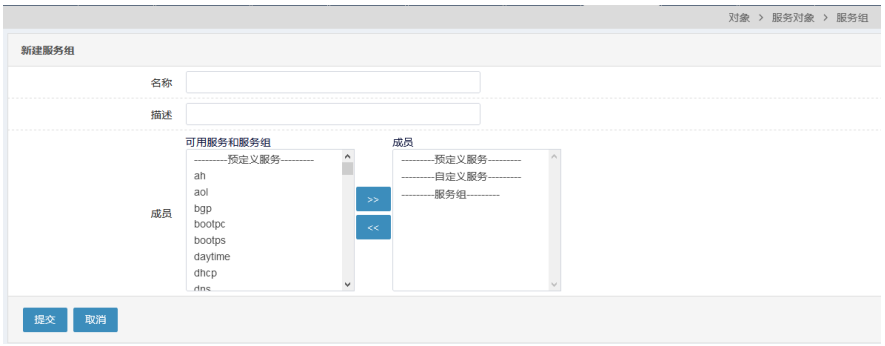
1. 进入**对象->服务对象->自定义服务**，在自定义服务对象首列选中可勾选所要批量删除的服务对象，如下图：

2. 点击 ，批量删除完成。

71.2.4 配置服务组

配置步骤：

1. 进入**对象->服务对象->服务组**，点击**新建**，如下图：



名称：为新建服务组设置名称。

描述：对新建服务组做描述。

可用服务和服务组：显示已有的服务对象，可从中选择预定义服务与自定义服务添加到服务组中。

2. 点击**提交**。

一个服务组可以被多个服务组包含，但是一个服务组包含只能有一层嵌套。

71.2.5 批量删除服务组

可对未被引用的服务组对象进行批量删除操作。

1. 进入**对象->服务对象->服务组**，在服务组对象首列选中可勾选所要批量删除的服务组，如下图：

2. 点击 ，批量删除完成。

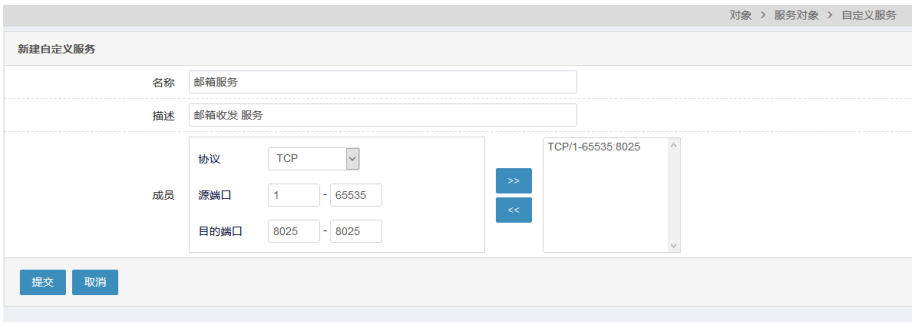
71.3 配置案例

71.3.1 配置案例1：添加自定义服务

案例描述

添加一个自定义 TCP 服务。

1．进入**对象->服务对象->自定义服务**，点击**新建**，如下图：



2．点击 >> 添加。

3．点击**提交**完成设置。

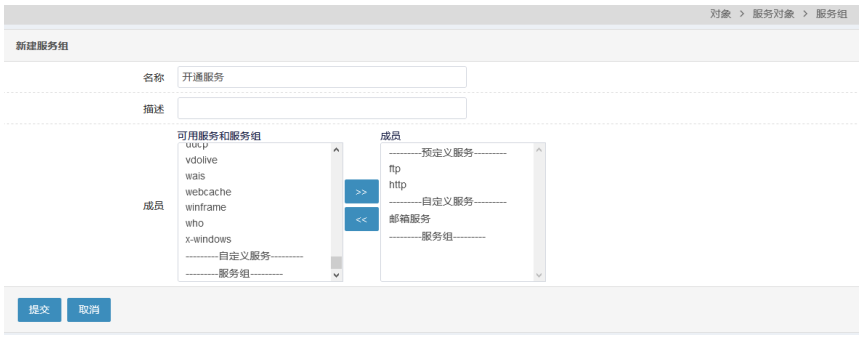
71.3.2 配置案例2：添加服务组

案例描述

服务组是服务的集合，为了管理方便配置服务组。

配置步骤：

1. 进入**对象->服务对象->服务组**，点击**新建**，如下图：



2. 添加 FTP，HTTP 和自定义服务**邮件服务**到开通服务组。

3. 点击 >> 添加。

4. 点击**提交**完成设置。

71.4 服务对象监控与维护

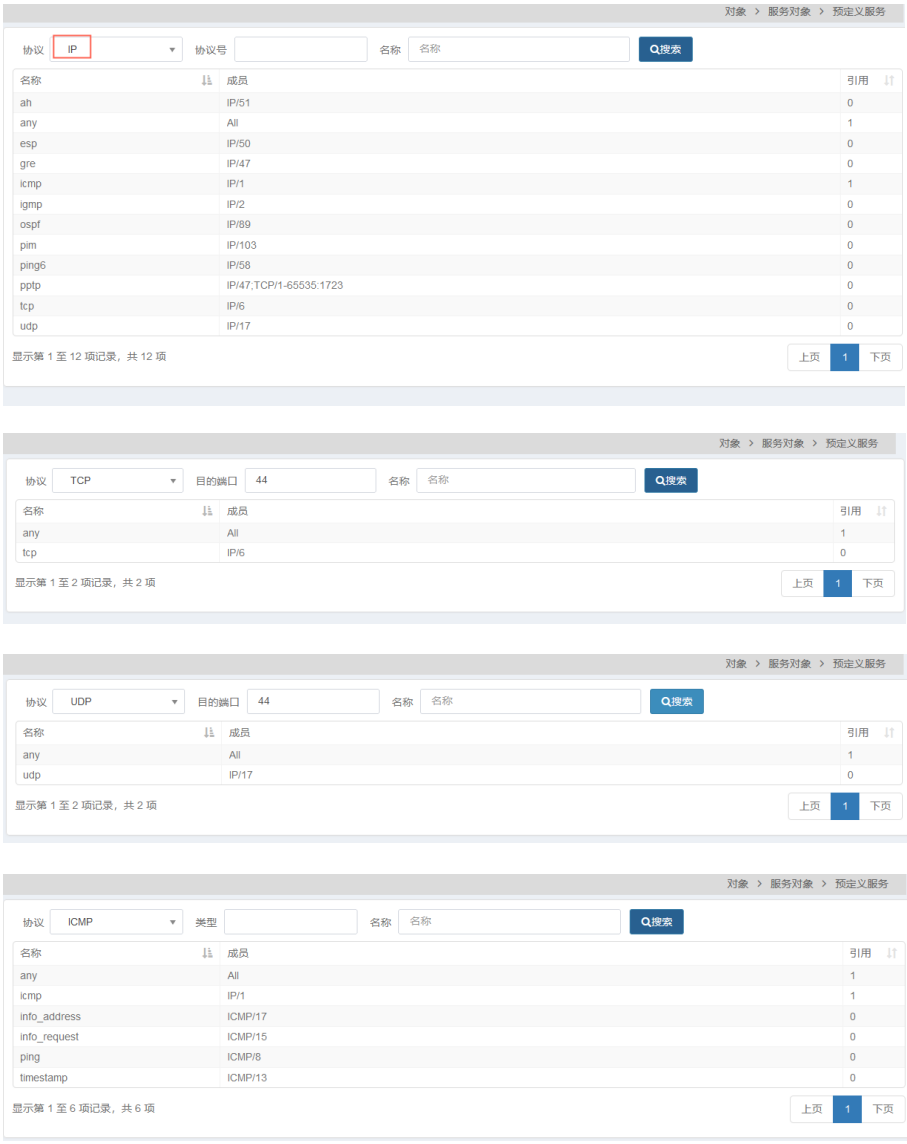
71.4.1 查看预定义服务

进入**对象->服务对象>预定义服务**，如下图：

1. 协议查找：

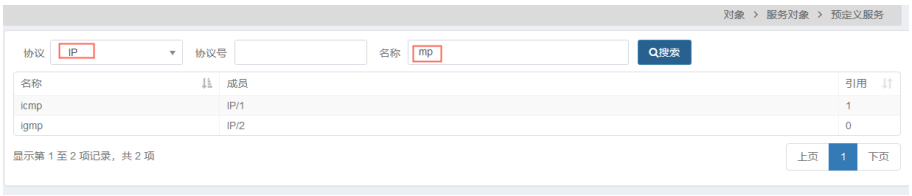
在**协议**输入(TCP/UDP/ICMP/IP)其中一种，点击 搜索 可以查看匹配项如下

图：



2. 名称查找：

在**名称**输入关键字，点击 搜索 可以查看匹配项如下图：



提示

因为预定义服务不可删除，故引用不做详情展示。

预定义服务协议若仅选中某协议搜索，目的端口、类型或协议号默认为所有。

71.4.2 查看自定义服务

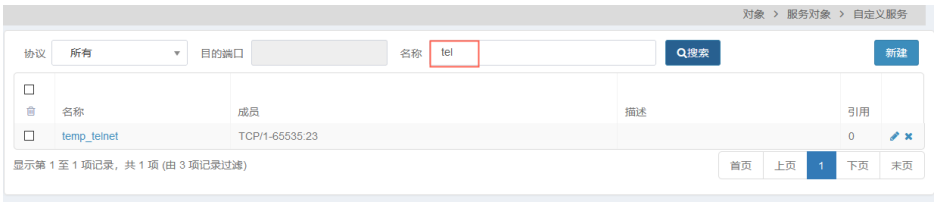
进入**对象->服务对象->自定义服务**，如下图：

1. 协议查找：

在**协议**输入 TCP，**目的端口**输入相应值，点击 搜索 可以查看匹配项如下图：

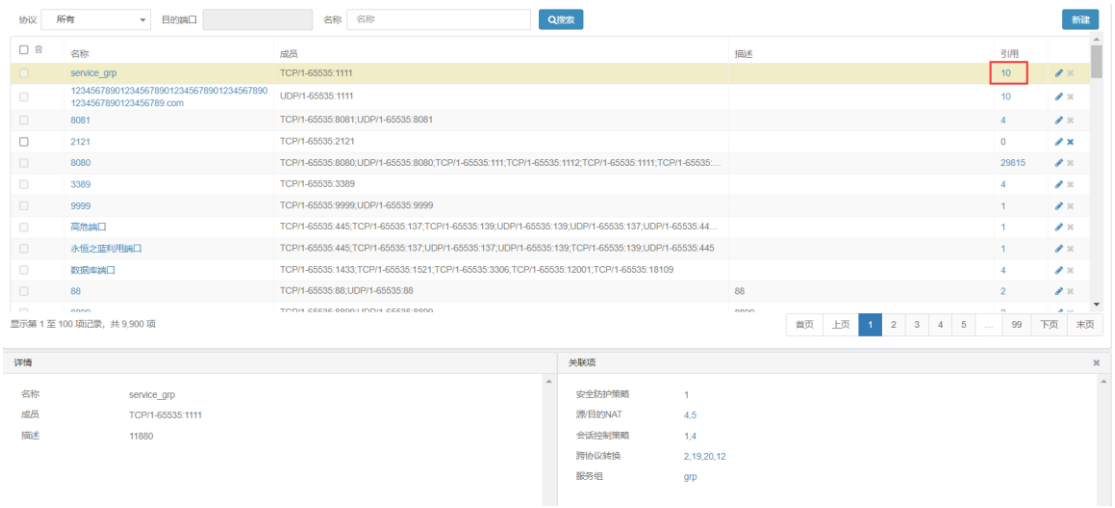
2. 名称查找：

在**名称**输入关键字，点击 搜索 可以查看匹配项如下图：



3. 引用详情展示：

点击**自定义服务对象**中非 0 引用数，可查看该对象被其他模块的关联项详情，如下图：



点击某个关联项，可跳转至对应模块进行解引用该自定义服务对象编辑操作，当该对象引用数减少至 0 时，可对其进行删除操作。

71.4.3 查看服务组

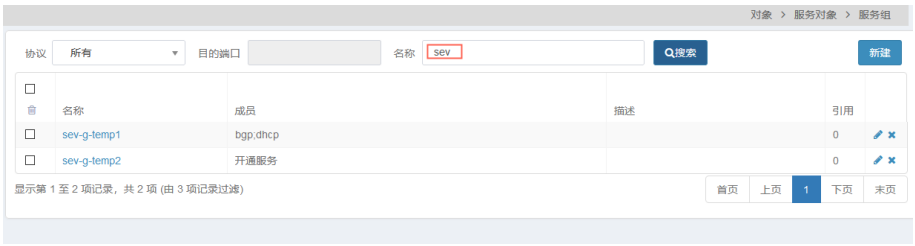
进入**对象->服务对象>服务组**，如下图：

1. 协议查找：

在**协议**输入 UDP，**目的端口**默认，点击 搜索 可以查看匹配项如下图：

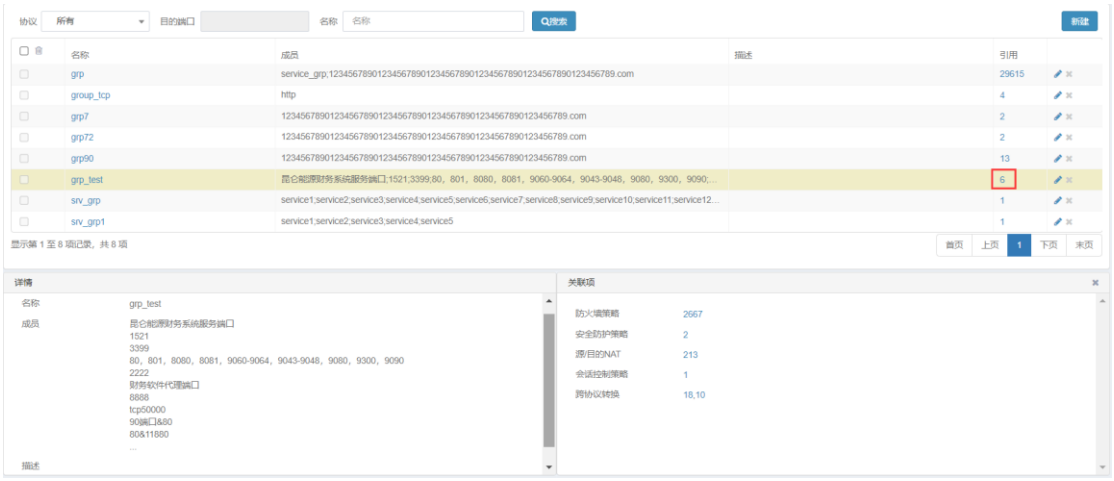
2. 名称查找：

在**名称**输入关键字，点击 搜索 可以查看匹配项如下图：



3. 引用详情展示：

点击服务组对象中非 0 引用数，可查看该对象被其他模块的关联项详情，如下图：



点击某个关联项，可跳转至对应模块进行解引用该服务组对象编辑操作，当该对象引用数减少至 0 时，可对其进行删除操作。

71.5 常见故障分析

71.5.1 故障现象：提交不成功

现象	当设置完毕后点击提交，显示提交失败。
分析	查看端口号是否正确。

72 第72章 应用对象

72.1 概述

为了方便用户的配置和管理，设备中引入了应用对象的概念。在策略的配置中，可以引用应用对象或应用组，方便进行访问控制。

应用对象，包括预定义应用、自定义应用、应用组三个部分。

- **预定义应用**：具体的用户应用，例如 QQ、微信等。目前有 20 大类 2000 多种应用。通过应用特征库进行更新，不需要用户配置。
- **自定义应用**：系统为用户提供自定义应用对象的接口。用户可通过协议类型、源地址、源端口、目的地址、目的端口共 5 个因素自定义应用对象。
- **应用组**：需要用户自行配置，可引用预定义应用和自定义应用。

在实际使用中，由各种策略来引用应用对象。

配合防火墙策略、应用控制策略、流量控制策略、会话控制策略使用，可实现将某些应用的流量进行阻断、限速等功能。

配合策略路由来使用，可以将某些应用的流量引入到指定链路中，实现“应用引流”的功能。对具体应用的流量引导，在实际网络环境中有较大的实用价值。例如，某网络环境有两条链路，其中一条为优质链路。用户往往会采用一些措施来保证优质链路的带宽，来避免一些大的流量（如 P2P 下载）对带宽的过度占有。

72.2 配置应用对象

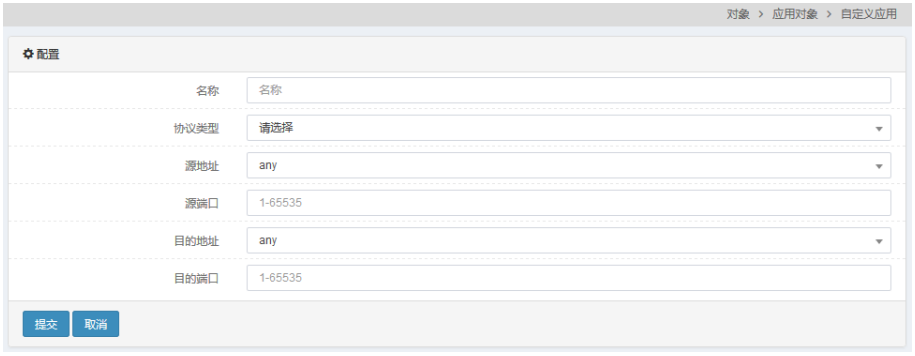
72.2.1 配置自定义应用

配置步骤：

1.进入**对象>应用对象>自定义应用**

该界面显示当前系统中已经配置的自定义应用对象。

2.点击**新建**，进入自定义应用配置页面。



名称：新建的自定义应用名称，不得超过 63 个字符。

协议类型：选择协议类型，可选项为 TCP 或 UDP。

源地址：自定义应用的源地址，可以引用已定义的某个地址对象或地址组对象，any 表示为匹配任意的源地址。

源端口：自定义应用的源端口，允许的取值范围是 1~65535。

目的地址：自定义应用的目的地址，可以引用已定义的某个地址对象或地址组对象，any 表示为匹配任意的目的地址。

目的端口：自定义应用的目的端口，允许的取值范围是 1~65535。

3.点击**提交**，进行配置提交，完成自定义应用的配置。

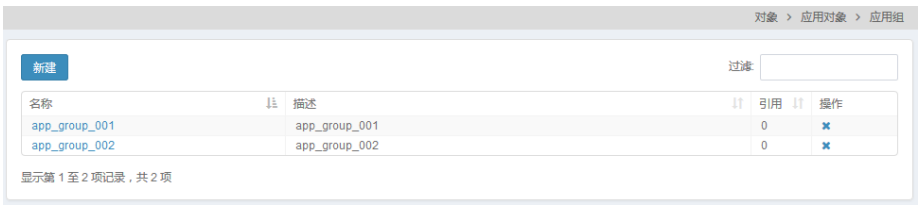
注意	自定义应用对象在应用对象的处理中优先级最高，一定要精确配置各个参数，否则可能会造成应用识别错误，进而引起引用了应用对象的策略无法正确匹配。

72.2.2 配置应用组

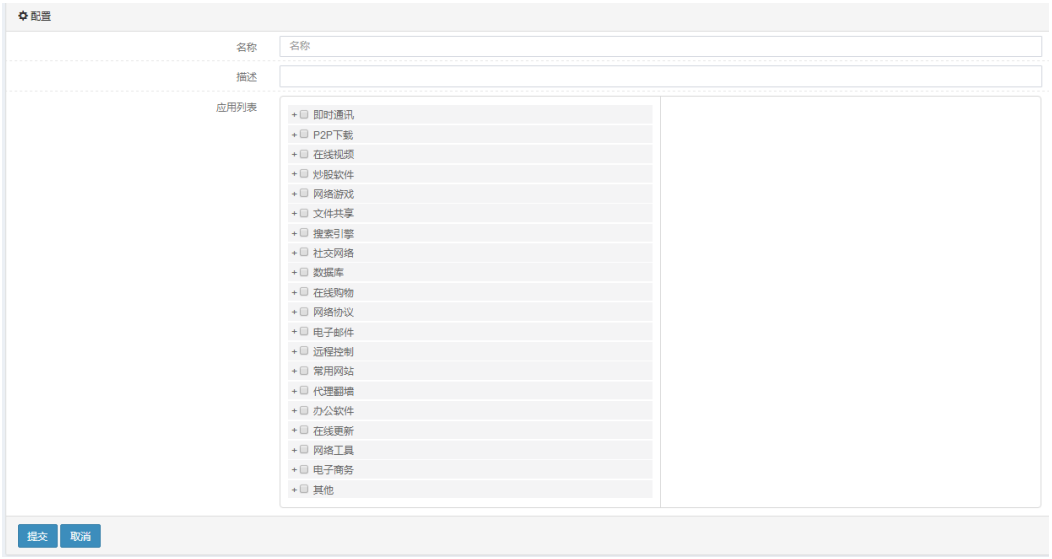
配置步骤：

1.进入**对象>应用对象>应用组**

该界面显示当前系统中已经配置的应用组对象。



2.点击**新建**，进入应用组配置页面



名称：新建的应用组对象名称，不得超过 63 个字符。

描述：新建的应用组描述，不得超过 127 个字符。

应用列表：系统所支持的所有应用列表，包括预定义应用和自定义应用，如上图所示。用户可通过在具体应用前面打勾的方式来选择应用，也可以通过在应用分类前面打勾的方式选择某一类应用；同样的，用户可通过在已选择应用前面的 将已选择的应用进行去除。

应用选择完成之后，点击**提交**，完成自定义应用组的配置。

在配置自定义应用组时，只有配置了自定义应用时，应用列表展示才会展示自定义应用。

72.3 配置案例

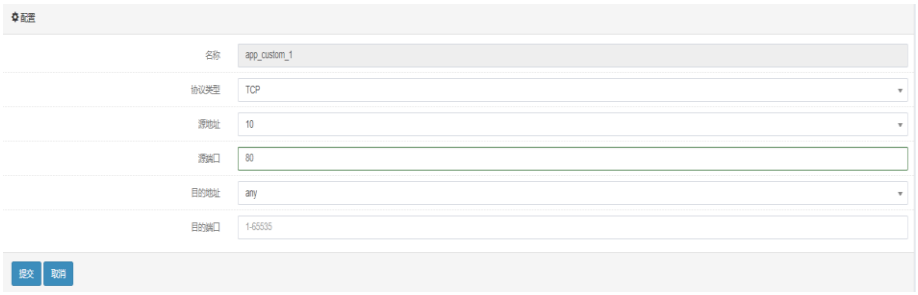
72.3.1 配置案例1：增加自定义应用

案例描述

系统中新建 1 个自定义应用对象。

配置步骤：

1. 进入**对象->应用对象>自定义应用**，点击**新建**，如下图：



2. 配置各项参数。本案例中录入的参数为：名称 app_custom_1,协议 TCP，源地址是名称为 10 的地址对象，源端口 80。

3. 点击**提交**完成自定义应用配置。

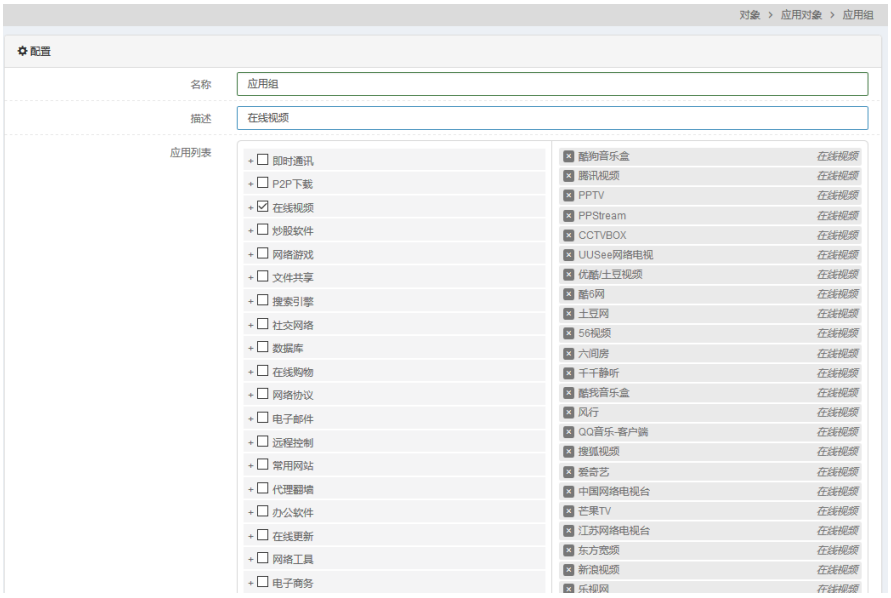
72.3.2 配置案例2：增加应用组

案例描述

系统中配置 1 个应用组对象，引用在线视频分类。

配置步骤：

1. 进入**对象->应用对象>应用组**，点击**新建**，如下图：



2. 输入应用组名称、描述，选择在线视频分类。

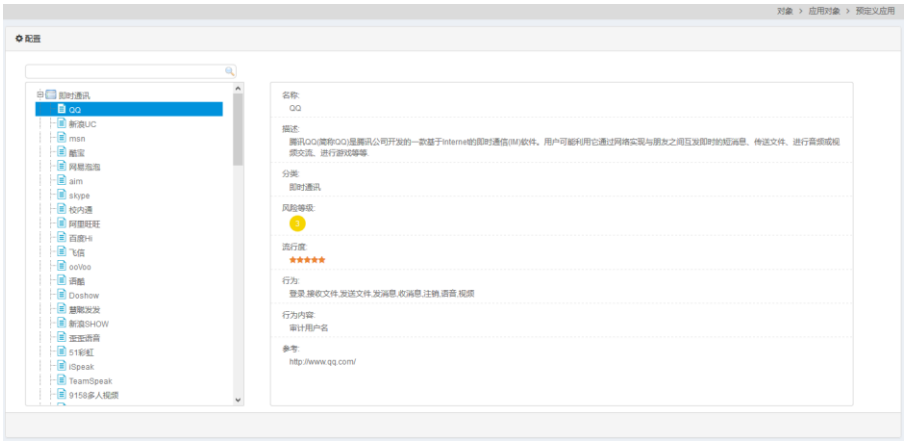
3. 点击**提交**完成设置。

72.4 监控与维护

72.4.1 查看预定义应用

进入**对象>应用对象>预定义应用**，通过左侧树状目录中选择应用，如下图

所示：

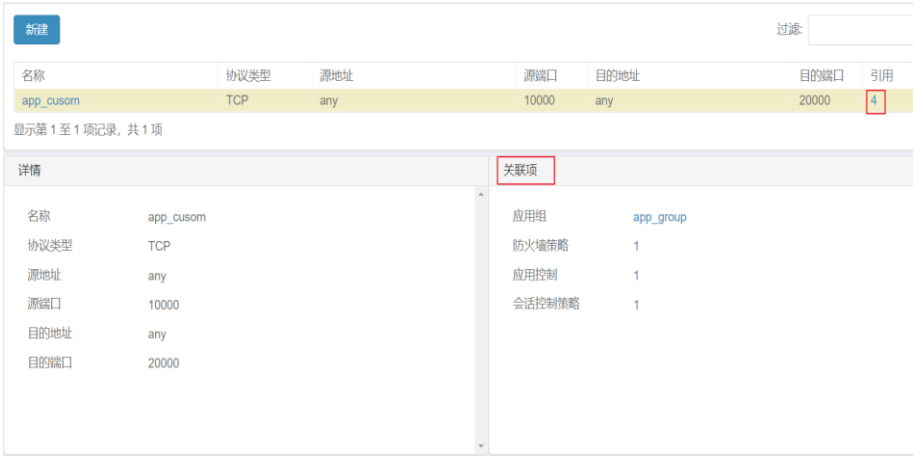


72.4.2 查看自定义应用

进入**对象>应用对象>自定义应用**，如下图所示：

引用详情显示：

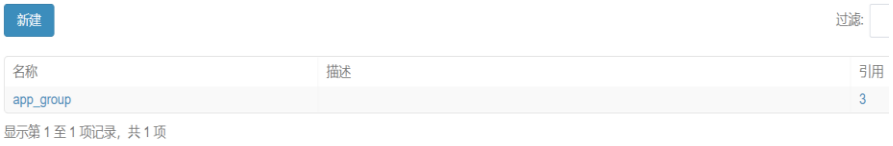
点击非 0 引用数字，可查看该应用对象或者应用组对象被其他模块的引用详情，如下图所示：



点击某个关联项，可跳转至对应模块对引用的应用对象进行编辑操作，当该地址对象引用数减少至 0 时，可对其进行删除操作。

72.4.3 查看应用组

进入**对象>应用对象>应用组**，如下图所示：



引用详情显示：

点击非 0 引用数字之后，可查看该应用组被其他模块的引用详情，如下图所示：

点击某个关联项，可跳转至对应模块对引用的应用组对象进行编辑操作，当该地址对象引用数减少至 0 时，可对其进行删除操作。

73 第73章 用户对象

73.1 用户对象概述

为了方便用户的配置和管理，T 系列防火墙设备中引入了用户对象的概念。在其它功能(如 web 认证、L2TP、SSL-VPN)的配置中，可以引用用户对象来定义配置生效的条件。

用户对象里包括用户和用户组。

用户：用户分为认证用户和静态绑定用户，认证用户又分为本地用户，radius 用户以及 ldap 用户。

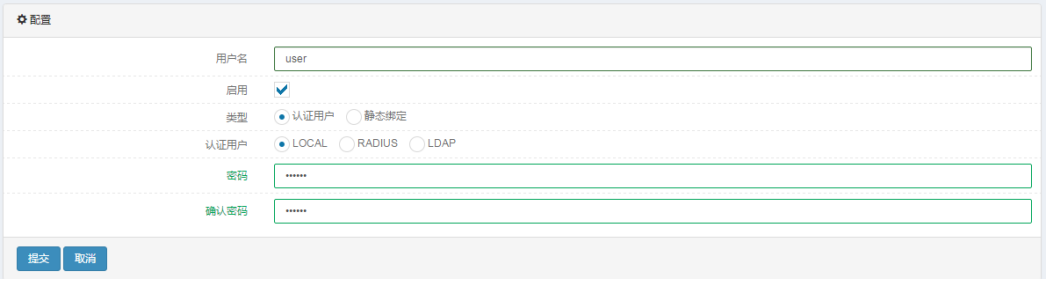
用户组：用户组是用户的集合。

73.2 配置用户对象

73.2.1 配置本地认证用户对象

配置本地用户对象

进入**对象>用户对象>用户**，点击**新建**



用户名：用户认证成功后，设备上看到的用户名。

启用：该用户名有效。

类型：认证用户或者静态用户。

认证用户：认证用户类型，包括本地用户，radius 用户，ldap 用户。

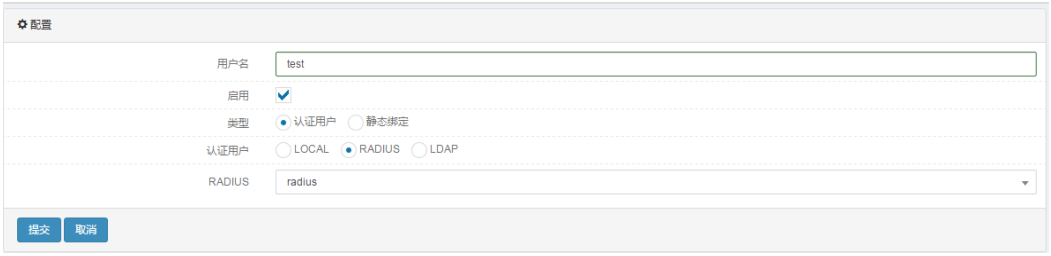
密码：用户认证时的密码。

确认密码：需要和密码一致。

73.2.2 配置radius用户对象

配置 radius 用户对象

进入**对象>用户对象>用户**，点击**新建**



用户名：radius 服务器上的用户名

启用：该用户名有效。

类型：认证用户

认证用户： radius

Radius：radius 服务器对象

配置 radius 用户需要存在 radius 服务器对象，radius 服务器对象配置请参考相应章节。

73.2.3 配置ldap用户对象

配置 ldap 用户对象

进入**对象>用户对象>用户**，点击**新建**

用户名：ldap 服务器上的用户名

启用：该用户名有效。

类型：认证用户

认证用户： ldap

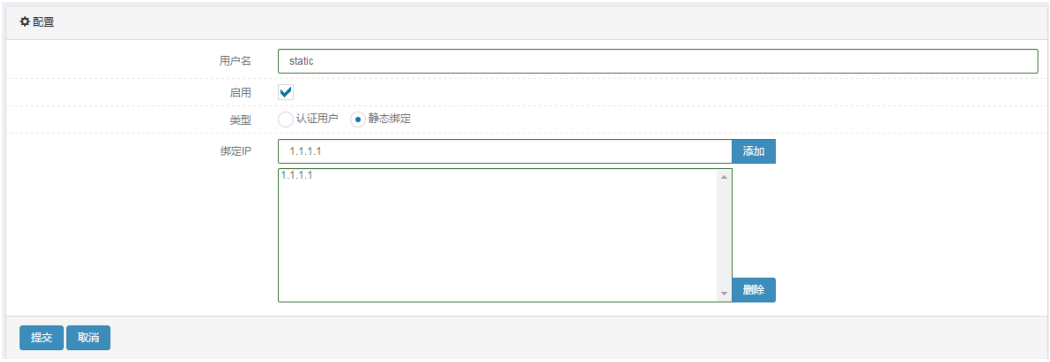
ldap：ldap 服务器对象

配置 ldap 用户需要存在 ldap 服务器对象，ldap 服务器对象配置请参考相应章节。

73.2.4 配置静态用户对象

配置静态用户对象

进入**对象>用户对象>用户**，点击**新建**



用户名：策略中引用的用户名

启用：该用户名有效。

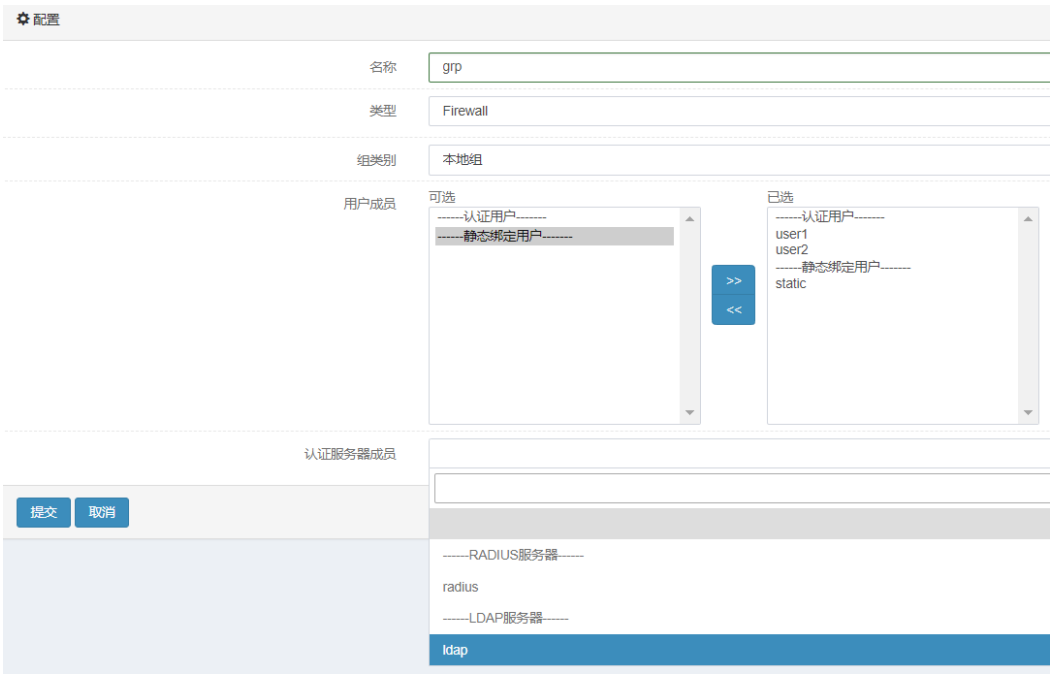
类型：静态用户

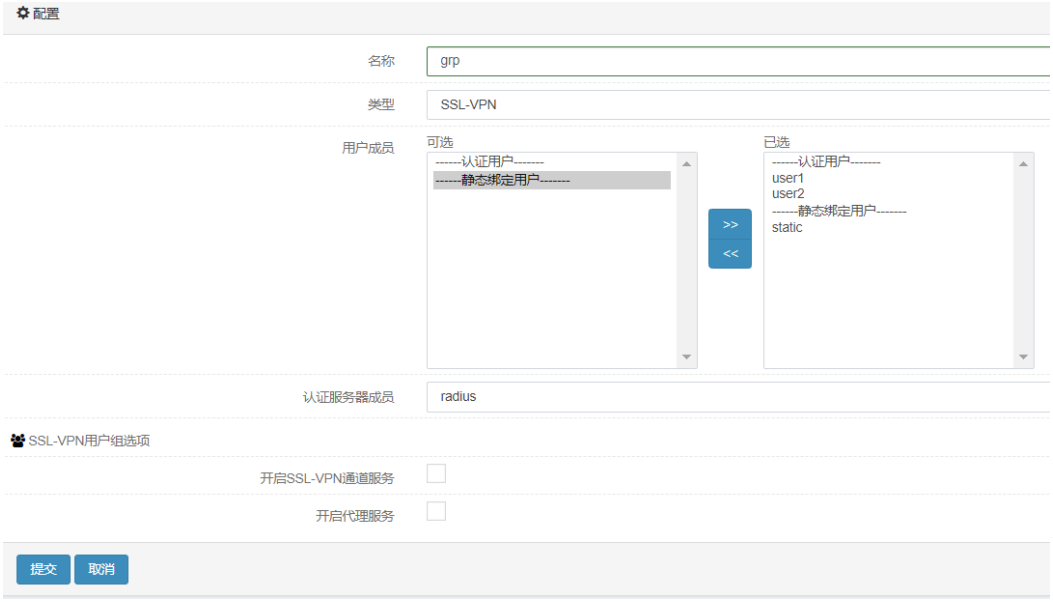
绑定 IP： 用户名和 IP 地址的绑定关系

73.3 配置用户组对象

配置用户组对象：web 认证和 L2TP 配置中所使用的用户对象都针对用户组对象。

进入**对象>用户对象>用户组**，点击**新建**





名称：用户组名称

类型：用户组所属类型分别为 Firewalls 和 SSL-VPN，默认为 Firewall

用户成员：用户对象成员，包括认证用户和静态用户

认证服务器成员：可以选择 radius 用户或者 ldap 用户

SSL-VPN 用户组选项：类型为 SSL-VPN 时，此选项才会显示

开启 SSL-VPN 通道服务：使该组用户可以使用 SSL VPN 隧道模式（可选）

开启代理服务：使该组用户可以使用 Web 代理模式（可选）

73.4 用户对象查看

查看用户对象

进入**对象>用户对象>用户**

查看已配置的用户列表

用户名：用户名称

类型：用户类型

绑定 IP：用户绑定的 IP 地址

状态：启用状态

引用：用户对象被引用的次数

操作：可重命名用户名，并且当该用户名未被引用时可做删除操作

点击**引用**列后面的数字，查看用户对象被引用详情

点击某个关联项，可跳转至对应模块进行解引用该地址对象编辑操作，当该地址对象引用数减少至 0 时，可对其进行删除操作。

73.5 用户组对象查看

查看用户组对象

进入**对象>用户对象>用户组**

查看已配置的用户组列表

名称：用户组名称

成员：用户组成员

类型：用户组类型，分 Firewalls 和 SSL-VPN

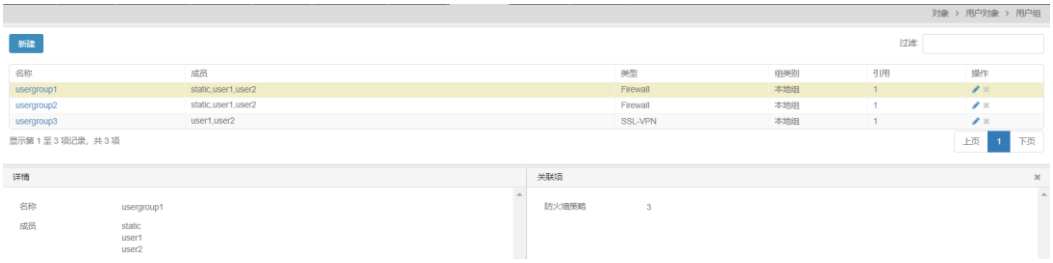
组类别：用户组类别，分本地组和同步组

引用：用户组对象被引用的次数

操作：可重命名用户名，并且当该用户组未被引用时可做删除操作

点击**引用**列后面的数字，查看用户组对象被引用详情

点击某个关联项，可跳转至对应模块进行解引用该地址对象编辑操作，当该地址对象引用数减少至 0 时，可对其进行删除操作。


对象 › 用户对象 › 用户组
新建
过滤
名称 成员 类型 组类别 引用 操作
usergroup1 static,user1,user2 Firewall 本地组 1
usergroup2 static,user1,user2 Firewall 本地组 1
usergroup3 user1,user2 SSL-VPN 本地组 1
显示第 1 至 3 项记录，共 3 项
上页 1 下页
详情
名称 usergroup1
成员 static
user1
user2
关联项
防火墙策略 3

74 第74章 认证服务器对象

74.1 认证服务器对象概述

T 系列防火墙支持使用 RADIUS 服务器、LDAP 服务器的用户认证。（1）可以添加一个 RADIUS 服务器对象，以允许用户使用选定的 RADIUS 服务器进行认证。（2）可以添加一个 LDAP 服务器对象，以允许用户使用选定的 LDAP 服务器进行认证。在 web 认证与管理员认证中，可以选择配置的服务器对象进行远程认证。（3）使用 AD 域同步策略可以将 LDAP 服务器上的用户组同步到设备上，方便用户使用。

74.2 配置认证服务器对象

74.2.1 配置RADIUS服务器对象

如果您配置了 RADIUS，当某个 web 认证用户、管理员用户被配置为要求使用 RADIUS 服务器认证的时候，T 系列防火墙将连接 RADIUS 服务器以获得认证。

进入**对象>认证服务器>RADIUS**，点击**新建**

名称：RADIUS 服务器名称，标识 RADIUS 服务器。

服务器 IP：RADIUS 服务器的 IP 地址。

服务器密码：RADIUS 服务器的共享密钥。

认证端口：RADIUS 服务器用于认证的端口。默认 1812。

点击**认证服务器**下的 **RADIUS 配置**标签页，显示当前系统中配置的所有 RADIUS 服务器。

74.2.2 配置LDAP服务器

如果您配置了 LDAP，当某个 web 认证用户、管理员用户被配置为要求使用 LDAP 服务器认证的时候，T 系列防火墙将连接 LDAP 服务器以获得认证。

进入**对象>认证服务器>LDAP**，点击**新建**

名称：LDAP 服务器名称，标识 LDAP 服务器。

服务器 IP：LDAP 服务器的 IP 地址。

端口：LDAP 服务器用于认证的端口。缺省为 389

区别名：用来指明在 LDAP 服务器上查找数据的起始位置。如，ldap 服务器上，在路径 test.com 中，容器 users 下有用户 user2。则区别名中配置为”dc=test，dc=com”。

管理员：LDAP 服务器的管理员用户。如，登陆 ldap 服务器的系统用户名为 administrator，密码为 111111，且该系统用户也存在于 ldap 服务器下，处于 test.com 中容器 users 下。则此管理员配置为”cn=administrator,cn=users,dc=test,dc=com”密码为”111111”。

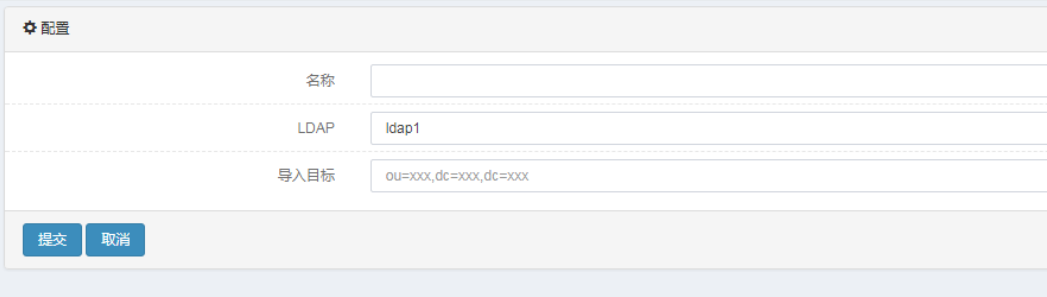
密码：LDAP 服务器的管理员密码。

点击**认证用户**下的 **LDAP** 标签页，显示当前系统中配置的所有 LDAP 服务器。

74.3 配置AD域同步策略

74.3.1 新建同步策略

1. 进入**对象>认证服务器>AD 域同步**，点击**新建**：



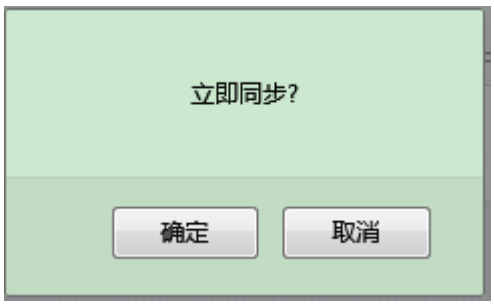
名称：同步策略的名称，标识模板名称。

LDAP：LDAP 服务器名称，标识 LDAP 服务器。

导入目标：DN，即同步 LDAP 服务器上哪个路径下的用户组名称。

2. 点击**提交，显示**：

3. 点击**立即同步**，显示。



4. 点击**确定**，则立即同步用户组。

74.3.2 配置案例

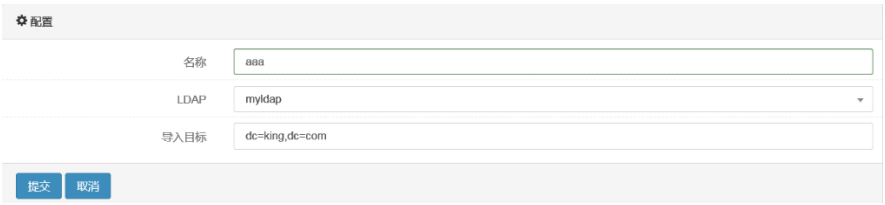
案例描述

同步服务器为 3.3.3.2 上的路径为 dc=king，dc=com 下的用户组。

配置步骤：

1. 进入**对象>认证服务器>LDAP**，新建 LDAP 服务器：

2. 进入**对象>认证服务器>AD 域同步**，新建同步策略：



3. 点击立即同步：

4. 查看同步结果，组类别为**同步组**的即为同步过来的组：

75 第75章 URL 分类

75.1 概述

为了方便用户的配置和管理，设备中引入了 URL 分类的概念。在策略的配置中，可以引用 URL 分类来定义配置生效的条件，方便控制。

应用对象，实际上包括预定义 URL 分类、自定义 URL 分类、URL 组三个部分。

- **预定义 URL 分类**：将常见的 URL 进行分类，例如娱乐、金融理财、互联网门户等，通过 URL 特征库更新，不需要用户配置。
- **自定义 URL 分类**：需要用户自行配置。
- **URL 组**：需要用户自行配置，可引用预定义 URL 分类和自定义 URL 分类。

在实际使用中，由各种策略来引用 URL 分类和 URL 组。

配合应用控制策略使用，可实现将某些应用的流量进行阻断、限速等功能。

75.2 配置URL分类

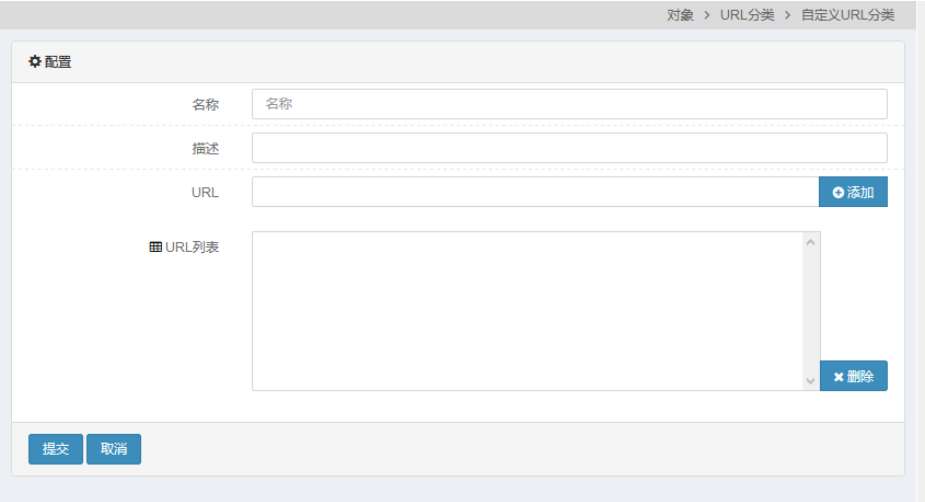
75.2.1 配置自定义URL分类

配置步骤：

1.进入**对象>URL 分类>自定义 URL 分类**

该界面显示已配置的自定义 URL 分类。

2.点击**新建**，进入自定义 URL 分类配置页面。



名称：为新建自定义 URL 分类的名称，不得超过 63 个字符。

描述：为新建自定义 URL 分类的描述，不得超过 127 个字符。

URL：将指定 URL 字符串添加到该分类下，不得超过 127 个字符。

URL 列表：已添加到该分类下的 URL 字符串列表。

3.点击**提交**。

注意

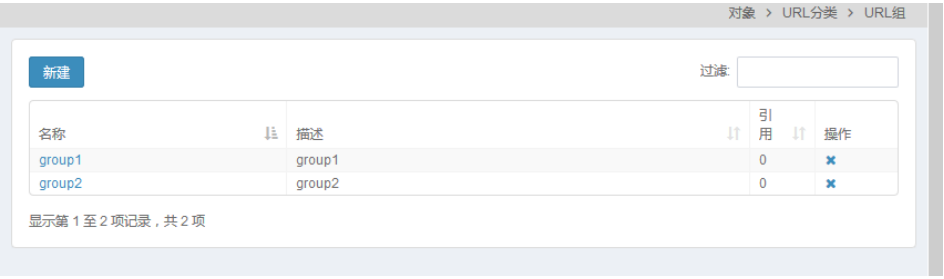
自定义 URL 分类优先级最高，一定要合理配置添加到自定义 URL 分类的 URL 字符串，否则其他访问也被识别成了自定义 URL 分类，导致其他控制策略无法匹配到真正 URL 分类。

75.2.2 配置URL组

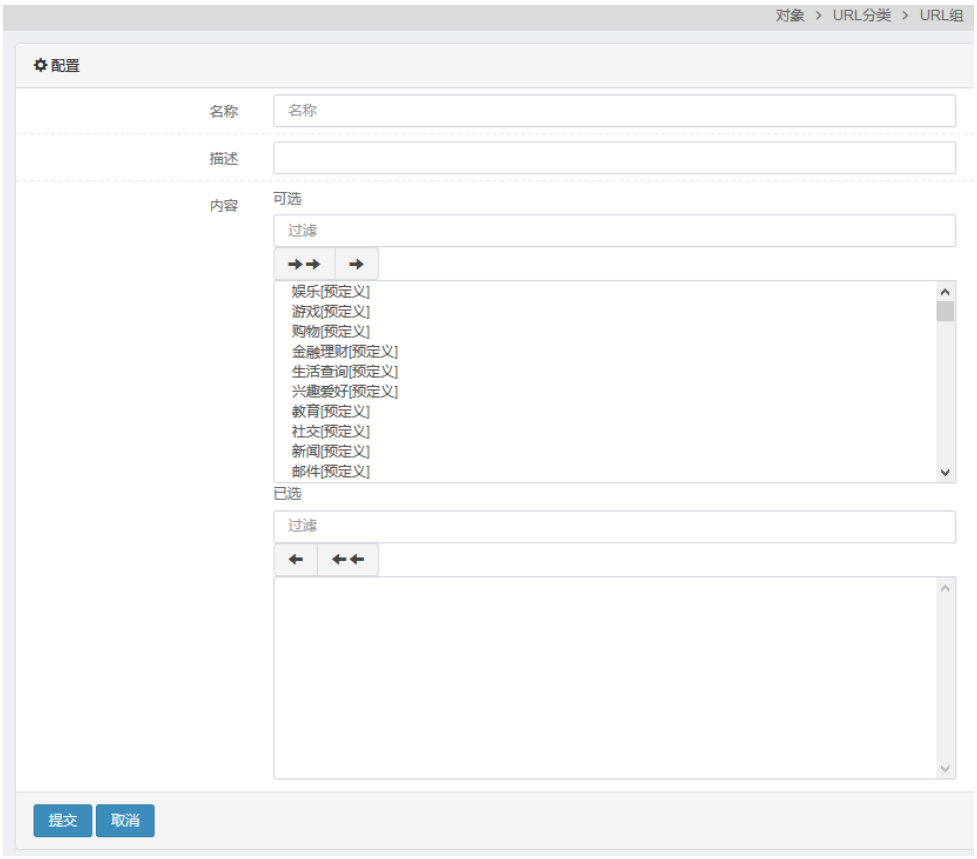
配置步骤：

1.进入**对象>URL 分类>URL 组**

该界面显示已配置的 URL 组。



2.点击**新建**，进入 URL 组配置页面



名称：为新建 URL 组的名称，不得超过 63 个字符。

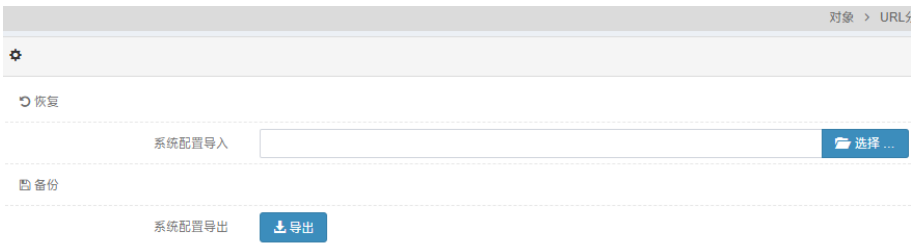
描述：为新建 URL 组的描述，不得超过 127 个字符。

内容：为设备上已配置的自定义 URL 分类和所有预定义 URL 分类。

选中所想要的 URL 分类，点击**提交**。

75.3 自定义URL分类配置备份恢复

进入**对象>URL 分类>备份恢复**



系统配置导入：选择配置文件导入到设备中。

系统配置导出：将设备中的配置文件导出。

75.4 配置案例

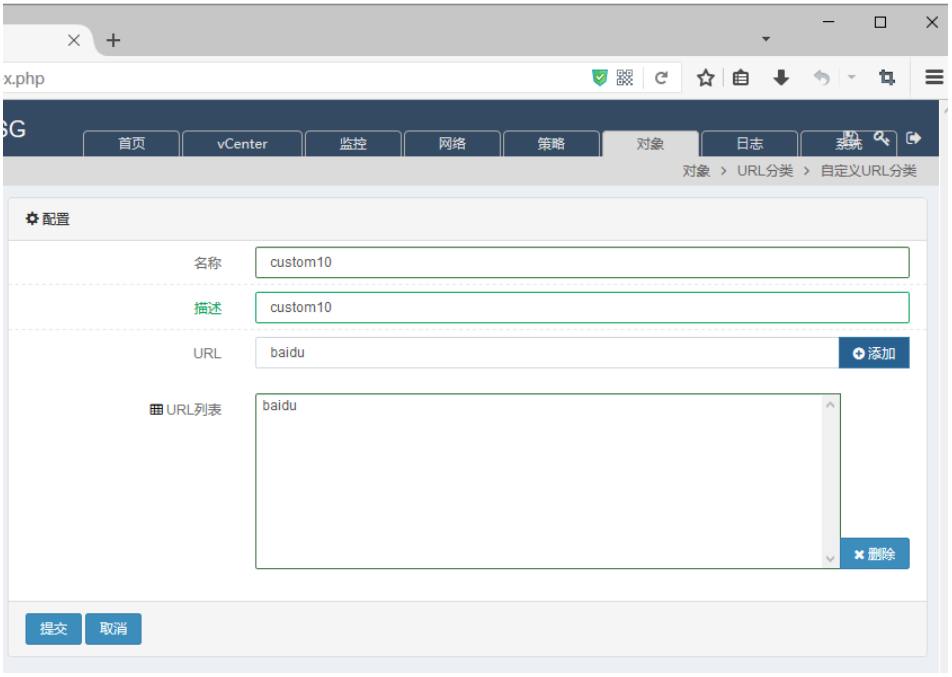
75.4.1 配置案例1：增加自定义URL分类

案例描述

增加一个自定义 URL 分类，被其他策略引用。

配置步骤：

1.进入**对象->URL 分类>自定义 URL 分类**，点击**新建**，如下图：



2.输入参数。

3.点击**提交**完成设置。

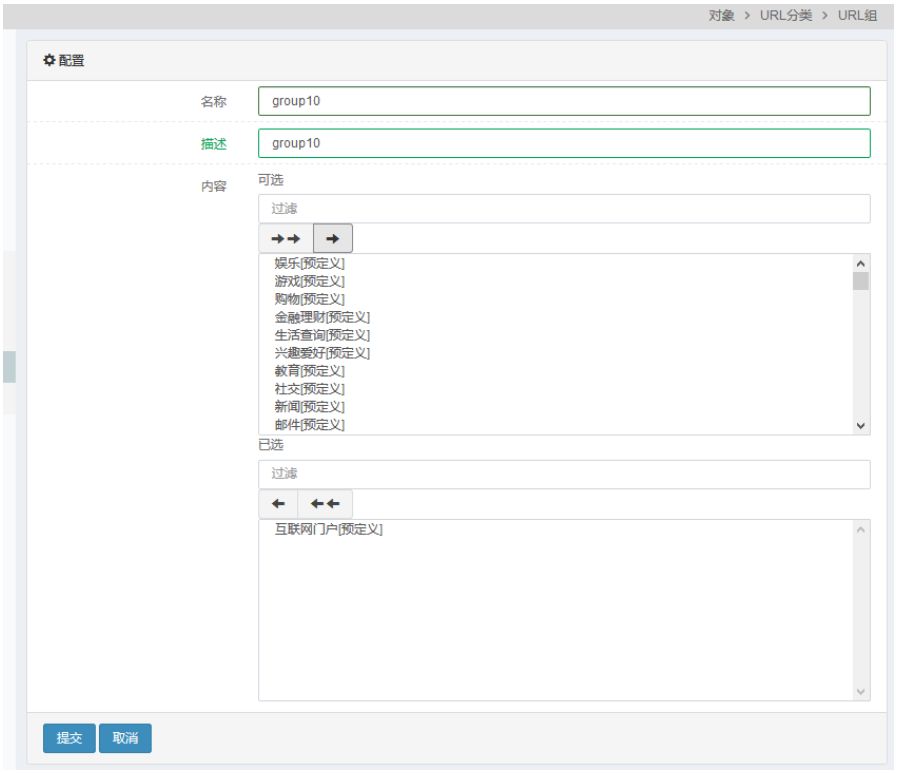
75.4.2 配置案例2：增加URL组

案例描述

配置 URL 组，引用互联网门户分类，使引用该 URL 组的策略对互联网门户类的 URL 访问生效。

配置步骤：

1. 进入**对象->URL 分类>URL 组**，点击**新建**，如下图：



2. 输入 URL 组名称、描述，选择互联网门户分类。
3. 点击**提交**完成设置。

75.5 监控与维护

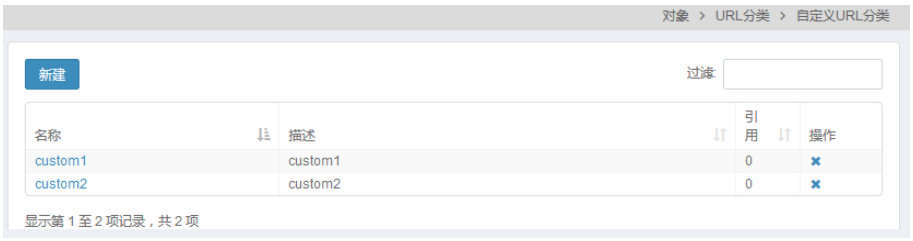
75.5.1 查看预定义URL分类

进入**对象>URL 分类>预定义 URL 分类**，如下：

ID	名称	描述
1	娱乐	提供综合性娱乐、影视的网站。
2	游戏	提供各种电子游戏的网站。
3	购物	提供网络购物站点的网站。
4	金融理财	提供各种类型金融理财的网站。
5	生活查询	提供涉及日常生活的综合资讯或服务的网站。
6	兴趣爱好	提供各种类别的兴趣爱好相关的网站。
7	教育	提供各类教育资讯或提供相关服务信息的网站。
8	社交	提供建立社会性网络的互联网应用服务的网站。
9	新闻	提供综合型新闻、资讯的网站。
10	邮件	用于电子手段提供信息交换的通信方式的网站。
11	博彩	提供合法的公益性彩票的资讯、预测信息或经国家允许的在线投注网站。
12	行业门户	用于提供互联网的门户网站和企业应用系统的门户系统的网站
13	互联网门户	提供有关信息服务的应用系统的网站。
14	百科文库	提供天文、地理、自然、人文、宗教、信仰等学科知识的网站。
15	宗教信仰	提供各类宗教团体或民间信仰团体的网站，及介绍宗教信仰相关知识、历史、商品的网站。
16	翻墙网站	提供绕过相应的IP封锁、内容过滤、域名劫持、流量限制等，实现对网络内容访问的网站。
17	非法行为	含有违反国家各项法律法规内容或利用法律漏洞从事不合法活动的网站。
18	低俗行为	提供人体艺术图片、上门按摩服务、成人保健、成人情趣用品买卖、一夜情交友信息、同志交友
19	安全隐患	以病毒、恶意代码、间谍软件等方式非法获得用户资料及造成用户设备或财产损失的网站。
20	在线更新	提供在线更新，以及售后服务的网站。
21	网络资源	本身不提供网页内容，只是作为其他网页的素材存储网址的网站。
22	在线音乐	提供为用户检索，在线收听音频相关信息的网站。
23	在线视频	提供在线观看视频的网站。
24	网页游戏	提供在线网页游戏的网站。

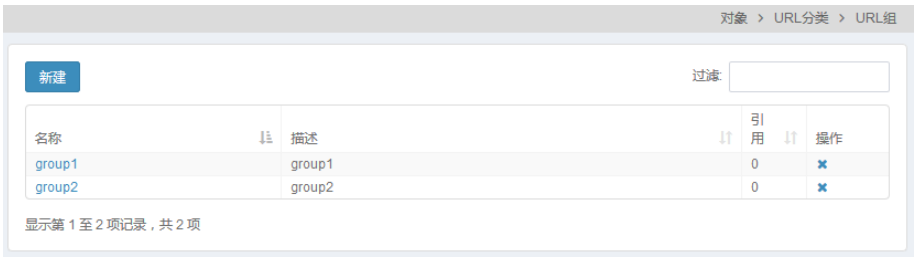
75.5.2 查看自定义URL分类

进入**对象>URL 分类>自定义 URL 分类**，如下：



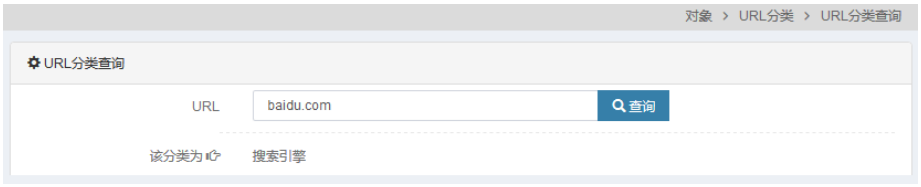
75.5.3 查看URL组

进入**对象>URL 分类>URL 组**，如下：



75.5.4 URL分类查询

进入**对象>URL 分类>URL 分类查询**，如下：



URL：为待查询 URL，不得超过 127 个字符。

输入待查询 URL，点击**查询**。

76 第76章 域名对象

76.1 概述

为了方便用户的配置和管理，设备中引入了域名对象的概念。在策略的配置中，可以引用域名对象，方便控制。

域名对象，包括自定义域名、域名组两个部分。

- **自定义域名**：需要用户自行配置。
- **域名组**：需要用户自行配置，可引用自定义域名。

在实际使用中，由策略来引用域名对象。

配合路由策略来使用，可以将访问某些域名的流量引入到指定链路中，实现引流的功能，在实际网络环境中有较大的实用价值。

76.2 配置域名对象

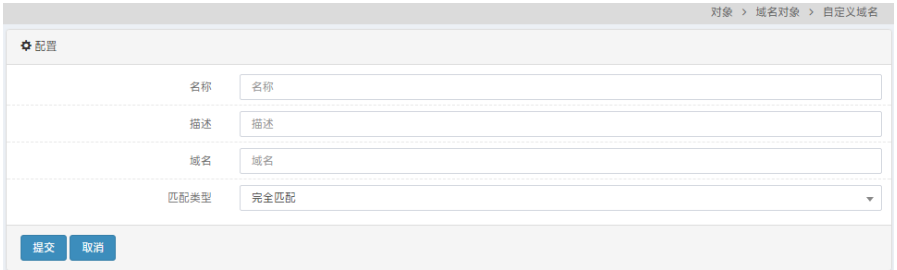
76.2.1 配置自定义域名

配置步骤：

1.进入**对象>域名对象>自定义域名**

该界面显示已配置的自定义域名。

2.点击**新建**，进入自定义域名配置页面。



名称：为新建自定义域名的名称，不得超过 63 个字符。

描述：为新建自定义域名的描述，不得超过 127 个字符。

域名：为新建自定义域名的域名匹配字符串。

匹配类型：为新建自定义域名的匹配类型，包括完全匹配和包含。

3.点击**提交**。

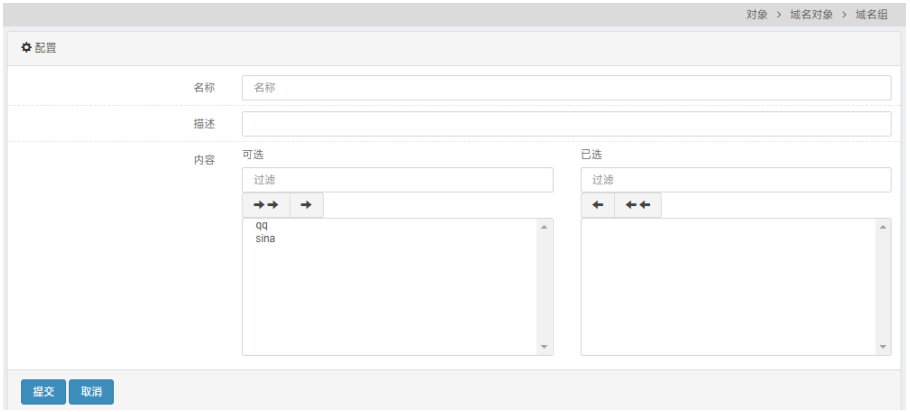
76.2.2 配置域名组

配置步骤：

1.进入**对象>域名对象>域名组**

该界面显示已配置的域名组。

2.点击**新建**，进入域名组配置页面



名称：为新建域名组的名称，不得超过 63 个字符。

描述：为新建域名组的描述，不得超过 127 个字符。

内容：为已配置的自定义域名列表。如上图所示。

选中所想要的应用，点击**提交**。

76.3 配置案例

76.3.1 配置案例1：增加自定义域名

案例描述

增加一个自定义域名，被其他策略引用。

配置步骤：

1. 进入**对象->域名对象>自定义域名**，点击**新建**，如下图：

2. 输入参数。
3. 点击**提交**完成设置。

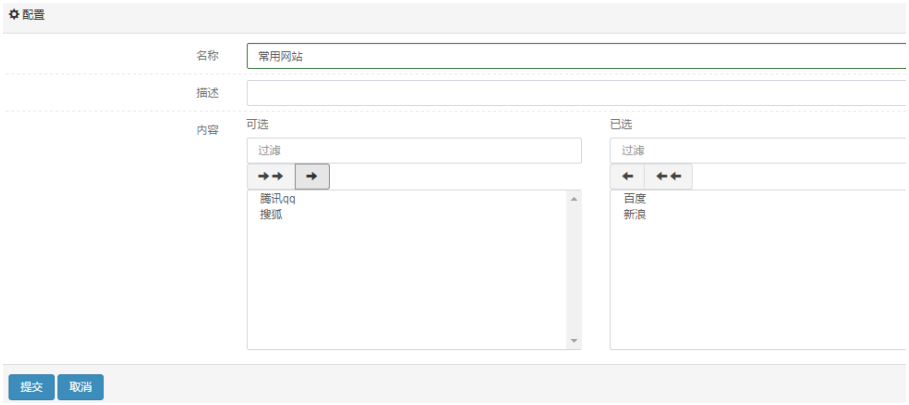
76.3.2 配置案例2：增加域名组

案例描述

配置域名组，引用自定义域名，使引用该域名组的策略对访问该域名的流量生效。

配置步骤：

1. 进入**对象->域名对象>域名组**，点击**新建**，如下图：



2. 输入域名组名称、描述，选择自定义域名。
3. 点击**提交**完成设置。

76.4 监控与维护

76.4.1 查看自定义域名

进入**对象>域名对象>自定义域名**，如下：

76.4.2 查看域名组

进入**对象>域名对象>域名组**，如下：

77 第77章 时间对象

77.1 概述

为了方便用户配置和管理，防火墙设备中引入了时间对象概念，时间对象分为绝对时间和周期时间。在其它功能的配置中，可以引用时间对象来定义配置生效的条件。

绝对时间：配置服+务在指定的时间内生效。

周期时间：配置服务在指定的时间范围内在指定的周期（星期一 ~ 星期日）执行。

77.2 配置时间对象

77.2.1 配置绝对时间

绝对时间中只能配置一个有效时间范围。

进入**对象>时间对象>绝对时间**，点击**新建**，如下图：

名称：为新建绝对时间设置名称。

描述：对新建绝对时间做描述。

开始时间：绝对时间的起始时间（年，月，日，时，分）。

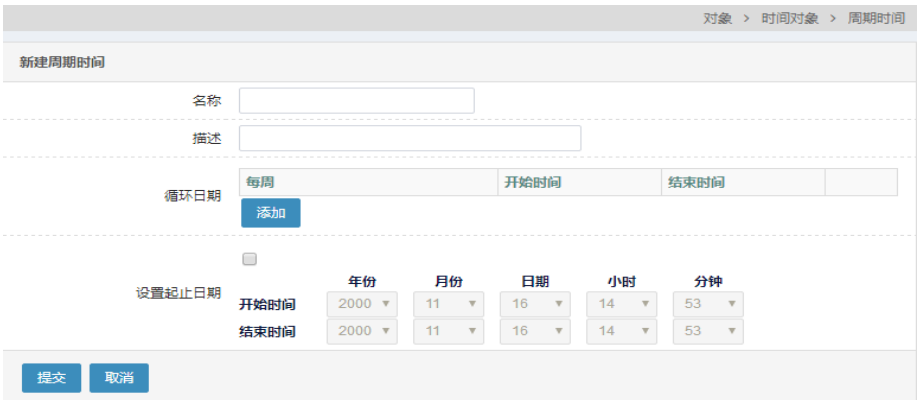
结束时间：绝对时间的终止时间（年，月，日，时，分）。

点击**提交**。

77.2.2 配置周期时间

周期时间中可以定义有效时间范围和有效时间段。有效时间范围只能有一个，而有效时间段可以有多个。有效时间段之间是或的关系，满足其中一个即可；有效时间范围和有效时间段之间是与的关系，都满足才生效。

1. 进入**对象->时间对象>周期时间**，点击**新建**，如下图：



名称：为新建周期时间设置名称。

描述：对新建周期时间做描述。

开始时间：有效时间范围的起始时间（年，月，日，时，分）。

结束时间：有效时间范围的终止时间（年，月，日，时，分）。

循环日期：点击增加按钮可以添加日期设置有效时间段，如下图：

2. 点击**提交**。

77.3 配置案例

77.3.1 配置案例1：增加绝对时间

案例描述

增加一个绝对时间对象，此对象目的是被防火墙策略引用，使该防火墙策略只在一个特定的时间生效。

配置步骤：

1. 进入**对象->时间对象>绝对时间**，点击**新建**，如下图：

2. 输入参数。

3. 点击**提交**完成设置。

77.3.2 配置案例2：增加周期时间

案例描述

配置周期时间，使引用该对象的策略周期性生效。

配置步骤：

1. 进入**对象->时间对象>周期时间**，点击**新建**，如下图：

2. 点击**提交**完成设置。

77.4 绝对时间与周期时间监控与维护

77.4.1 查看绝对时间

点击**对象->时间对象>绝对时间**，如下图：

77.5 常见故障分析

77.5.1 故障现象：提交不成功

现象	当设置完毕后点击提交，显示提交失败。
分析	结束时间比开始时间早。
解决	修改结束时间到开始时间之后。

78 第78章 健康检查

78.1 健康检查概述

健康检查用来对路由下一跳或远端设备进行探测，来获取路由下一跳或远端设备的健康状况。一旦发现链路或设备故障，将不再往该链路上进行流量分担。

支持的健康检查方式包括 ICMP，TCP，UDP，HTTP，HTTPS，RADIUS，LDAP，FTP，POP3，SMTP 等等，除了使用 ICMP 能够对连通性监控外，对具体的服务可以使用相应的检查方式提供更准确的监控。

T 系列防火墙提供了 IPv4 和 IPv6 服务器的健康检查功能。

78.2 配置健康检查

进入**对象>健康检查**，点击**新建**。

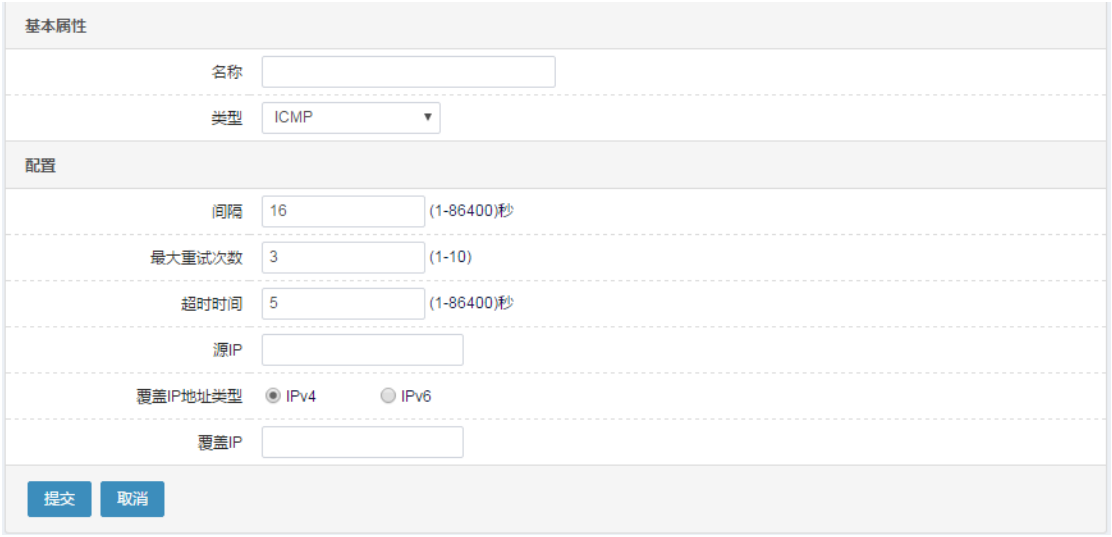
名称：健康检查模板的名称。

类型：健康检查的类型。选择类型后弹出具体类型的模板配置。

配置步骤：

1. 输入**名称**。
2. 选择**类型**。

当类型为 ICMP 时，配置界面如下：



名称：指定新建健康检查模板的名称。

类型：指定新建健康检查模板的协议类型。

间隔：健康检查发送状态探测包的间隔时间，单位为秒。

最大重试次数：健康检查探测包探测失败后的重试次数。例如，默认参数 3 次，如果发送 3 个健康检查状态包都没收到回应或者 3 次都探测失败，则健康检查返回状态为失败的最终结果。

超时时间：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

源 IP：指定发送健康检查探测包的源 IP 地址，当健康检查源 IP 地址需要指定时填写此项。

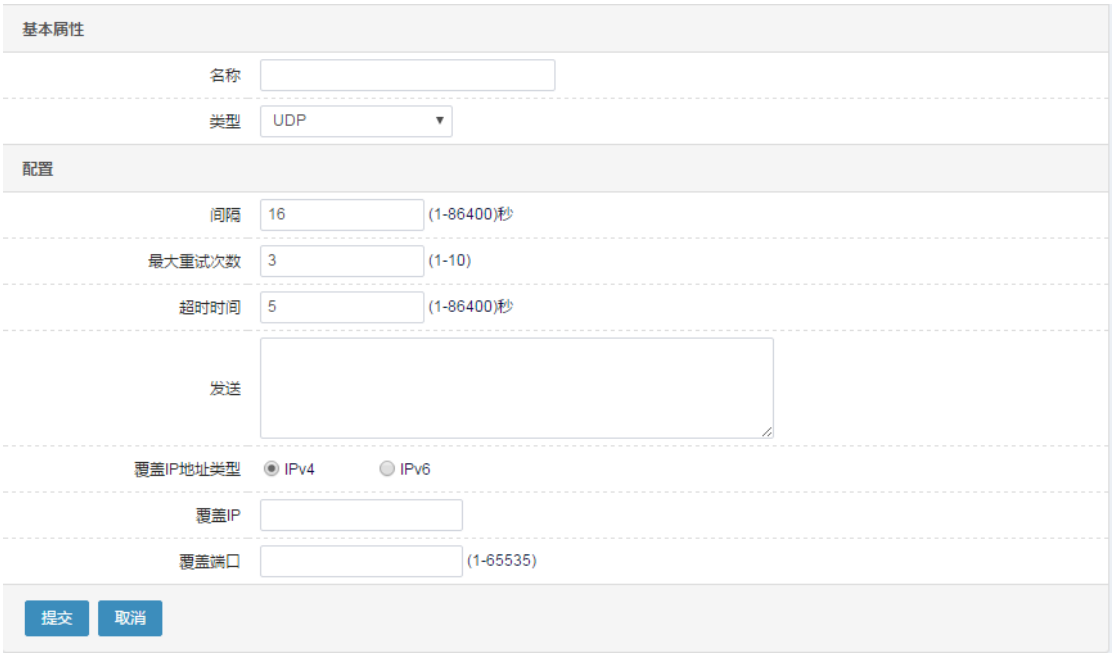
覆盖 IP 地址类型：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

覆盖 IP：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机或链路时填写此项。

配置步骤：

8. 输入**间隔**。
9. 输入**最大重试次数**。
10. 输入**超时时间**。
11. 选择**覆盖 IP 地址类型**。
12. 选择输入**覆盖 IP**。
13. 点击**提交**。

当类型为 UDP 时，配置界面如下：



名称：指定新建健康检查模板的名称。

类型：指定新建健康检查模板的协议类型。

间隔：健康检查发送状态探测包的间隔时间，单位为秒。

最大重试次数：健康检查探测包探测失败后的重试次数。例如，默认参数 3 次，如果发送 3 个健康检查状态包都没收到回应或者 3 次都探测失败，则健康检查返回状态为失败的最终结果。

超时时间：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

发送：UDP 报文中的发送内容。

覆盖 IP 地址类型：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

覆盖 IP：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机或链路时填写此项。

覆盖端口：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置。

配置步骤：

1. 输入**间隔**。
2. 输入**最大重试次数**。
3. 输入**超时时间**。
4. 选择输入**发送**。
5. 选择**覆盖 IP 地址类型**。

6. 选择输入**覆盖 IP 和覆盖端口**。
7. 点击**提交**。

提示	UDP 健康检查必须组合其他方式的健康检查使用，如 ICMP。因为 UDP 在服务不可用或者探测地址不存在时现象是相同的。

当类型为 TCP 时，配置界面如下：

名称：指定新建健康检查模板的名称。

类型：指定新建健康检查模板的协议类型。

间隔：健康检查发送状态探测包的间隔时间，单位为秒。

最大重试次数：健康检查探测包探测失败后的重试次数。例如，默认参数 3 次，如果发送 3 个健康检查状态包都没收到回应或者 3 次都探测失败，则健康检查返回状态为失败的最终结果。

超时时间：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

发送：TCP 报文中的发送内容。

接收：接收到报文中应含的内容。当接收到的内容不包含此内容时，状态为 DOWN。

覆盖 IP 地址类型：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

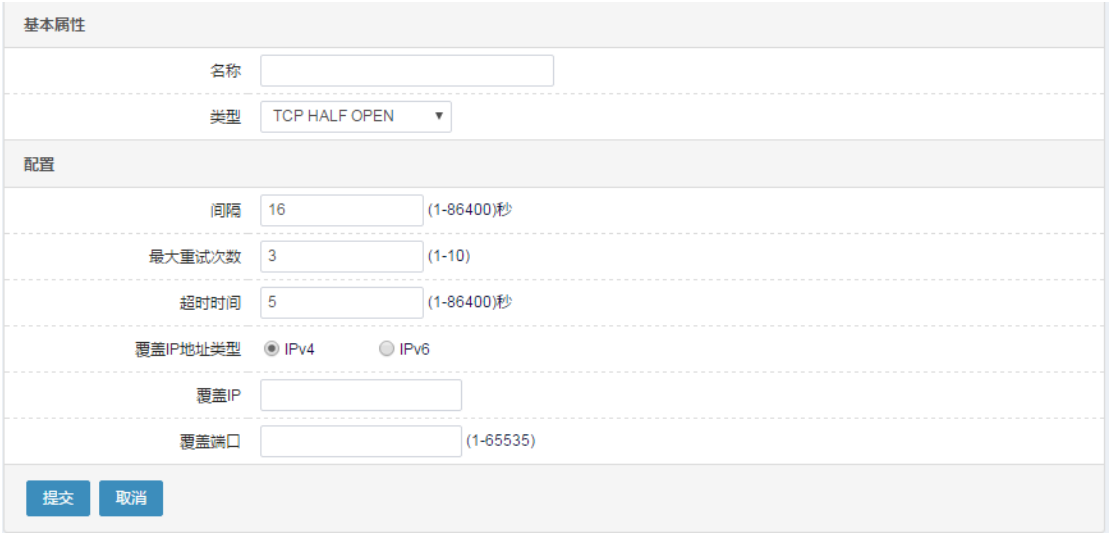
覆盖 IP：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机或链路时填写此项。

覆盖端口：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置。

配置步骤：

1. 输入**间隔**。
2. 输入**最大重试次数**。
3. 输入**超时时间**。
4. 选择输入**发送**内容。
5. 选择输入**接收**内容。
6. 选择**覆盖 IP 地址类型**。
7. 选择输入**覆盖 IP 和覆盖端口**。
8. 点击**提交**。

当类型为 TCP HALF OPEN 时，配置界面如下：



名称：指定新建健康检查模板的名称。

类型：指定新建健康检查模板的协议类型。

间隔：健康检查发送状态探测包的间隔时间，单位为秒。

最大重试次数：健康检查探测包探测失败后的重试次数。例如，默认参数 3 次，如果发送 3 个健康检查状态包都没收到回应或者 3 次都探测失败，则健康检查返回状态为失败的最终结果。

超时时间：发送的健康检查探测包在此时间内如果没收到回应包，则此次

健康检查探测失败，单位为秒。

覆盖 IP 地址类型：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

覆盖 IP：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机或链路时填写此项。

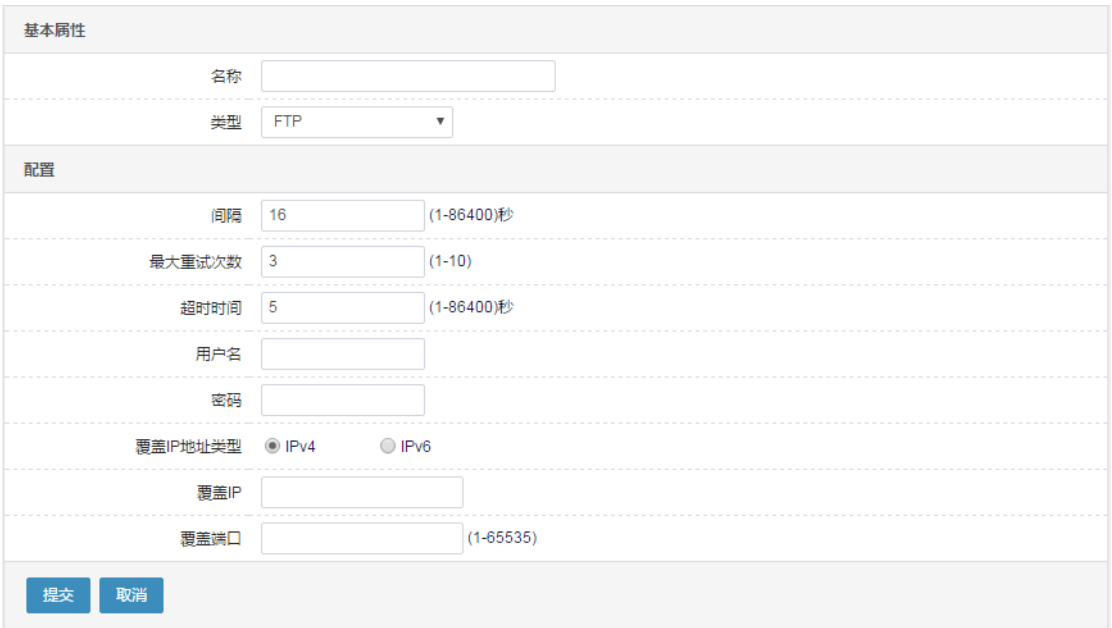
覆盖端口：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置。

配置步骤：

1. 输入**间隔**。
2. 输入**最大重试次数**。
3. 输入**超时时间**。
4. 选择**覆盖 IP 地址类型**。
5. 选择输入**覆盖 IP**。
6. 点击**提交**。

同 TCP 类型健康检查相比，TCP HALF OPEN 类型健康检查在设备和服务器之间不建立连接，减少了报文交互。

当类型为 FTP 时，配置界面如下：



名称：指定新建健康检查模板的名称。

类型：指定新建健康检查模板的协议类型。

间隔：健康检查发送状态探测包的间隔时间，单位为秒。

最大重试次数：健康检查探测包探测失败后的重试次数。例如，默认参数 3 次，如果发送 3 个健康检查状态包都没收到回应或者 3 次都探测失败，则健康检查返回状态为失败的最终结果。

超时时间：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

用户名：FTP 认证的用户名。

密码：FTP 用户的密码。

覆盖 IP 地址类型：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

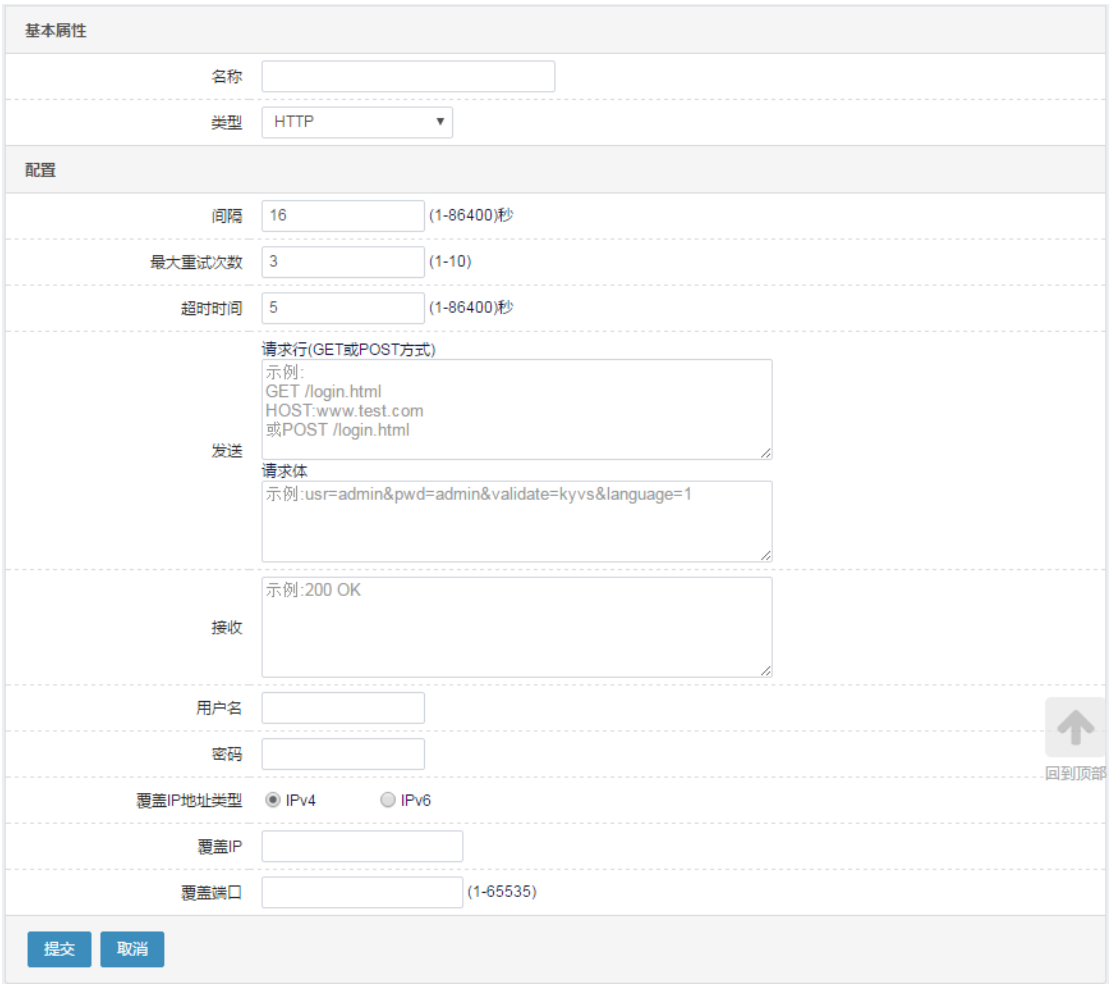
覆盖 IP：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机或链路时填写此项。

覆盖端口：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置。

配置步骤：

1. 输入**间隔**。
2. 输入**最大重试次数**。
3. 输入**超时时间**。
4. 输入**用户名。**
5. 输入**密码。**
6. 选择**覆盖 IP 地址类型**。
7. 选择输入**覆盖 IP 和覆盖端口**。
8. 点击**提交**。

当类型为 HTTP/HTTPS 时，配置界面如下：



名称：指定新建健康检查模板的名称。

类型：指定新建健康检查模板的协议类型。

间隔：健康检查发送状态探测包的间隔时间，单位为秒。

最大重试次数：健康检查探测包探测失败后的重试次数。例如，默认参数 3 次，如果发送 3 个健康检查状态包都没收到回应或者 3 次都探测失败，则健康检查返回状态为失败的最终结果。

超时时间：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

发送：HTTP/HTTPS 报文中的发送内容。

接收：接收到报文中应含的内容。当接收到的内容不包含此内容时，状态为 DOWN。

用户名：HTTP/HTTPS 认证的用户名。

密码：HTTP/HTTPS 用户的密码。

覆盖 IP 地址类型：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

覆盖 IP：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况

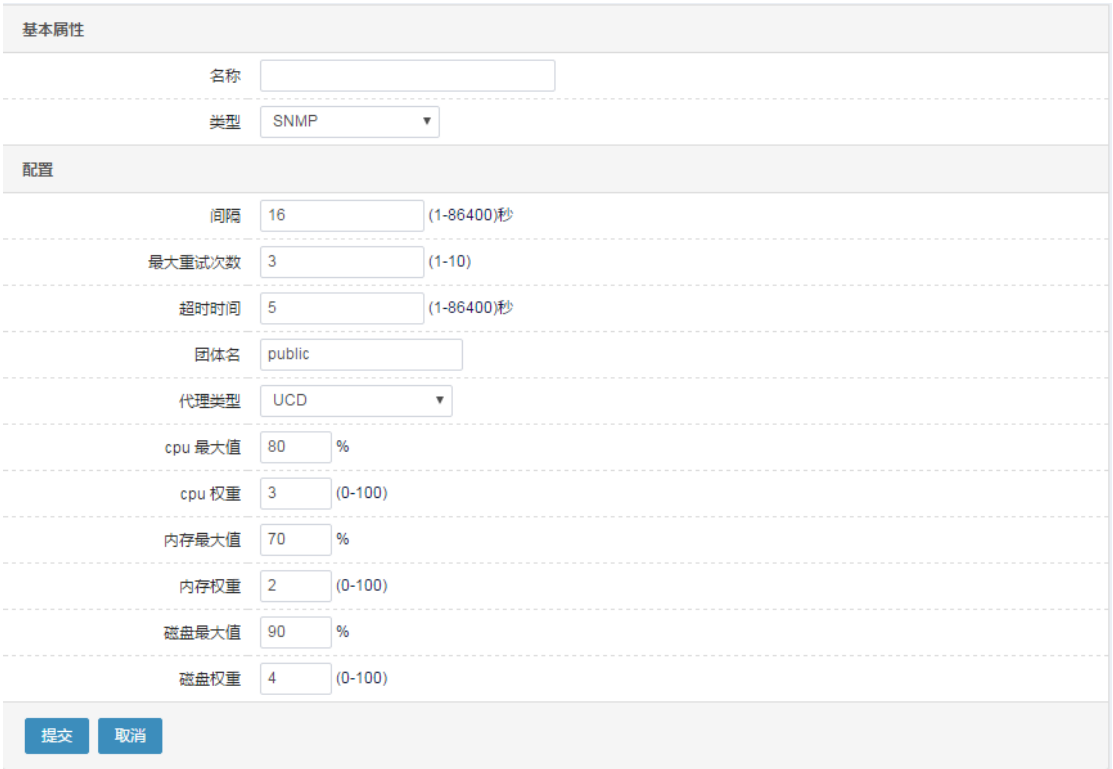
依赖于其他 IP 的主机或链路时填写此项。

覆盖端口：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置。

配置步骤：

1. 输入**间隔**。
2. 输入**最大重试次数**。
3. 输入**超时时间**。
4. 选择输入**发送**内容。
5. 选择输入**接收**内容。
6. 选择输入**用户名。**
7. 选择输入**密码。**
8. 选择**覆盖 IP 地址类型**。
9. 选择输入**覆盖 IP 和覆盖端口**。
10. 点击**提交**。

当类型为 SNMP 时，配置界面如下：



名称：指定新建健康检查模板的名称。

类型：指定新建健康检查模板的协议类型。

间隔：健康检查发送状态探测包的间隔时间，单位为秒。

最大重试次数：健康检查探测包探测失败后的重试次数。例如，默认参数 3 次，如果发送 3 个健康检查状态包都没收到回应或者 3 次都探测失败，则健康检查返回状态为失败的最终结果。

超时时间：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

团体名:SNMP 代理认证的密码。

代理类型：可以选择 UCD(linux)和 windows 两种类型。

cpu 最大值：cpu 使用率阈值，超过此值认为服务器不可用。

cpu 权重：cpu,内存，磁盘三者参与负载计算时所占的权重比例。

内存最大值：内存使用率阈值，超过此值认为服务器不可用。

内存权重：cpu,内存，磁盘三者参与负载计算时所占的权重比例。

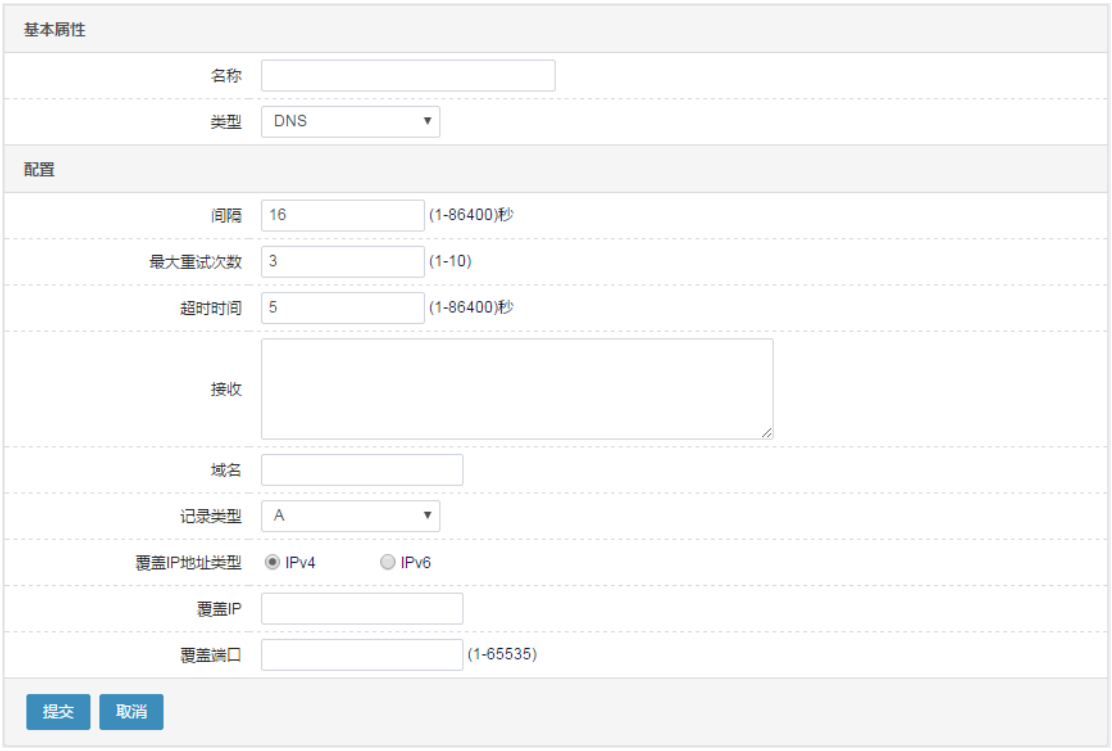
磁盘最大值：磁盘使用率阈值，超过此值认为服务器不可用。

磁盘权重： cpu,内存，磁盘三者参与负载计算时所占的权重比例。

配置步骤：

1. 输入**间隔**。
2. 输入**最大重试次数**。
3. 输入**超时时间**。
4. 输入**团体名。**
5. 选择**代理类型**。
6. 输入 **cpu 最大值**。
7. 输入 **cpu 权重**。
8. 输入**内存最大值**。
9. 输入**内存权重**。
10. 输入**磁盘最大值**。
11. 输入**磁盘权重**。
12. 点击**提交**。

当类型为 DNS 时，配置界面如下：



名称：指定新建健康检查模板的名称。

类型：指定新建健康检查模板的协议类型。

间隔：健康检查发送状态探测包的间隔时间，单位为秒。

最大重试次数：健康检查探测包探测失败后的重试次数。例如，默认参数 3 次，如果发送 3 个健康检查状态包都没收到回应或者 3 次都探测失败，则健康检查返回状态为失败的最终结果。

超时时间：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

接收：接收到报文中应含的内容。当接收到的内容不包含此内容时，则此次健康检查失败。

域名：去 DNS 服务器上解析的域名。

记录类型：选择 DNS 记录类型

覆盖 IP 地址类型：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

覆盖 IP：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机时填写此项。

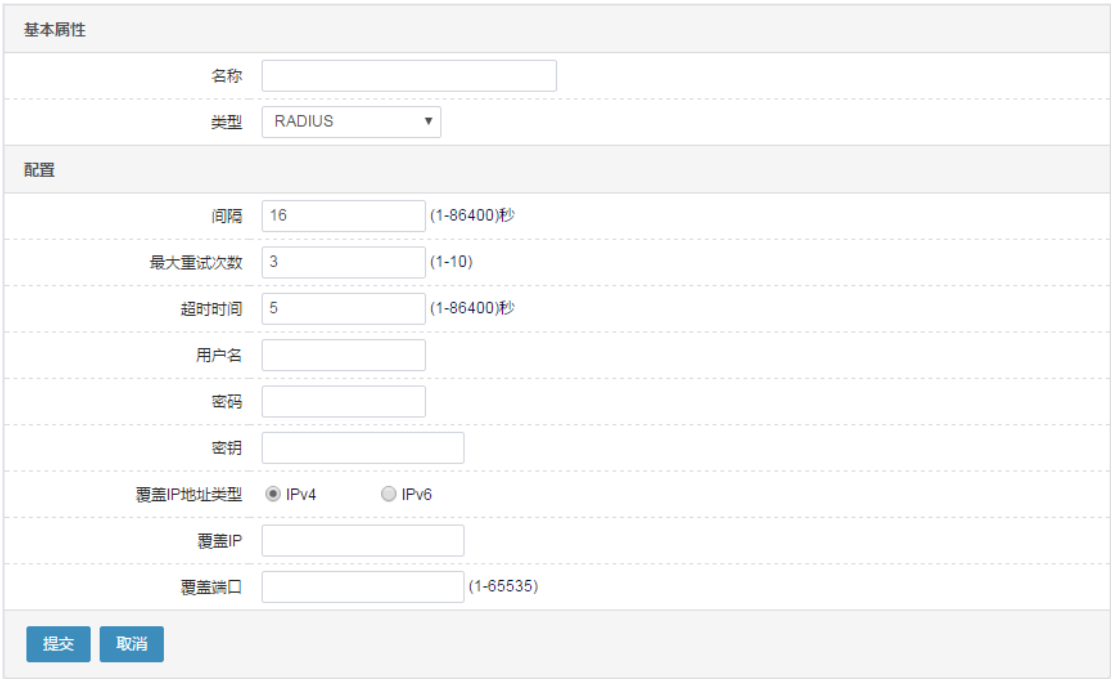
覆盖端口：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置。

配置步骤：

1. 输入**间隔**。

2. 输入**最大重试次数**。
3. 输入**超时时间**。
4. 选择输入**接收**内容。
5. 输入**域名**。
6. 选择**覆盖 IP 地址类型**。
7. 选择输入**覆盖 IP 和覆盖端口**。
8. 点击**提交**。

当类型为 RADIUS 时，配置界面如下：



名称：指定新建健康检查模板的名称。

类型：指定新建健康检查模板的协议类型。

间隔：健康检查发送状态探测包的间隔时间，单位为秒。

最大重试次数：健康检查探测包探测失败后的重试次数。例如，默认参数 3 次，如果发送 3 个健康检查状态包都没收到回应或者 3 次都探测失败，则健康检查返回状态为失败的最终结果。

超时时间：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

用户名：RADIUS 认证用户名称。

密码：RADIUS 用户密码。

密钥：和 RADIUS 服务器的协商密钥。

覆盖 IP 地址类型：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

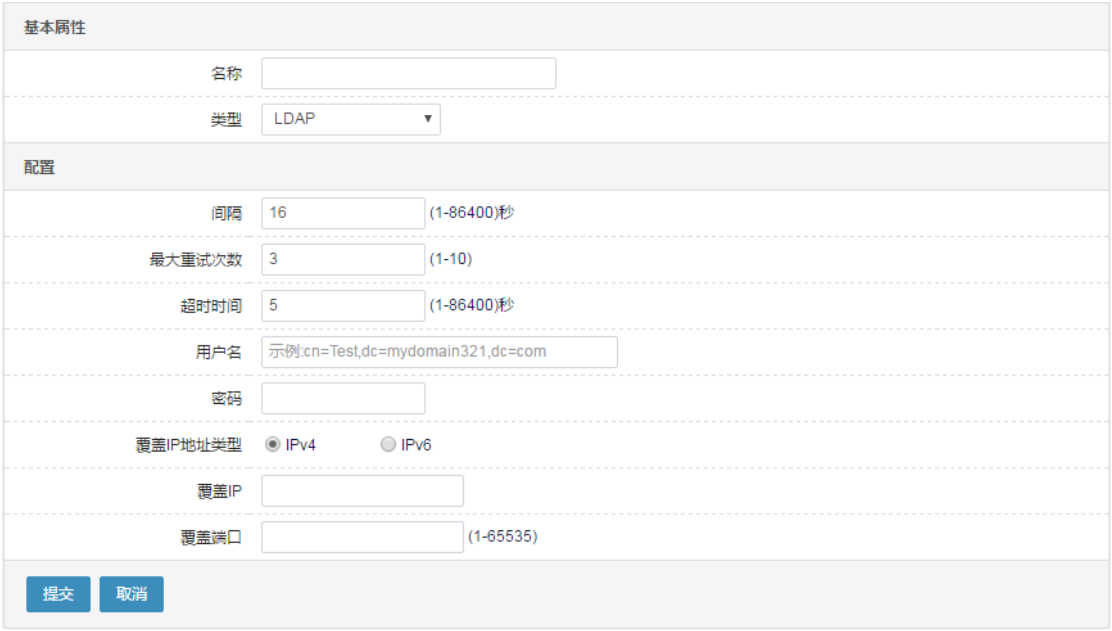
覆盖 IP：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康检查方式的健康状况依赖于其他 IP 的主机或链路时填写此项。

覆盖端口：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置。

配置步骤：

1. 输入**间隔**。
2. 输入**最大重试次数**。
3. 输入**超时时间**。
4. 输入**用户名**。
5. 输入**密码**。
6. 输入**密钥**。
7. 选择**覆盖 IP 地址类型**。
8. 选择输入**覆盖 IP**。
9. 选择输入**覆盖端口**。
10. 点击**提交**。

当类型为 LDAP 时，配置界面如下：



名称：指定新建健康检查模板的名称。

类型：指定新建健康检查模板的协议类型。

间隔：健康检查发送状态探测包的间隔时间，单位为秒。

最大重试次数：健康检查探测包探测失败后的重试次数。例如，默认参数 3 次，如果发送 3 个健康检查状态包都没收到回应或者 3 次都探测失败，则健康检查返回状态为失败的最终结果。

超时时间：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

用户名：LDAP 用户名称。

密码：LDAP 用户密码。

覆盖 IP 地址类型：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

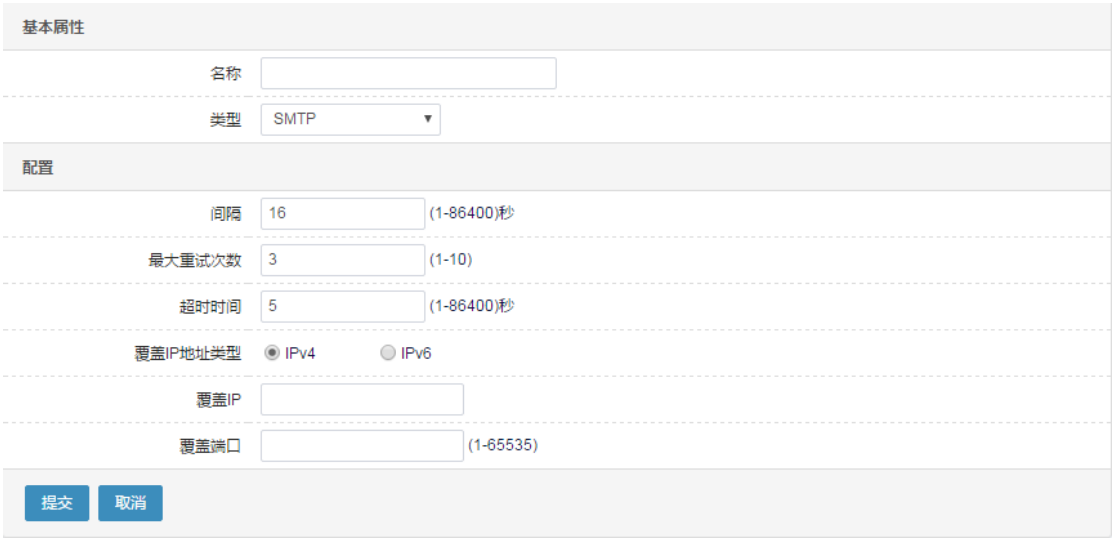
覆盖 IP：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机时填写此项。

覆盖端口：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置。

配置步骤：

1. 输入**间隔**。
2. 输入**最大重试次数**。
3. 输入**超时时间**。
4. 输入**用户名**。
5. 输入**密码**。
6. 选择**覆盖 IP 地址类型**。
7. 选择输入**覆盖 IP**。
8. 选择输入**覆盖端口**。
9. 点击**提交**。

当类型为 SMTP 时，配置界面如下：



名称：指定新建健康检查模板的名称。

类型：指定新建健康检查模板的协议类型。

间隔：健康检查发送状态探测包的间隔时间，单位为秒。

最大重试次数：健康检查探测包探测失败后的重试次数。例如，默认参数 3 次，如果发送 3 个健康检查状态包都没收到回应或者 3 次都探测失败，则健康检查返回状态为失败的最终结果。

超时时间：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

覆盖 IP 地址类型：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

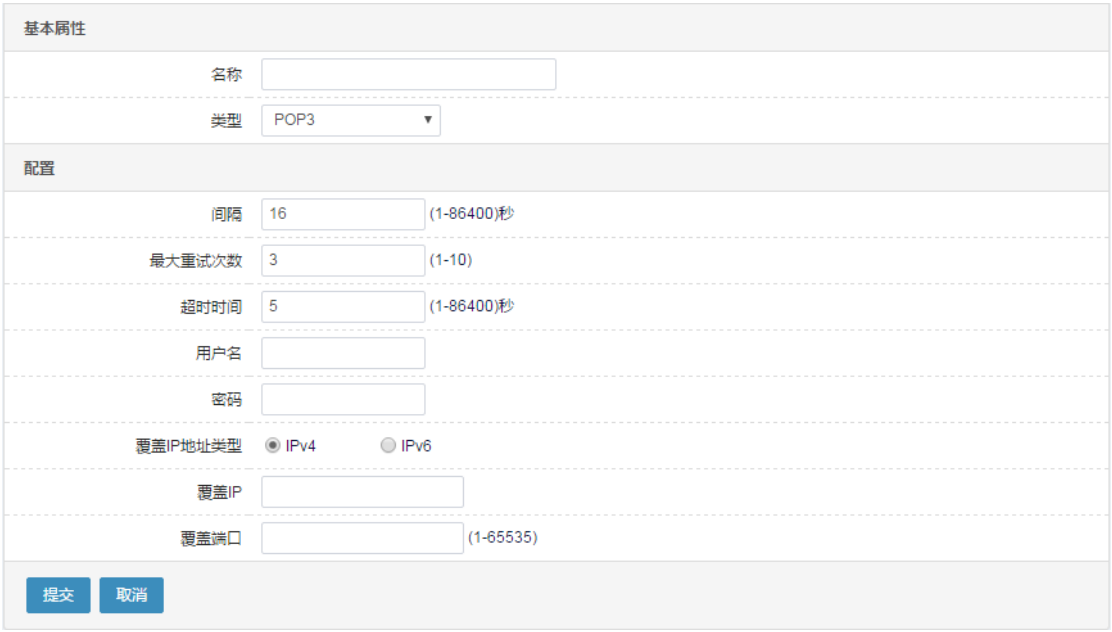
覆盖 IP：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机时填写此项。

覆盖端口：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置。

配置步骤：

1. 输入**间隔**。
2. 输入**最大重试次数**。
3. 输入**超时时间**。
4. 选择**覆盖 IP 地址类型**。
5. 选择输入**覆盖 IP**。
6. 选择输入**覆盖端口**。
7. 点击**提交**。

当类型为 POP3 时，配置界面如下：



名称：指定新建健康检查模板的名称。

类型：指定新建健康检查模板的协议类型。

间隔：健康检查发送状态探测包的间隔时间，单位为秒。

最大重试次数：健康检查探测包探测失败后的重试次数。例如，默认参数 3 次，如果发送 3 个健康检查状态包都没收到回应或者 3 次都探测失败，则健康检查返回状态为失败的最终结果。

超时时间：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

用户名：POP3 用户名。

密码：POP3 用户密码。

覆盖 IP 地址类型：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

覆盖 IP：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机时填写此项。

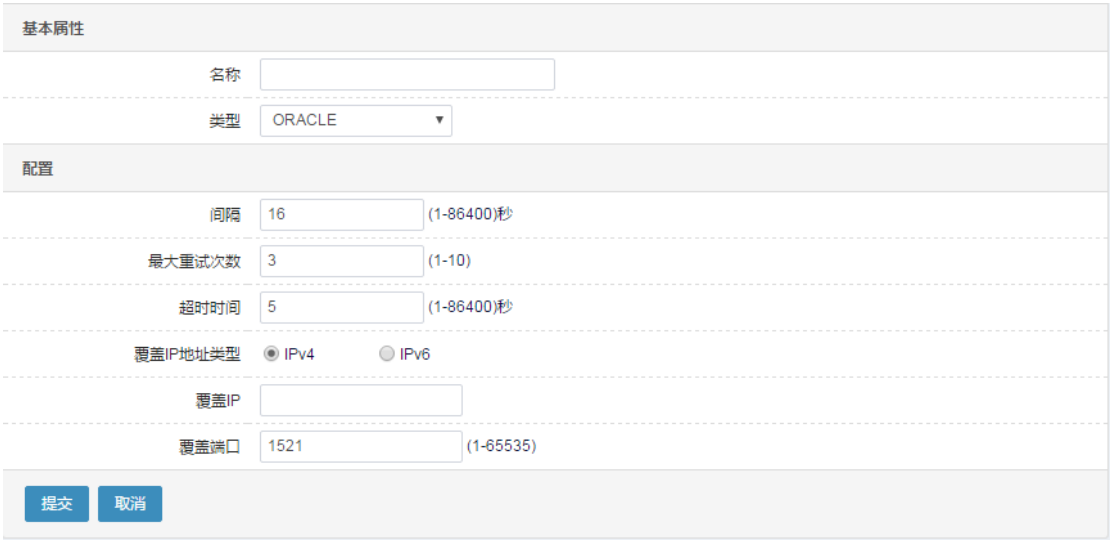
覆盖端口：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置。

配置步骤：

1. 输入**间隔**。
2. 输入**最大重试次数**。
3. 输入**超时时间**。
4. 选择输入**用户名**。

5. 选择输入**密码**。
6. 选择**覆盖 IP 地址类型**。
7. 选择输入**覆盖 IP**。
8. 选择输入**覆盖端口**。
9. 点击**提交**。

当类型为 ORACLE 时，配置界面如下：



名称：指定新建健康检查模板的名称。

类型：指定新建健康检查模板的协议类型。

间隔：健康检查发送状态探测包的间隔时间，单位为秒。

最大重试次数：健康检查探测包探测失败后的重试次数。例如，默认参数 3 次，如果发送 3 个健康检查状态包都没收到回应或者 3 次都探测失败，则健康检查返回状态为失败的最终结果。

超时时间：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

覆盖 IP 地址类型：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

覆盖 IP：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机时填写此项。

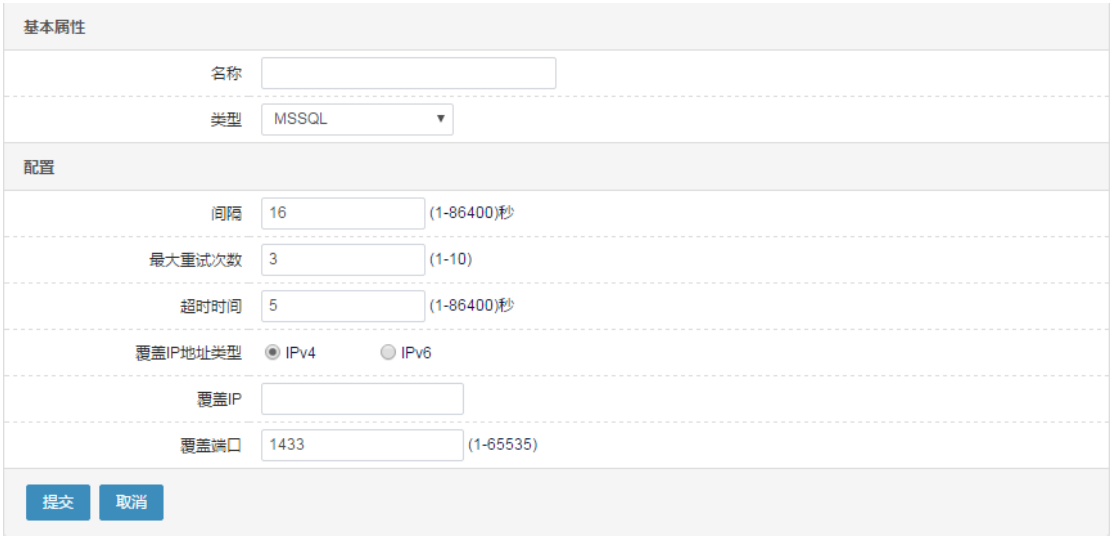
覆盖端口：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置，默认端口 1521。

配置步骤：

1. 输入**间隔**。
2. 输入**最大重试次数**。

3. 输入**超时时间**。
4. 选择**覆盖 IP 地址类型**。
5. 选择输入**覆盖 IP**。
6. 点击**提交**。

当类型为 MSSQL 时，配置界面如下：



名称：指定新建健康检查模板的名称。

类型：指定新建健康检查模板的协议类型。

间隔：健康检查发送状态探测包的间隔时间，单位为秒。

最大重试次数：健康检查探测包探测失败后的重试次数。例如，默认参数 3 次，如果发送 3 个健康检查状态包都没收到回应或者 3 次都探测失败，则健康检查返回状态为失败的最终结果。

超时时间：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

覆盖 IP 地址类型：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

覆盖 IP：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机时填写此项。

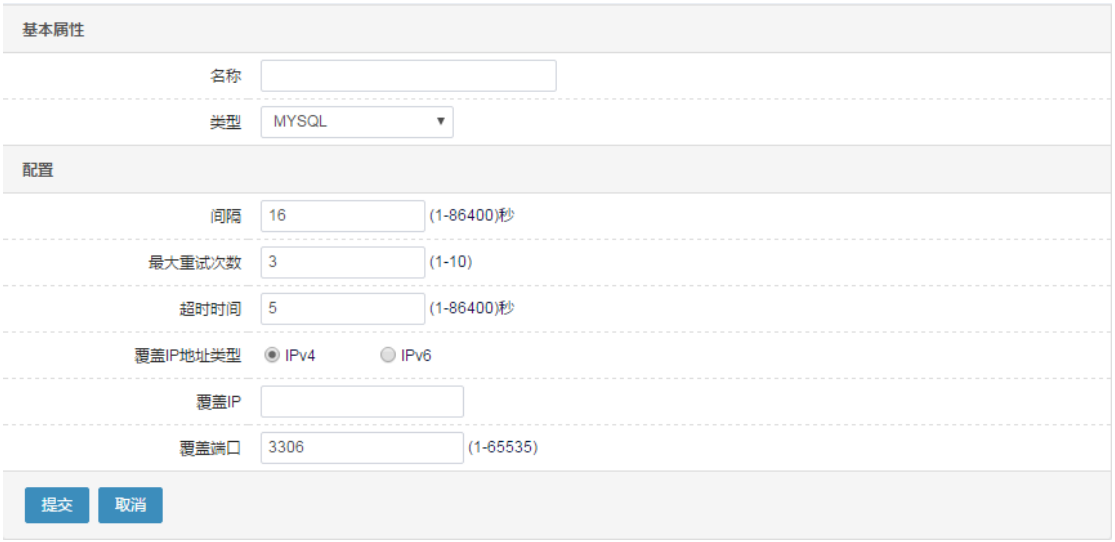
覆盖端口：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置，默认端口 1433。

配置步骤：

1. 输入**间隔**。
2. 输入**最大重试次数**。
3. 输入**超时时间**。

4. 选择**覆盖 IP 地址类型**。
5. 选择输入**覆盖 IP**。
6. 点击**提交**。

当类型为 MYSQL 时，配置界面如下：



名称：指定新建健康检查模板的名称。

类型：指定新建健康检查模板的协议类型。

间隔：健康检查发送状态探测包的间隔时间，单位为秒。

最大重试次数：健康检查探测包探测失败后的重试次数。例如，默认参数 3 次，如果发送 3 个健康检查状态包都没收到回应或者 3 次都探测失败，则健康检查返回状态为失败的最终结果。

超时时间：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

覆盖 IP 地址类型：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

覆盖 IP：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机时填写此项。

覆盖端口：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置，默认端口 3306。

配置步骤：

1. 输入**间隔**。
2. 输入**最大重试次数**。
3. 输入**超时时间**。
4. 选择**覆盖 IP 地址类型**。

5. 选择输入**覆盖 IP**。

6. 点击**提交**。

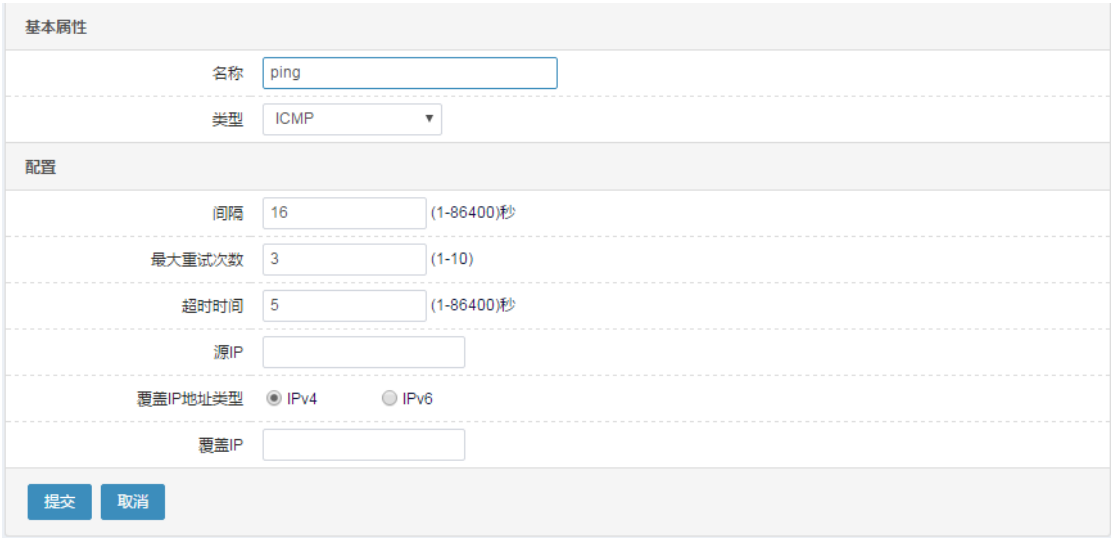
78.3 配置案例

案例描述：

新建一个 ICMP 类型的健康检查模板，然后在策略路由中引用此模板，对下一跳进行探测，返回探测结果显示。

配置步骤：

4. 新建 ICMP 类型的模板：

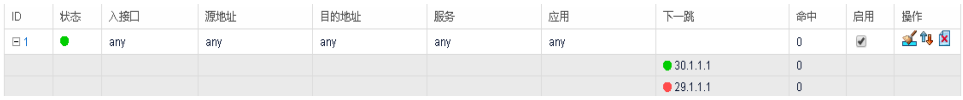


5. 在策略路由中引用该 ICMP 模板：

6. 查看健康检查结果

如下图所示，下一跳 30.1.1.1 可以 ping 通，健康检查成功。下一跳

29.1.1.1 不能 ping 通，健康检查失败。



ID	状态	入接口	源地址	目的地址	服务	应用	下一跳	命中	启用	操作
⊟ 1		any	any	any	any	any		0		
							30.1.1.1	0		
							29.1.1.1	0		

79 第79章 CA 证书

79.1 证书概述

PKI（公钥基础设施）技术采用证书管理公钥，通过第三方的可信任机构--认证中心 CA(Certificate Authority)，把用户的公钥和用户的其他标识信息（如名称、e-mail、身份证号等）捆绑在一起，在 Internet 上验证用户的身份。目前，通用的办法是采用建立在 PKI 基础之上的数字证书，通过把要传输的数字信息进行加密和签名，保证信息传输的机密性、真实性、完整性和不可否认性，从而保证信息的安全传输。

设备上的 PKI 本地证书主要包含三项配置：导入用户证书、导入第三方 CA 证书、导入第三方 CA 的 CRL。这三个功能是相对独立又相互联系，即可以根据具体需要，导入不同的本地证书、不同的 CA 证书、不同的 CRL，但要验证某个终端证书时，需要导入该终端证书的 CA 证书、CRL，以便对该终端证书进行验证。

79.2 配置证书管理

对设备所要使用的客户端证书、第三方 CA 证书、第三方 CRL 进行导入导出配置。

79.2.1 配置通用证书

上传证书配置步骤

1. 进入**对象>CA 证书>本地证书>通用证书**，点击**导入通用证书**

可以选择三种格式的证书上传

导入 PKCS12 格式证书

参数说明：

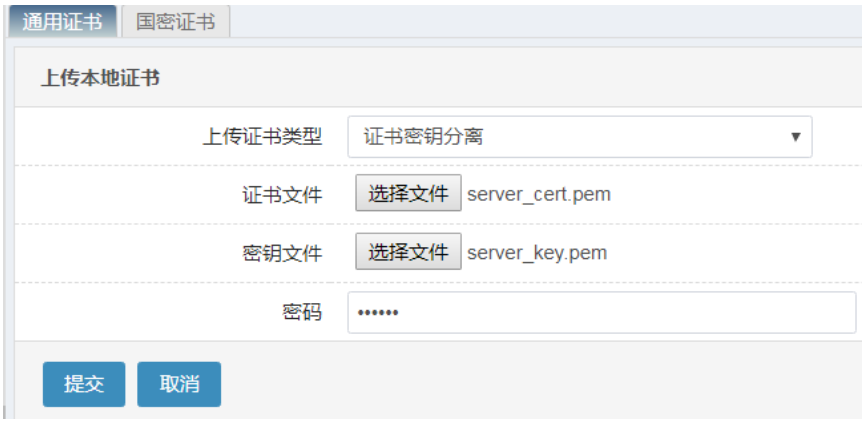
上传证书类型：可选择上传证书的类型，下拉菜单中可选项为 PKCS12 格式、证书密钥分离和证书链三种。

有密钥文件的证书：PKCS12 格式文件的位置。

密码：数字证书的密码。

为保护私钥安全性，导入的 PKCS12 格式证书必须有密码保护。

导入证书密钥分离的证书。



参数说明：

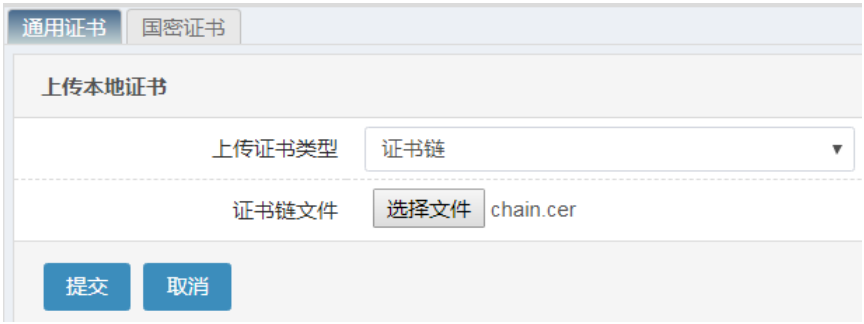
上传证书类型：可选择上传证书的类型，下拉菜单中可选项为 PKCS12 格式、证书密钥分离和证书链三种。

证书文件：数字证书文件位置。

密钥文件：数字证书私钥文件位置。

密码：加密私钥文件使用的密码。

导入证书链。



参数说明：

上传证书类型：可选择上传证书的类型，下拉菜单中可选项为 PKCS12 格

式、证书密钥分离和证书链三种。

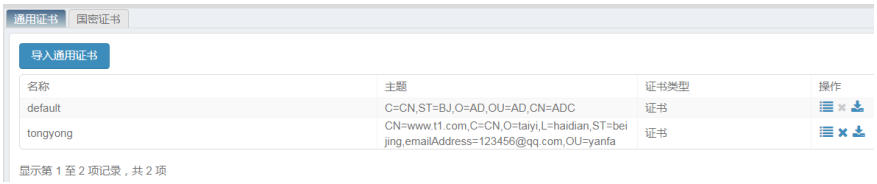
证书链文件：通过浏览本地文件的形式选择待上传的证书链文件。

2. 点击**提交。**

查看证书配置步骤

1. 进入**对象>CA 证书>本地证书>通用证书**

该界面显示已导入的数字证书。



2. 点击 查看某一个证书的具体信息，显示证书详细信息。

参数说明：

主题：证书的主题列表，如果是证书链可以通过下拉框选择多个主题切换证书

证书名称：证书的名称

发行者：证书的发行者

主题：证书的主题

有效起始：证书生效的开始时间

有效终止：证书生效的终止时间

版本：证书的版本号

序列号：证书的序列号

扩展：证书的扩展信息

导出证书配置步骤

1. 进入**对象>CA 证书>本地证书>通用证书**

2. 点击 导出某一个证书，在弹出的窗口选择导出证书存放路径，点确定导出证书。

删除证书配置步骤

1. 进入**对象>CA 证书>本地证书>通用证书**

2. 点击 删除某一个证书。

3. 点击**确认**删除证书。

如果证书之后对应的删除按钮处于灰化状态表示该证书正在被应用或者该证书是默认证书，无法进行删除操作

79.2.2 配置国密证书

上传证书配置步骤

1. 进入**对象>CA 证书>本地证书>国密证书**，点击**导入国密证书**

可以选择两种格式的证书上传

导入 PKCS12 格式证书

参数说明：

上传证书类型：可选择上传证书的类型，下拉菜单中可选项为 PKCS12 格式、证书密钥分离两种。

有密钥文件的证书：通过浏览本地文件的方式选择待上传的 PKCS12 格式国密证书。

密码：数字证书的密码。

为保护私钥安全性，导入的 PKCS12 格式证书必须有密码保护。

导入证书密钥分离的证书。

参数说明：

上传证书类型：可选择上传证书的类型，下拉菜单中可选项为 PKCS12 格式、证书密钥分离两种。

证书文件：通过浏览本地文件的形式选择待上传的证书文件。

密钥文件：通过浏览本地文件的形式选择待上传证书对应的密钥文件。

密码：待上传证书密钥文件的加密密码。

2. 点击**提交。**

查看证书配置步骤

1. 进入**对象>CA 证书>本地证书>国密证书**

该界面显示已导入的数字证书。

2. 点击 查看某一个证书的具体信息，显示证书详细信息。

参数说明：

主题：证书的主题列表，如果是证书链可以通过下拉框选择多个主题切换证书

证书名称：证书的名称

发行者：证书的发行者

主题：证书的主题

有效起始：证书生效的开始时间

有效终止：证书生效的终止时间

版本：证书的版本号

序列号：证书的序列号

扩展：证书的扩展信息

导出证书配置步骤

1. 进入**对象>CA 证书>本地证书>通用证书**

2. 点击 导出某一个证书，在弹出的窗口选择导出证书存放路径，点确定导出证书。

删除证书配置步骤

1. 进入**对象>CA 证书>本地证书>通用证书**
2. 点击 删除某一个证书。
3. 点击**确认**删除证书。

提示

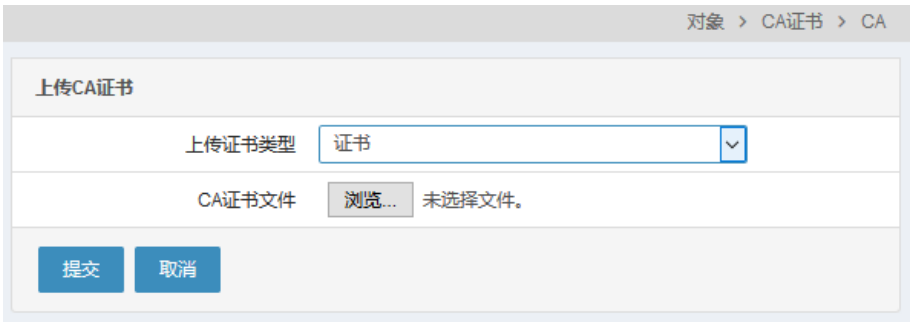
如果证书之后的删除按钮是灰化状态则表示表示该证书正在被引用，无法进行删除操作。

79.2.3 配置CA证书

上传证书配置步骤

1. 进入**对象>CA 证书>CA**，点击**导入 CA 中心证书**，可以选择两种上传 CA 证书的方式。

导入单个 CA 证书

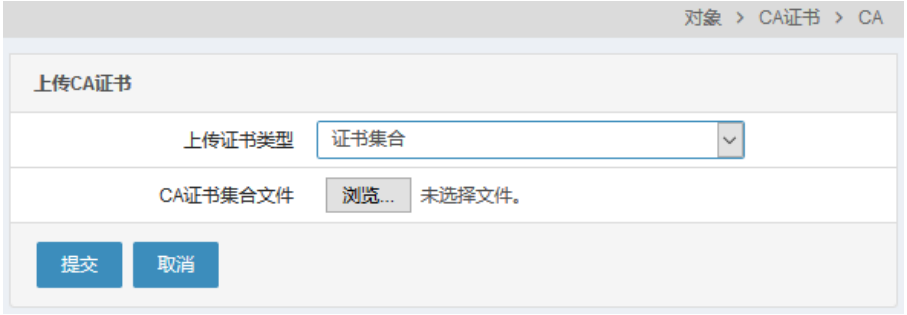


参数说明：

上传证书类型：选择上传 CA 证书的类型，分别为证书以及证书集合

CA 证书文件：要上传的 CA 证书文件位置

导入 CA 证书集合



参数说明：

上传证书类型：选择上传 CA 证书的类型，分别为证书以及证书集合

CA 证书集合文件：要上传的 CA 证书集合文件位置

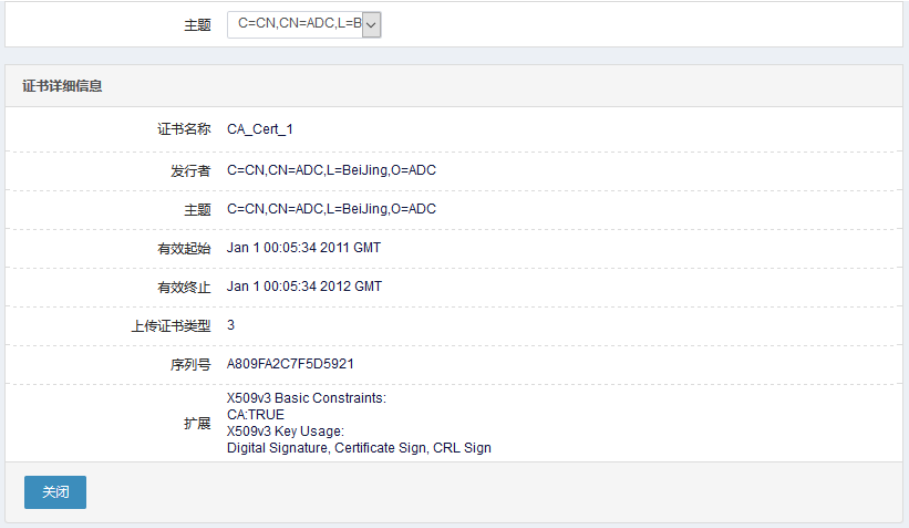
2. 点击**提交**

查看证书配置步骤

1. 进入**对象>CA 证书>CA**

该界面显示已导入的 CA 证书。

2. 点击 查看某一个 CA 证书的具体信息，显示证书详细信息。



参数说明：

主题：证书的主题列表，如果是 CA 证书集合可以通过下拉框在多个主题中选择一个主题来切换证书

证书名称：证书的名称

发行者：证书的发行者

主题：证书的主题

有效起始：证书生效的开始时间

有效终止：证书生效的终止时间

版本：证书的版本号

序列号：证书的序列号

扩展：证书的扩展信息

导出证书配置步骤

1. 进入**对象>CA 证书>CA**

该界面显示已导入的 CA 证书。

2. 点击导出某一个证书，在弹出的窗口选择导出证书存放路径，点击**确定**导出证书。

删除证书配置步骤

1. 进入**对象>CA 证书>CA**

该界面显示全部导入的 CA 证书。

2. 点击删除某一个证书。

3. 点击**确认**删除证书。

提示

删除证书时出现时表明证书正在被引用，无法删除。

79.2.4 配置CRL证书

上传 CRL 配置步骤

1. 进入**对象>CA 证书>CRL**，点击**导入 CRL。**

参数说明：

上传文件：要上传的 CRL 证书文件位置

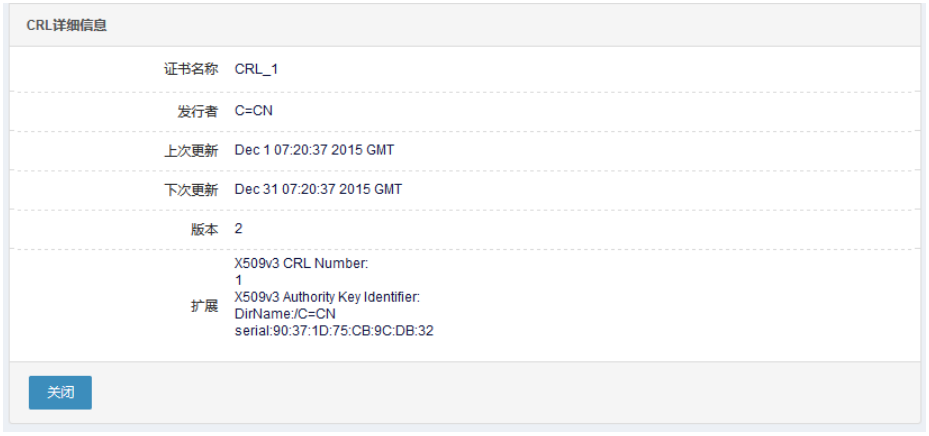
2. 点击**提交。**

查看 CRL 配置步骤

1. 进入**对象>CA 证书>CRL**

该界面显示已导入的 CRL 证书。

2. 点击 查看某一个 CRL 证书的具体信息，显示证书详细信息。



参数说明：

证书名称：证书的名称

发行者：证书的发行者

上次更新：证书上次更新时间

下次更新：证书下次更新时间

版本：证书的版本号

扩展：证书的扩展信息

导出 CRL 配置步骤

1. 进入**对象>CA 证书>CRL**

该界面显示已导入的 CRL 证书。

2. 点击导出某一个 CRL 证书，在弹出的窗口选择导出证书存放路径，点击**确定**导出证书。

删除 CRL 配置步骤

1. 进入**对象>CA 证书>CRL**

该界面显示已导入的 CRL 证书。

2. 点击删除某一个 CRL 证书。

3. 点击**确认**删除证书。

提示

删除证书时出现时表明证书正在被引用，无法删除。

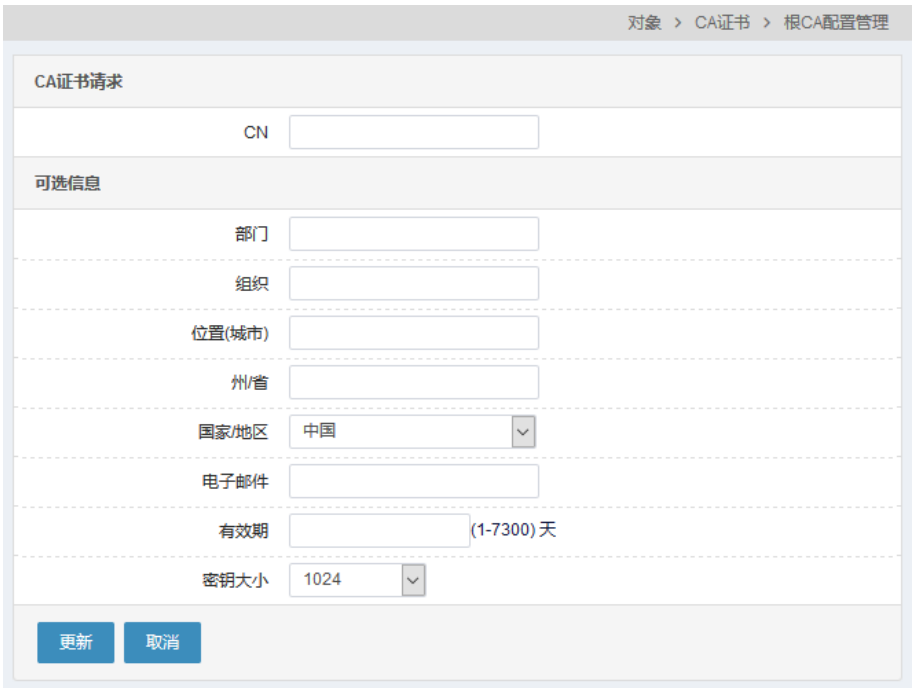
79.2.5 配置管理根CA配置

生成根 CA 配置步骤

1. 进入**对象>CA 证书>根 CA 配置管理**

该界面显示根 CA 配置中心。

2. 点击**生成 CA 根证书**，在弹出的窗口确认覆盖原 CA 根证书，进入 CA 证书请求界面。



参数说明：

CN：证书 common name 信息

部门：证书部门信息

组织：证书组织信息

位置（城市）：证书位置信息

州/省:证书州/省信息

国家/地区：证书国家/地区信息

电子邮件：证书电子邮件信息

有效期：设置证书有效期，范围 1 到 7300 天

密钥大小：设置证书密钥大小，可选 1024bit 和 2048bit 的证书

3. 点击**更新**按钮，生成根 CA 证书。

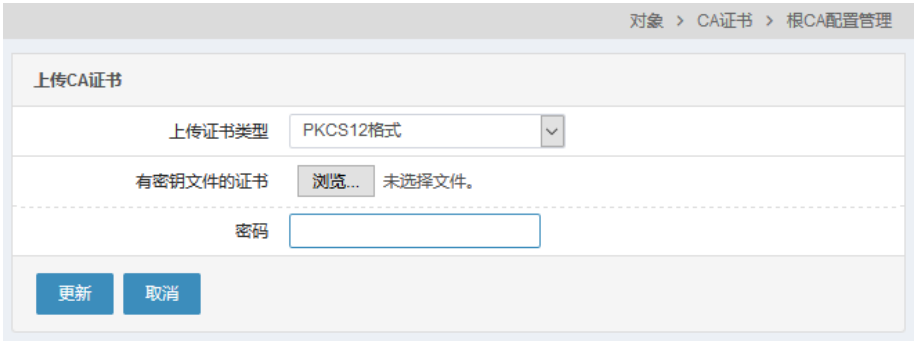
导入根 CA 配置步骤

1. 进入**对象>CA 证书>根 CA 配置管理**

该界面显示根 CA 配置中心。

2. 点击**导入 CA 根证书**， 在弹出的窗口确认覆盖原 CA 根证书，进入证书导入界面，导入方式分为 PKCS12 格式和证书密钥分离两种。

导入 PKCS12 格式根 CA 证书的界面。



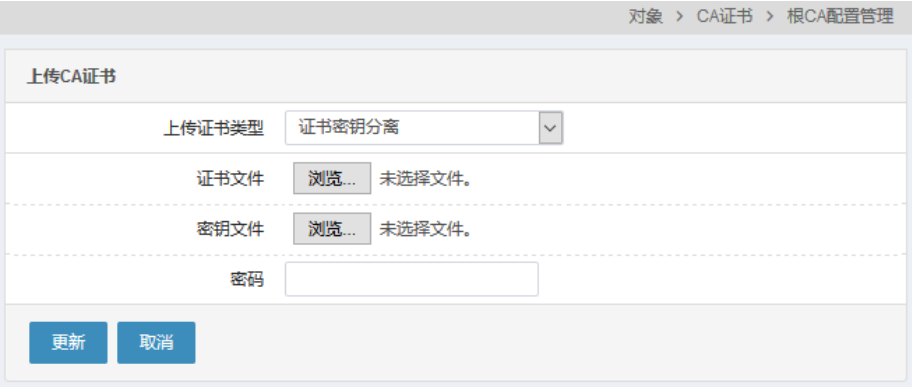
参数说明：

上传证书类型：选择导入 CA 根证书的类型，可选择 PKCS12 格式和证书密钥分离两种。

有密钥文件的证书：点击选择证书文件存放的位置。

密码：配置证书文件的密码。

导入证书密钥分离格式根 CA 证书的界面。



参数说明：

上传证书类型：选择导入 CA 根证书的类型，可选择 PKCS12 格式和证书密钥分离两种。

证书文件：点击选择证书文件存放的位置。

密钥文件：点击选择密钥文件存放的位置。

密码：配置密钥文件的密码。

3. 点击**更新**按钮，完成根 CA 证书上传。

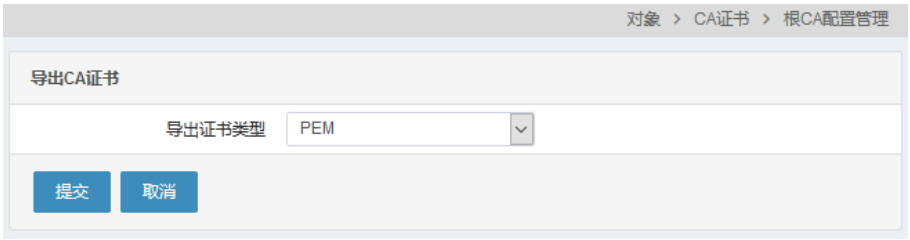
导出根 CA 配置步骤

1. 进入**对象>CA 证书>根 CA 配置管理**

该界面显示根 CA 配置中心。

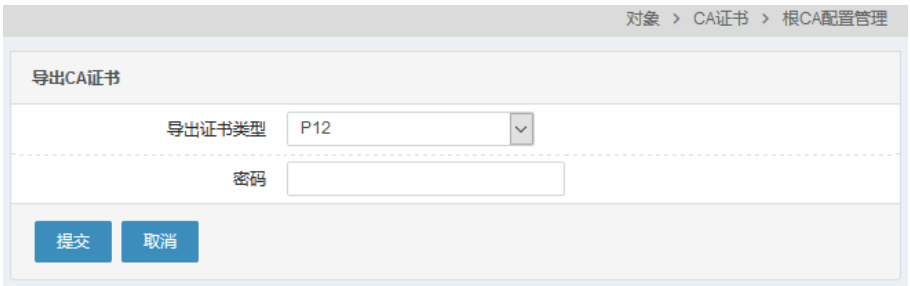
2. 点击**导出 CA 根证书**，进入根 CA 证书导出界面，可以选择导出为 PEM 格式和 P12 格式两种类型的 CA 证书。其中 PEM 格式证书不包含密钥文件。

导出为 PEM 格式证书的界面。



参数说明：

导出证书类型：选择导出证书的类型，可选择 PEM 格式和 P12 格式两种导出为 P12 格式证书的界面。



参数说明：

导出证书类型：选择导出证书的类型，可选择 PEM 格式和 P12 格式两种。

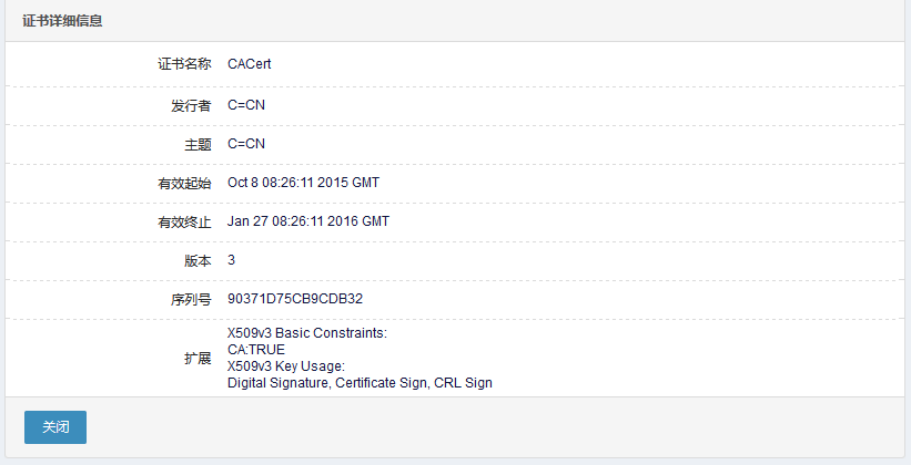
密码：设置导出后 P12 证书的密码。

查看根 CA 配置步骤

1. 进入**对象>CA 证书>根 CA 配置管理**

该界面显示根 CA 配置中心。

2. 点击**查看 CA 根证书**，查看 CA 根证书。



参数说明：

证书名称：证书的名称

发行者：证书的发行者

主题：证书的主题

有效起始：证书生效的开始时间

有效终止：证书生效的终止时间

版本：证书的版本号

序列号：证书的序列号

扩展：证书的扩展信息

管理根 CA 的 CRL 配置步骤

1. 进入**对象>CA 证书>根 CA 配置管理**

该界面显示根 CA 配置中心。

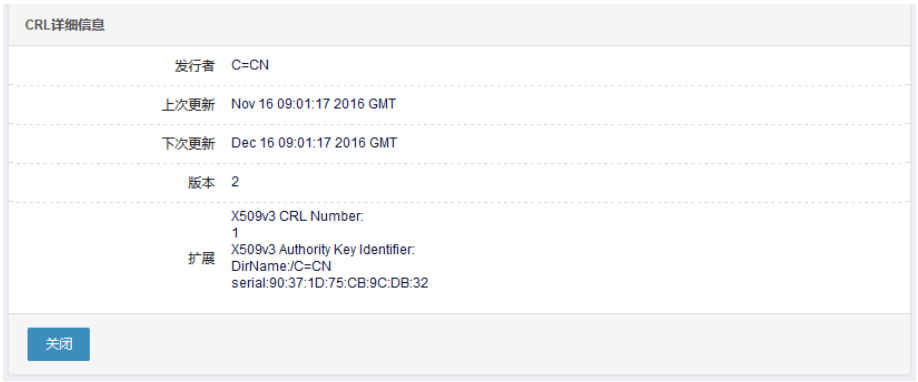
在 CRL 管理一栏，可以对 CRL 自动更新周期进行配置，CRL 周期配置范围为 1-30 天

查看 CRL 详细信息配置步骤

1. 进入**对象>CA 证书>根 CA 配置管理。**

该界面显示根 CA 配置中心。

在 CRL 一栏，点击 查看 CRL 详细信息。



参数说明：

发行者：证书的发行者

上次更新：证书上次更新时间

下次更新：证书下次更新时间

版本：证书的版本号

扩展：证书的扩展信息

导出 CRL 配置步骤

1. 进入**对象>CA 证书>根 CA 配置管理**

该界面显示根 CA 配置中心。

在 CRL 一栏，点击导出 CRL 文件。

更新 CRL 配置步骤

1. 进入**对象>CA 证书>根 CA 配置管理**

该界面显示根 CA 配置中心。

在 CRL 一栏，点击手动更新 CRL。

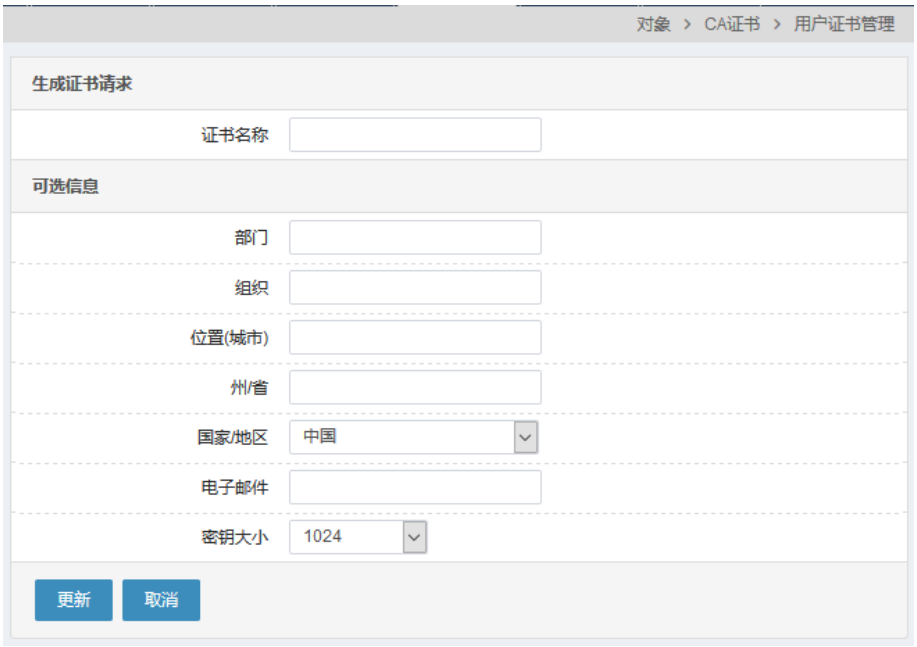
79.2.6 配置管理用户证书

生成用户证书请求步骤

1. 进入**对象>CA 证书>用户证书管理**

该界面显示用户证书列表。

2. 点击**生成证书请求**，进入证书请求配置页面。



参数说明：

证书名称：配置证书的 CN 信息

密码：数字证书的密码

确认密码：数字证书的密码

部门：配置证书的部门信息

组织：配置证书的组织信息

位置（城市）：配置证书的位置信息

州/省：配置证书的州/省信息

国家/地区：配置证书的国家/地区信息

通用名称（域名）：证书通用名称（域名）

电子邮件：配置证书的电子邮件信息

密钥大小：配置证书的密钥大小，可以选择 1024bit 或者 2048bit 的证书

3. 点击**更新**，生成证书请求。

签发用户证书步骤

1. 进入**对象>CA 证书>用户证书管理**

该界面显示用户证书列表。

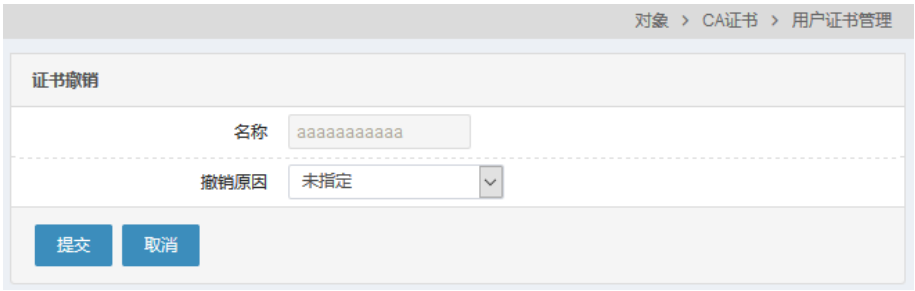
选择系统状态为未签发的用户证书请求，点击  图标对证书请求进行签发。

吊销用户证书步骤

1. 进入**对象>CA 证书>用户证书管理**

该界面显示用户证书列表。

选择系统状态为正常的用户证书，点击  图标对证书进行吊销，进入证书吊销界面。



参数说明：

撤销原因：配置证书的吊销原因，可选择未指定、密钥泄露、CA 密钥泄露和附属关系改变四种。

2. 点击**提交**，完成对证书的吊销。

删除用户证书步骤

1. 进入**对象>CA 证书>用户证书管理**

该界面显示用户证书列表。

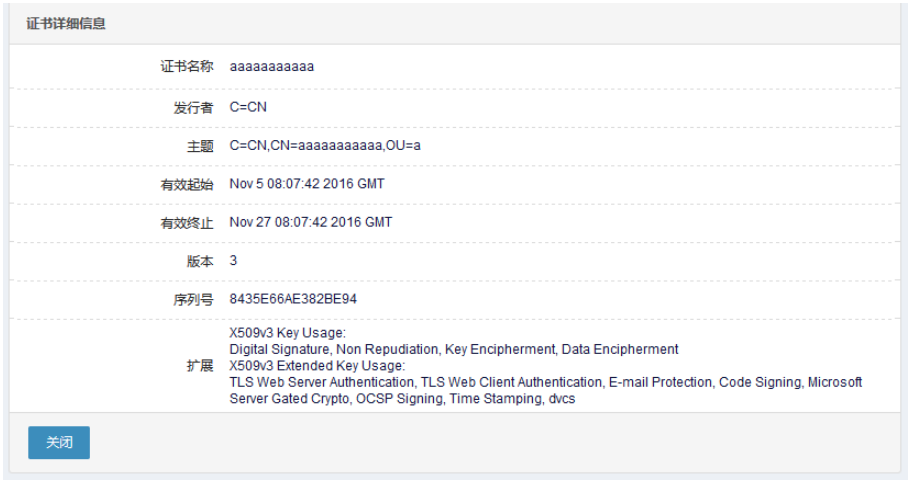
点击  图标删除证书或者证书请求。

查看用户证书信息步骤

1. 进入**对象>CA 证书>用户证书管理**

该界面显示用户证书列表。

点击  图标查看证书或者证书请求详细信息。



参数说明：

证书名称：证书的名称

发行者：证书的发行者

主题：证书的主题

有效起始：证书生效的开始时间

有效终止：证书生效的终止时间

版本：证书的版本号

序列号：证书的序列号

扩展：证书的扩展信息

导出用户证书步骤

1. 进入**对象>CA 证书>用户证书管理**

该界面显示用户证书列表。

选择系统状态为正常的证书，点击图标导出证书。

79.3 配置案例

案例描述：

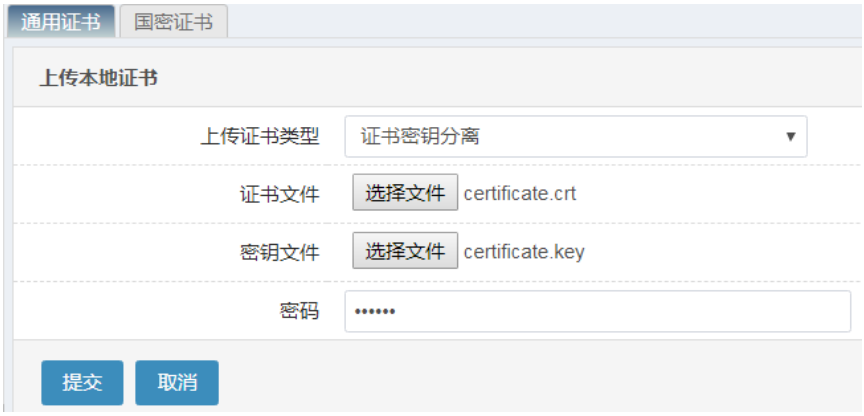
上传本地证书以及对应的证书链。本地证书由中间 CA 签发，中间 CA 由根 CA 签发。

配置方法：

为了能让证书被根 CA 认证，我们需要上传数字证书(certificate)，以及一个证书链(ROOT CA + Intermediate CA)。

配置步骤：

1. 获取 ROOT CA 和 Intermediate CA 证书，并根据这两个证书制作出证书链。
2. 进入**对象>CA 证书>本地证书>通用证书**。
3. 点击**导入通用证书**，根据 certificate 的格式导入本地证书。



4. 进入**对象>CA 证书>CA**。

5. 点击**导入 CA 中心证书**，将制作好的证书链文件导入到 CA 中。

79.4 常见故障

79.4.1 导入证书链失败

现象	导入证书链失败。
分析	1、证书链制作错误；2、证书链没有包含根CA。
解决	1、 检查各级证书链是否能够验证。 2、 证书链应当包含根 CA。

80 第80章 日志管理

80.1 日志概述

T 系列防火墙设备上的日志展示一共分为七大类，包括系统事件、审计事件、VPN 事件、配置审计、SDWAN 事件、流事件和安全事件。本设备支持标准的 SYSLOG 格式，包括本地日志，以及 E-mail 日志，提供给用户掌握系统运行状况的方法。

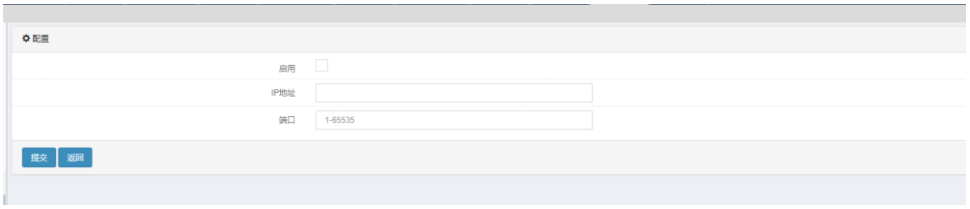
80.2 配置说明

80.2.1 缺省配置说明

内容	缺省设置	备注
本地日志过滤	关闭	可更改设置
E-Mail日志过滤	关闭	可更改设置
SYSLOG日志过滤	关闭	可更改设置
SYSLOG服务器	关闭	可更改设置
SYSLOG服务端口	514	可更改设置

80.2.2 配置SYSLOG服务器

进入**日志>日志管理>日志服务器，点击新建**，如下图：



参数说明：

启用：选中表示启用，不选表示关闭。

IP 地址：Syslog 服务器地址。

端口：Syslog 服务器端口。

一共可以配置 8 个服务器，表示可以同时将日志发送到数个不同的 Syslog 服务器，且之间互不影响。

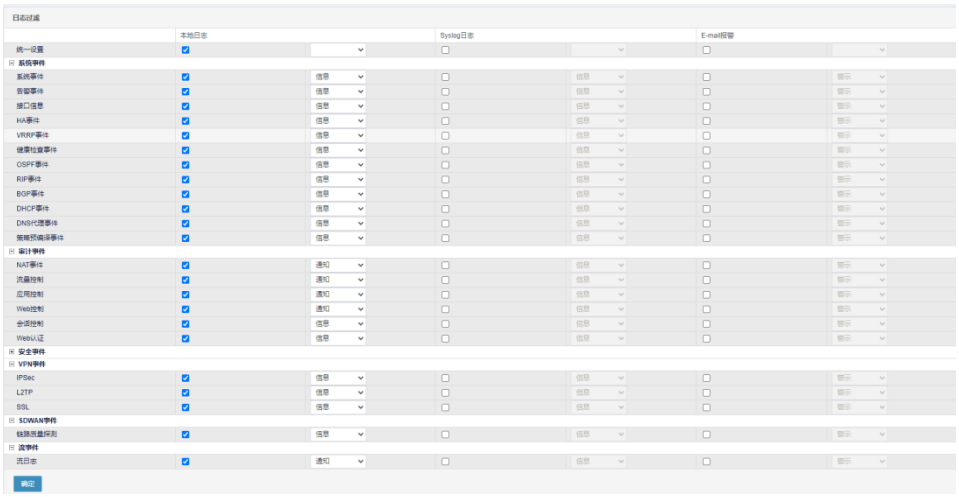
配置步骤：

1. 填写 SYSLOG 服务器地址。
2. 填写服务器端口。

3. 选择**启用**服务器。
4. 点击**提交**。

80.3 配置日志过滤

进入**日志>日志管理>日志过滤**，如下图：



参数说明：

模块名称：各模块对应的名称。

本地日志：是否启用本地日志及其级别。

Syslog 日志：是否启用 Syslog 日志及其级别。

E-mail 日志：是否启用 E-mail 日志及其级别。

配置步骤：

1. 选择对应模块，启用本地日志及其级别。
2. 选择对应模块，启用 Syslog 日志及其级别。
3. 选择对应模块，启用 E-mail 日志及其级别。
4. 点击**确定**。

提示

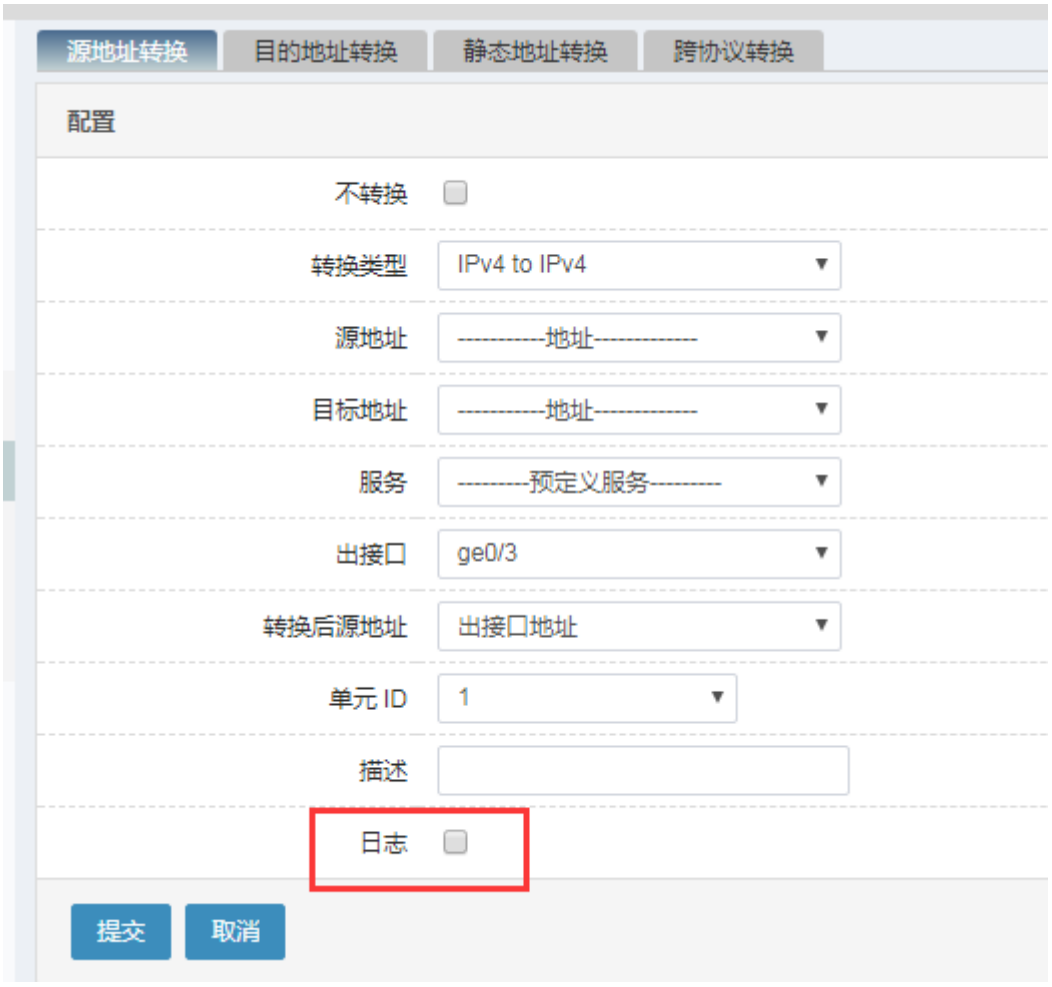
1.**日志过滤**中只对大于或等于该级别的日志有效。

2.**日志过滤**中涉及到的日志模块只是发送日志模块的一部分。

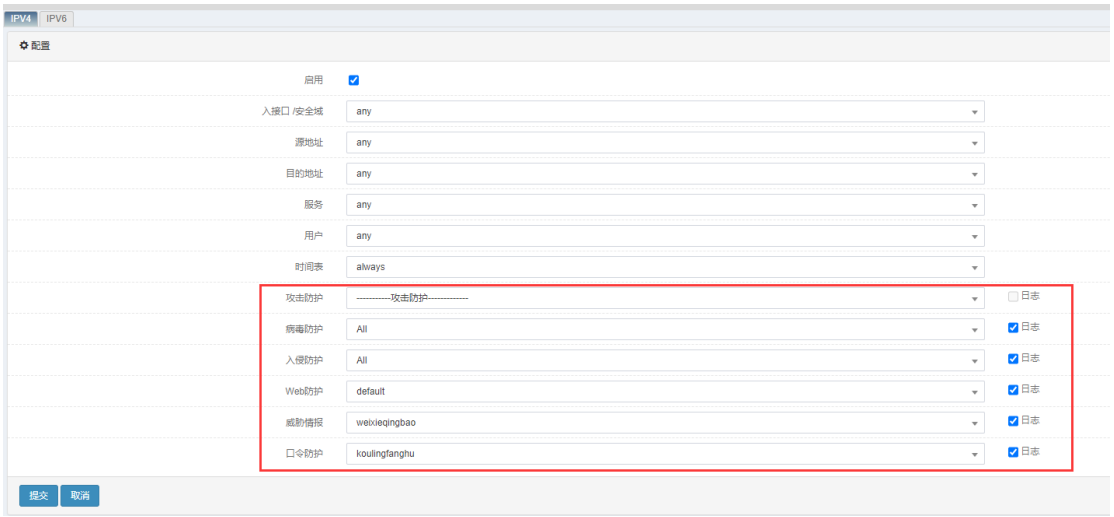
80.4 部分模块日志配置的注意事项

部分模块只是在日志过滤里面打钩后还是无法产生日志，必须在模块内部开启日志：

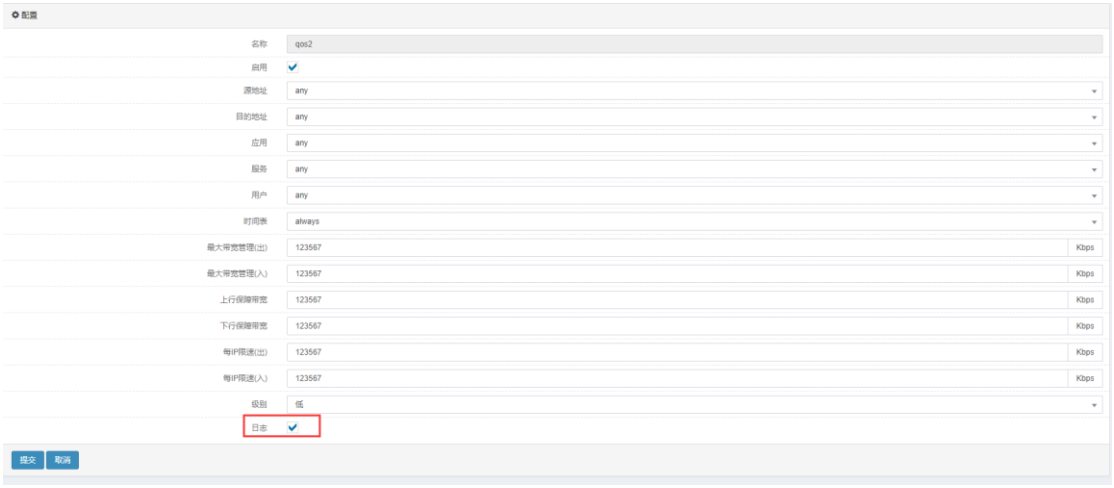
NAT（信息级别）：日志过滤中开启 NAT 日志，并且为信息级别才能够上报，并且需要在具体的 NAT 配置中开启 LOG，如下图：



攻击防护、病毒防护、入侵防护、web 防护、威胁情报、口令防护：需要在防护策略里面开启 LOG



QOS 策略（流控策略）：需要在配置策略的时候开启 LOG



应用控制、web 控制和会话控制都需要内部开启 LOG

80.5 监控与维护

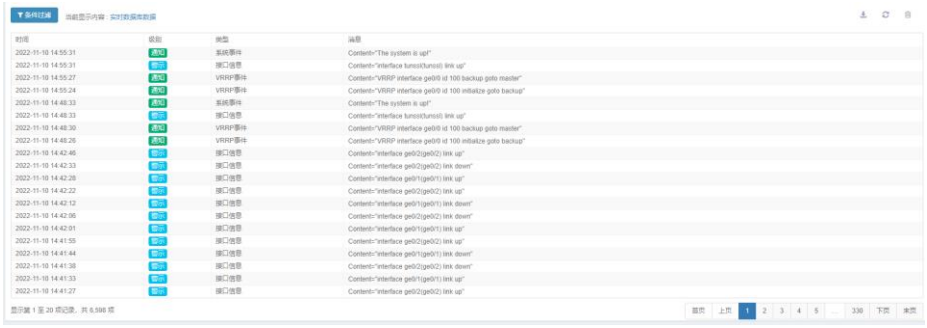
80.5.1 日志查看

T 系列防火墙设备上的日志展示一共分为七大类，包括**系统日志、审计日志、安全日志、VPN 日志、SDWAN 日志、流日志和配置审计**，其中系统日志包括系统事件和网络服务，审计日志包括 NAT 事件、流量控制、应用控制、Web 控制、会话控制和 Web 认证，安全日志包括防火墙策略、本地安全策略和攻击防护，其中攻击防护包括 14 类攻击日志：WEB 应用防护、防 Flood 攻击、防扫描、病毒防护、入侵防护、Web 防护、威胁情报、防 Dos 攻击、防 ARP 攻击、IP 黑名单、域名黑名单、白名单、口令防护和资产防护。SDWAN 日志包括链路质量探测。要查看对应分类的日志内容，需要在**日志**下选择对应分类，进入对应分类页签后，还可以根据“**条件过滤**”功能选择具体的日志模块、日志级别、日志产生时段、消息等进行日志的精确显示。

配置审计的日志内容和日志配置只能在 audit 审计用户下查看和操作。

系统日志、审计日志、安全日志、VPN 日志、SDWAN 日志、流日志和**配置审计**七大类下所展示的日志功能和日志格式没有区别，下面仅以**系统事件**类别的日志为代表进行说明。

进入**日志>系统日志>系统事件**，如下图：



参数说明：

时间：该日志消息的产生时间。

级别：该日志消息的级别。

类型：该日志消息的模块类型。

消息：该日志消息的具体内容。

条目统计：统计当前类别中所展示出的日志条数。

点击 ：可以将日志导出到 txt、xml，csv 三种格式中。(未过滤和过滤过的日志都可以正常导出)

点击 ：刷新日志消息。

点击 ：清空当前类别所有日志消息。

点击 条件过滤 ：设置过滤条件，详细配置参考“条件设置”。

提示

1. 对日志进行分类，分为七大类：系统事件、审计事件、安全事件、VPN 事件、SDWAN 事件、流事件、配置审计。审计事件、VPN 事件、配置审计、安全事件类别下的日志配置参考系统事件类别日志操作。
2. **配置审计日志**只有 audit 用户可以配置查看。

80.5.2 日志查询条件设置

在日志显示页面，可以通过**条件过滤**，来显示相应条件的日志。不设置条件时，默认显示所有日志。当配置有条件设置，如果需要取消所有条件，点击**重置**。

进入**日志>系统日志>系统事件**点击**条件过滤**，如下图：

类型：选择需要查看的日志模块。

级别：选择需要显示的日志级别。默认为所有，表示显示所有级别日志，选择具体级别时，会仅显示所选级别日志。

源 IP：触发日志的源 IP。可输入具体 ip 地址，也可输入带掩码的网段地址。

目的 IP：触发日志的目的 IP。可输入具体 ip 地址，也可输入带掩码的网段地址。

时间：日志产生的时间段。

消息：日志内容过滤。

配置步骤：

1. 选择对应**类型**。
2. 选择**级别**。
3. 选择**源 IP**。
4. 选择**目的 IP**。
5. 选择日志**时间**段。
6. 配置**消息**内容。
7. 点击**确定。**

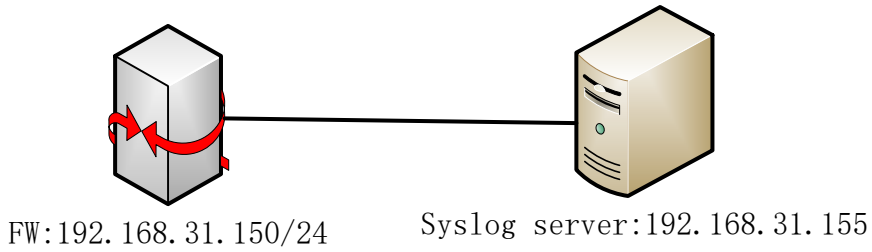
80.6 配置案例

80.6.1 配置案例：配置健康检查模块SYSLOG日志

案例描述：

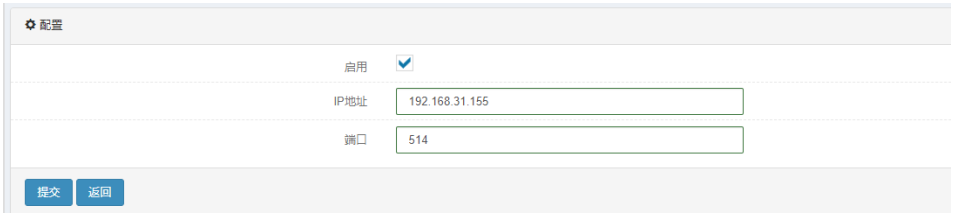
配置健康检查模块发送到日志服务器。

案例组网图：



配置步骤：

1. 进入**日志>日志管理>日志服务器：**



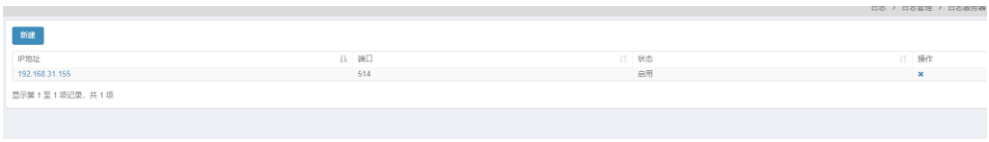
设置配置参数

IP 地址：Syslog 服务器地址为”192.168.31.155”。

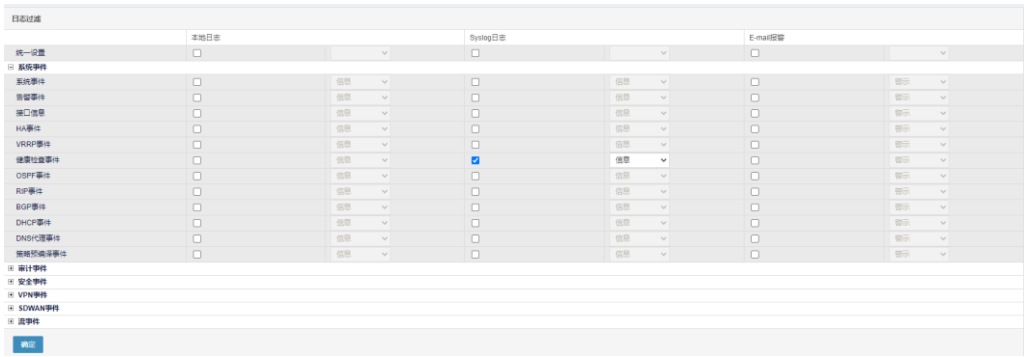
端口：Syslog 服务器端口为”514”。

启用：选中表示启用

2. 点击**提交**完成设置。



3. 进入**日志>日志过滤：**



4. 设置参数。

点击**确定**完成设置。

进行健康检查相关操作后，在 Syslog 服务器上能够看到健康检查模块产生的日志信息。

80.7 常见故障分析

80.7.1 故障现象1：SYSLOG日志失效

现象	在SYSLOG服务器上看不到对应模块日志
分析	1. 是否正确配置SYLOG服务器的地址和端口号 2. 是否指定模块的日志类别和等级到SYSLOG Server
解决	1. 正确配置SYSLOG服务器的地址和端口号 2. 指定模块的日志类别和等级到SYSLOG Server

80.7.2 故障现象2：E-mail日志失效

现象	没有收到对应模块日志信息的邮件
分析	1. 是否正确配置告警邮件配置参数 2. 是否启用对应模块发送E-mail日志 3. 所产生的日志级别是否满足发送E-email告警要求（警示及以上级别）
解决	1. 正确配置告警邮件配置参数，以及发送邮件需要的路由和dns配置，保证告警邮件功能中的测试邮件能够发送成功 2. 启用对应模块发送E-mail日志 3. 保证所需要发送E-mail告警日志的模块产生的日志是警示或以上级别。如果无法产生对应级别日志，则无法邮件告警。

81 第81章 日志合并

81.1 日志合并概述

T 系列防火墙设备上的日志展示一共分为四大类，包括系统事件、审计事件、配置审计和安全事件。有些模块在短时间内会产生大量相同的日志，不利于用户去查看，对此，对此类日志可以按源 IP 与目的 IP 进行合并。

可以进行合并的日志包括：流量控制，防 DOS 攻击，防火墙策略，防扫描，防 flood 攻击，本地安全策略以及黑名单。合并周期默认 60 秒。

81.2 配置日志合并

进入**日志>日志管理>日志合并**，如下图：

参数说明：

全局启用日志合并：日志合并开关。

合并周期：多少秒进行一次日志合并，默认 60 秒。

流量控制：流量控制日志合并开关。

防 DOS 攻击：防 DOS 攻击日志合并开关。

防火墙：防火墙策略日志合并开关。

防扫描：防扫描日志合并开关。

防 Flood 攻击：防 Flood 攻击日志合并开关。

本地安全策略：本地安全策略日志合并开关。

黑名单：黑名单日志合并开关。

点击**提交**。

配置步骤：

5. 勾选全局启用日志合并开关。
6. 配置合并周期。
7. 选择要合并的日志模块。
8. 点击确定。

注意

1、 开启日志合并后会依据选择的类型，若类型（源 IP、目的 IP、源+目的 IP）相同，匹配的策略 ID 相同（若策略存在 ID），匹配的策略动作相同（若策略存在动作）则会合并为同一条日志，在日志上报周期时间内都会合并为同一条日志，仅增加日志合并次数。

2、 当配置类型为源 IP 时，若日志进行了日志合并，目的 IP 字段会变为 merged，表示这条日志依据源 IP 进行了日志合并，目的 IP 地址进行了合并。（目的 IP 类型时，合并日志源 IP 字段为 merged）

81.3 配置案例

81.3.1 配置案例：配置防火墙策略日志合并

配置步骤：

1. 进入**日志>日志管理>日志合并**：

2. 查看防火墙策略日志合并结果。

时间	级别	类型	合并次数	消息
2021-06-18 16:31:23	信息	防火墙策略	342	SrcIP=merged DstIP=200.1.1.10 Protocol=TCP SrcPort=16896 DstPort=8090 PolicyID=2 Action=PERMIT Content="Session Setup"
2021-06-18 16:31:03	信息	防火墙策略	480	SrcIP=merged DstIP=200.1.1.10 Protocol=TCP SrcPort=16896 DstPort=8090 PolicyID=2 Action=PERMIT Content="Session Setup"
2021-06-18 16:30:43	信息	防火墙策略	463	SrcIP=merged DstIP=200.1.1.10 Protocol=TCP SrcPort=16896 DstPort=8090 PolicyID=2 Action=PERMIT Content="Session Setup"
2021-06-18 16:30:23	信息	防火墙策略	461	SrcIP=merged DstIP=200.1.1.10 Protocol=TCP SrcPort=16896 DstPort=8090 PolicyID=2 Action=PERMIT Content="Session Setup"
2021-06-18 16:30:03	信息	防火墙策略	475	SrcIP=merged DstIP=200.1.1.10 Protocol=TCP SrcPort=16896 DstPort=8090 PolicyID=2 Action=PERMIT Content="Session Setup"
2021-06-18 16:29:43	信息	防火墙策略	465	SrcIP=merged DstIP=200.1.1.10 Protocol=TCP SrcPort=16896 DstPort=8090 PolicyID=2 Action=PERMIT Content="Session Setup"
2021-06-18 16:29:23	信息	防火墙策略	471	SrcIP=merged DstIP=200.1.1.10 Protocol=TCP SrcPort=16896 DstPort=8090 PolicyID=2 Action=PERMIT Content="Session Setup"
2021-06-18 16:29:03	信息	防火墙策略	473	SrcIP=merged DstIP=200.1.1.10 Protocol=TCP SrcPort=16896 DstPort=8090 PolicyID=2 Action=PERMIT Content="Session Setup"
2021-06-18 16:28:44	信息	防火墙策略	457	SrcIP=merged DstIP=200.1.1.10 Protocol=TCP SrcPort=16896 DstPort=8090 PolicyID=2 Action=PERMIT Content="Session Setup"
2021-06-18 16:28:23	信息	防火墙策略	477	SrcIP=merged DstIP=200.1.1.10 Protocol=TCP SrcPort=16896 DstPort=8090 PolicyID=2 Action=PERMIT Content="Session Setup"
2021-06-18 16:28:03	信息	防火墙策略	475	SrcIP=merged DstIP=200.1.1.10 Protocol=TCP SrcPort=16896 DstPort=8090 PolicyID=2 Action=PERMIT Content="Session Setup"
2021-06-18 16:27:43	信息	防火墙策略	459	SrcIP=merged DstIP=200.1.1.10 Protocol=TCP SrcPort=16896 DstPort=8090 PolicyID=2 Action=PERMIT Content="Session Setup"
2021-06-18 16:27:23	信息	防火墙策略	479	SrcIP=merged DstIP=200.1.1.10 Protocol=TCP SrcPort=16896 DstPort=8090 PolicyID=2 Action=PERMIT Content="Session Setup"

82 第82章 流日志

82.1 流日志概述

为了方便快速查看一条数据流经过设备时的详细处理信息，流日志整合了若干模块（包括流管理、NAT 转换、防火墙策略、av、ips、威胁情报以及流量控制）的日志信息，在这条数据流拆除的时候，生成一条日志上报。设备针对长连接，会每隔 5 分钟上报一次。

82.2 流日志配置

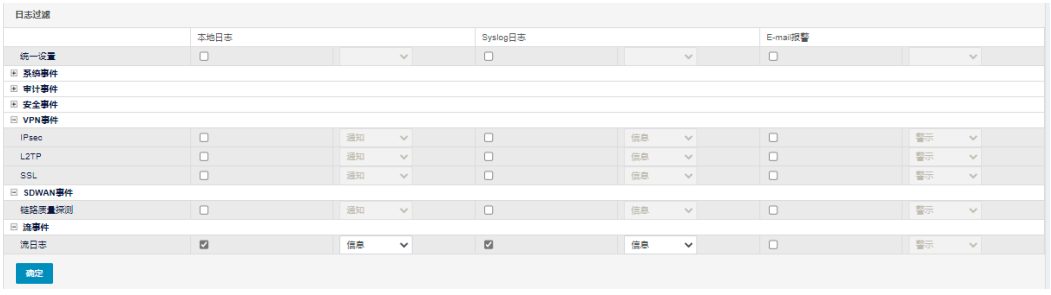
82.2.1 全局开关

1. 进入**日志>日志管理>流日志配置**，如下图：

2. 点击**启用**，开启流日志。

82.2.2 流日志过滤开关

1. 进入**日志>日志管理>日志过滤**，如下图：

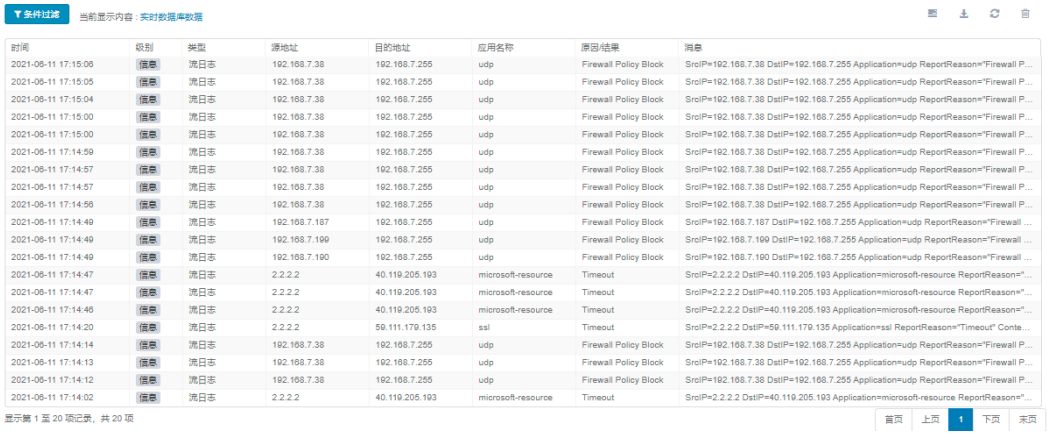


2. 点击**本地日志**或者 **syslog 日志**，开启日志，级别选择信息，点击**确定**。

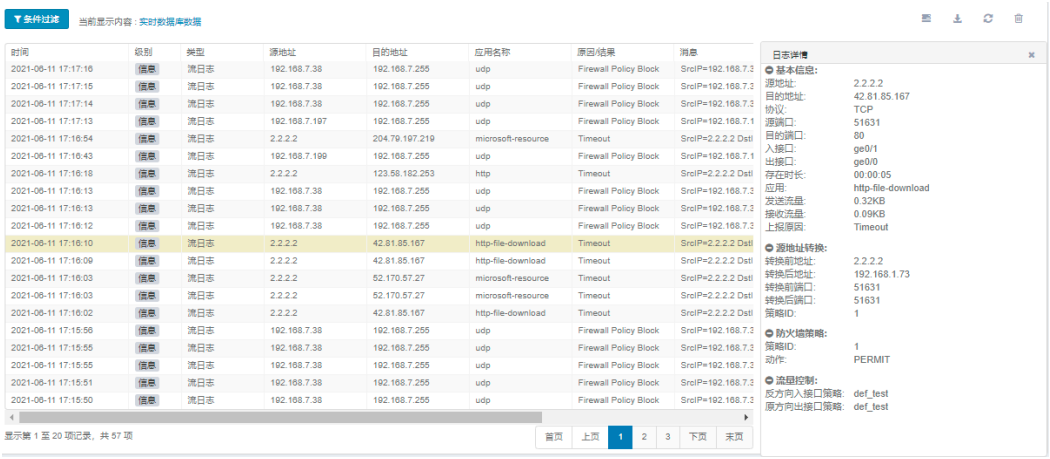
82.3 流日志展示

82.3.1 本地日志展示

1. 进入**日志>流日志**，如下图



2. 点击某一行，右侧出现飘窗，展示出这条流的详细信息。



展示列说明：

基本信息：展示流量的基本信息包含五元组、流量的入接口、出接口、识别的应用等信息。

策略匹配情况：若流量能匹配到防火墙策略、NAT 策略、流量控制策略、入侵防护策略、病毒防护策略、威胁情报策略几类策略类型，会将详细的策略匹配信息展示在流日志中。

注意

1、 默认情况下，若连接只有正向有流量，不会记录流日志；到设备本地的访问不会记录流日志。

2、 若流量为长连接，每隔 5 分钟会上报一条流日志。

3、 若匹配策略阻断，会立即上报阻断类型的流日志。

4、 若连接 5 分钟内自动老化拆除，会话拆除时上报流日志。

源

83 第83章 系统配置

83.1 系统配置概述

本章涉及设备的基本配置，通过相关配置，从而对设备自身能够进行管理。配置包括：

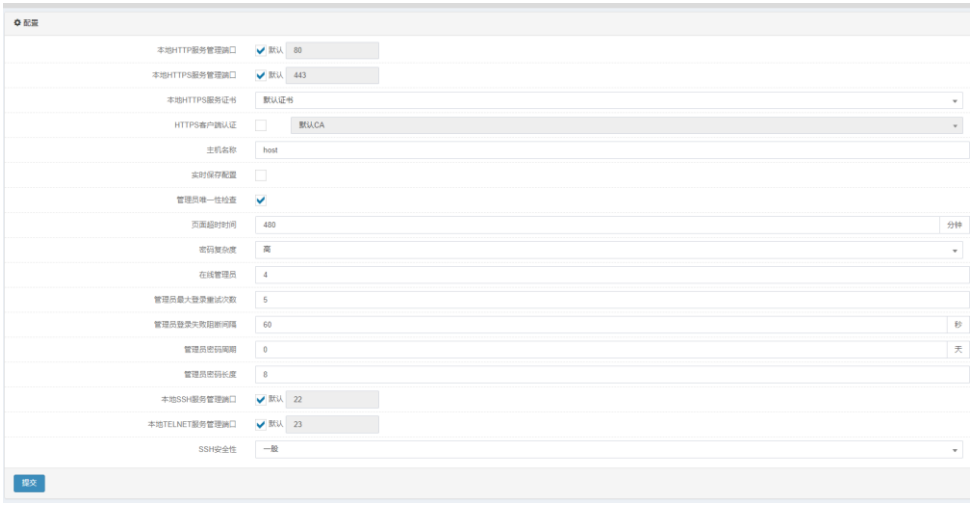
- 设备。配置设备主机名称，管理员登录限制，web 配置实时保存等。
- 系统监控。可以配置系统资源，如 memory/cpu 的监控阈值，当高于阈值时发送告警日志，使管理员及时了解设备状态。
- 时间配置。配置设备的系统时间和时区。系统时间可以通过手工配置，也可以通过 NTP 服务器获取。
- DNS 配置。可以配置 DNS 服务器来解析设备发出的域名解析请求。NTP 服务器域名通过此处配置的 DNS 服务器来解析。
- 备份恢复。可以为设备导入已有的配置，方便用户配置操作。同样可以将当前的配置导出供以后或其他设备使用。
- 告警邮件配置。用来发送 email 类型的日志。也可以将问题反馈以邮件的形式发送给收件人。
- 问题反馈。填写问题反馈的收件人及反馈内容。
- 设备重启。可以重启设备或者恢复出厂配置并重启设备以及设备进入虚拟 USG 管理系统。
- 集中管理。可以配置集中管理平台相关参数，从而通过集中管理平台管理设备。
- 设备运行记录。记录设备运行信息，用于排查问题。
- 配置自动备份。可以定期备份配置文件，防止设备因异常导致配置丢失。

83.2 配置说明

83.2.1 配置设备

配置步骤：

进入**系统>配置>设备**



本地 HTTP 服务管理端口: 默认为 80，通常不需修改。有需要时可修改服务端口。

本地 HTTPS 服务管理端口: 默认为 443，通常不需修改。有需要时可修改服务端口。

本地 HTTPS 服务证书：可以选择本地证书也可以用默认证书。

HTTPS 客户端认证：https 客户端认证的 CA 证书，可以默认 CA 证书，也可以选择本地的 CA 证书。

主机名称:设备的名称。

实时保存配置:选择此项后，web 上的配置都配置完成后，时间超过 10 分钟就自动进行配置保存。

管理员唯一性检查:选择此项后，一个管理员同时只能在一台 pc 上登录。

页面超时时间：在 web 无操作的情况下，超过该设置的时间，登录用户会自动退出。缺省为 10 分钟。

密码复杂度：配置密码复杂度。密码复杂度代表了设备密码的强度，分为高、中、低三个级别，高复杂度密码里必须包含特殊字符（!@#$%&`,-.）、数字（0-9）、大小写字母，并且密码的长度不得小于 8 位；中复杂度密码必须包含数字与特殊字符，并且密码的长度不得小于 8 位；低复杂度密码只要满足最小长度不低于 8 位。

在线管理员：最多可以同时登录的管理员个数。默认为 4 个。

管理员最大登录重试次数：默认为 5 次。

管理员失败登录阻断间隔：重试次数达到最大时，暂时阻断用户登录的时间间隔。

管理员密码周期：管理员密码修改周期，管理员密码超过该周期，提示修改密码。

管理员密码长度：配置管理员最小密码长度。

本地 SSH 服务管理端口：设备 ssh 服务器端口。

本地 TELNET 服务管理端口：设备 telnet 服务器端口。

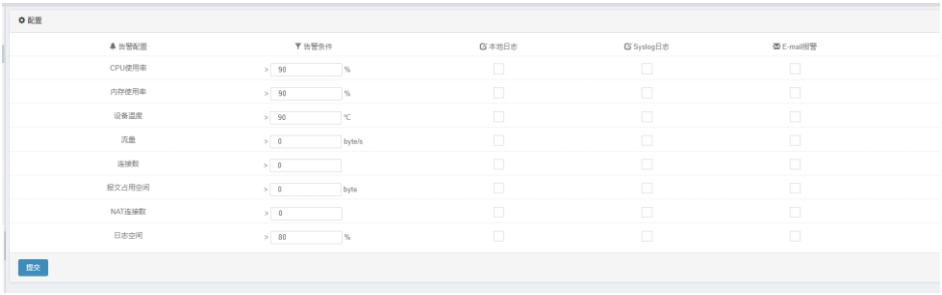
SSH 安全性：配置 ssh 安全性。

配置步骤：

1. 如果设备的 http/https 服务管理端口不是默认的 80/443,可以通过**本地 HTTP 服务管理端口/本地 HTTPS 服务管理端口**进行配置，通常选择**默认。**
2. 如果需要 https 的服务器验证或者客户端验证，配置**本地 HTTPS 服务证书或者 HTTPS 客户端认证**。
3. 配置**主机名称**，默认为 host。
4. 如果需要实时保存配置，勾选**实时保存配置**。
5. 如果要限制同一管理员同时在不同 pc 上登陆设备,勾选**管理员唯一性检查**。
6. 输入**页面超时时间**，默认为 10 分钟。
7. 选择**密码复杂度**，默认为高。
8. 输入**在线管理员**个数。
9. 输入**管理员最大登录重试次数**。
10. 输入**管理员失败登录阻断间隔**。
11. 输入**管理员密码周期**。
12. 输入**本地 SSH 服务管理端口**。
13. 输入**本地 TELNET 服务管理端口**。
14. 选择 **SSH 安全性**，默认为一般。
15. 点击**提交**。

83.2.2 系统监控

进入**系统>配置>系统监控**

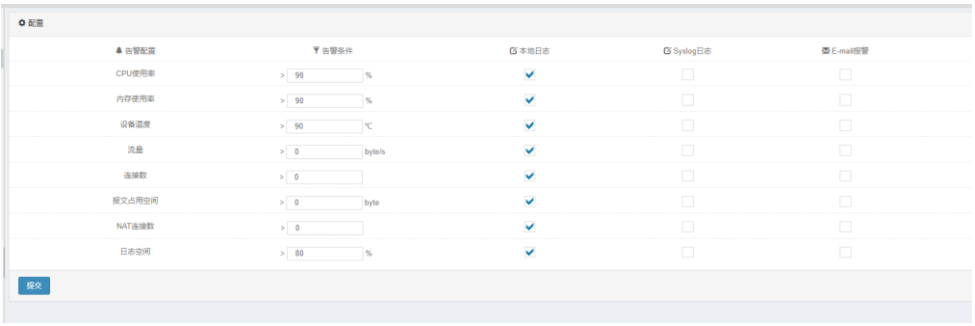


此界面可以设置 CPU 占用率、内存占用率、设备温度、流量、连接数、报

文占用空间、NAT 连接数以及日志空间的阈值，并可配置当达到阈值后，产生告警日志，CPU 占用率、内存占用率、设备温度、日志空间这些告警日志默认 5 分钟发送一次。

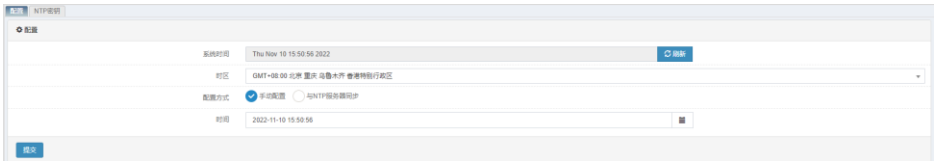
配置步骤：

1. 输入 cpu 告警阈值，分管理核和业务核，占用率是平均使用率。
2. 输入内存告警阈值，指共享内存使用率。
3. 输入温度告警阈值，指设备温度。
4. 输入流量告警阈值。
5. 输入连接数告警阈值。
6. 输入报文占用空间告警日志。
7. 输入 NAT 连接数告警阈值，指 NAT 规则并发连接数总和。
8. 输入日志空间告警阈值，指日志硬盘的使用率。
9. 选择日志类型。本地日志、Syslog 日志、E-mail 报警。Syslog 日志发送到日志模块，需要配置的日志服务器。E-mail 报警会将日志以 E-mail 形式发送到告警邮件配置的邮件地址。
10. 点击**提交**。



83.2.3 时间配置

进入**系统>配置>时间配置**



系统时间：显示当前的系统时间。

时区选择：配置所在的时区。

配置方式：可以手动配置系统时间，也可以选择 NTP 服务器来同步系统时间。

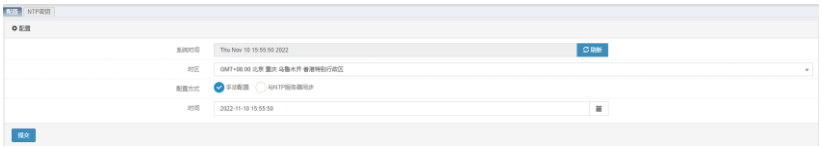
配置步骤：

1. 选择**配置方式**。**手动配置**或**与 NTP 服务器同步**。

2. 手动配置时，用户自己设定具体的时间。
3. 与 NTP 服务器同步时，需要指定 ntp **服务器**域名及**同步间隔**。

   有 2 个前提步骤：(1)配置默认路由。(2)配置 DNS。
4. 点击**提交**。

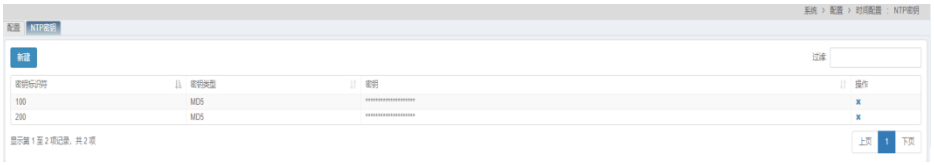
手动配置系统时间



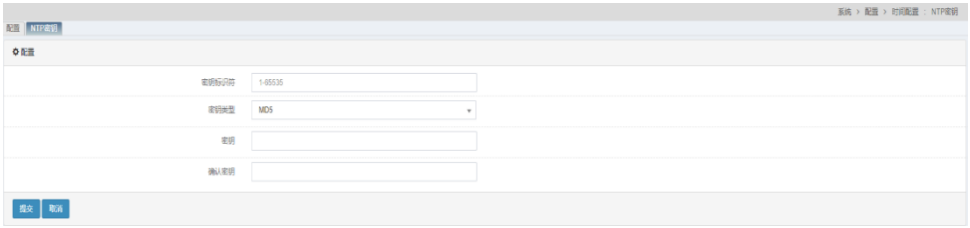
使用 NTP 服务器同步系统时间

1. 配置 **NTP 密钥**。

   A、在**时间配置**页面中，选择 **NTP 密钥**页面标签。**NTP 密钥**页面标签中显示已经配置的 NTP 密钥。



   B、点击**新建**按钮，显示**配置** NTP 密钥页面



   C、在**密钥标识符**中输入密钥标识符；

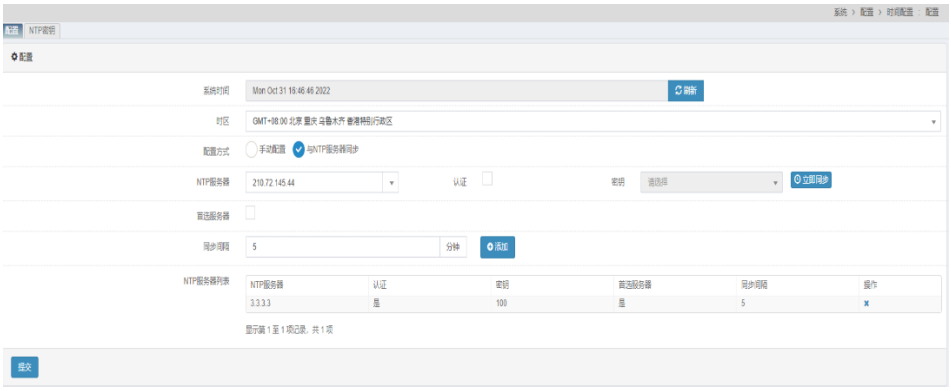
   在**密钥类型**中选择 **MD5**；

   在**密钥**和**确认密钥**中输入相同的密钥密文；

   D、点击**提交**。

   最多可以配置 64 条 NTP 密钥。

   可以在 NTP 密钥显示页面中，删除 NTP 密钥。
2. 在**时间配置**页面中选择**配置方式**为**与 NTP 服务器同步**。



3. 添加 NTP 服务器。

   在 **NTP 服务器**中选择或填写 NTP 服务器的 IP 地址或域名；

   如果需要与该 NTP 服务器进行认证，则选择**认证**，同时在**密钥**中选择认证时使用的密钥标识；

   如果该 NTP 作为首选服务器，则在**首选服务器**中勾选；

   在**同步间隔**中填写以分钟为单位的与该服务器进行时间同步的间隔；

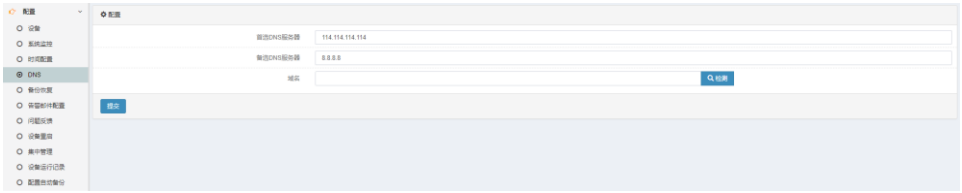
   点击**添加**，将该 NTP 服务器添加到 **NTP 服务器列表**当中。

   总共可以配置一个首选 NTP 服务器，和两个备选 NTP 服务器。

4. 点击**提交**。

83.2.4 DNS配置

进入**系统>配置>DNS**



首选 DNS 服务器: 首选 dns 服务器地址。

备选 DNS 服务器: 备选 dns 服务器地址，与首选 dns 通信地址同时发送 dns 请求报文，先收到谁回复的 dns 报文，就以哪个服务器的解析地址为结果。

域名: 配置了上面的服务器地址后，可以输入一个域名进行测试，dns 服务器是否可用。在这之前应该检查是否有路由到 dns 服务器。

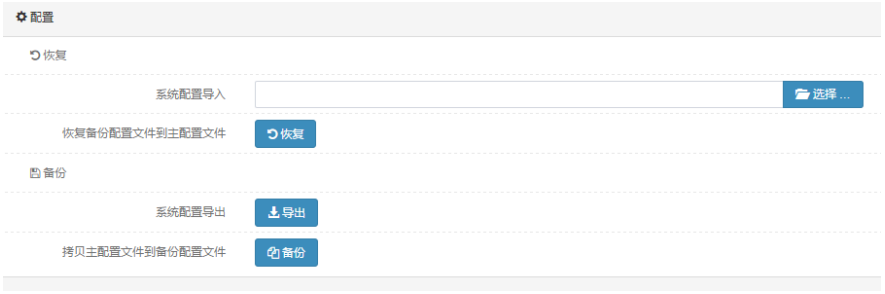
配置步骤:

1. 输入**首选 DNS 服务器。**
2. 输入**备选 DNS 服务器。**

3. 点击**提交**。

83.2.5 备份恢复

进入**系统>配置>备份恢复**



系统配置导入: 选择配置文件导入到设备中。

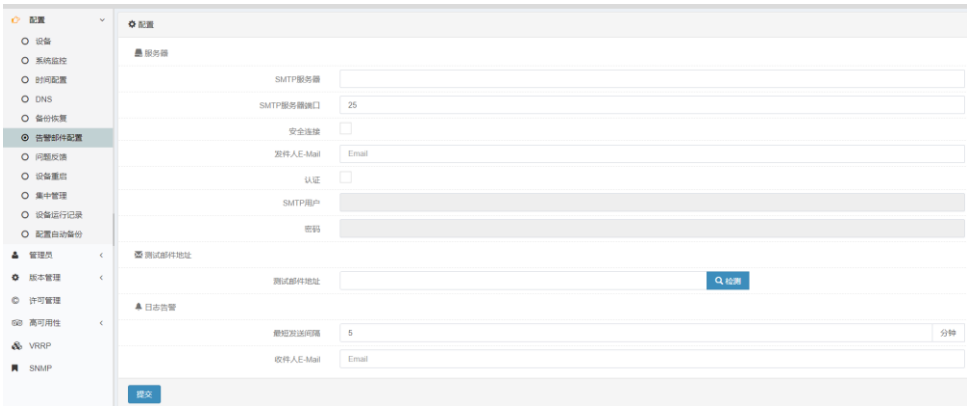
恢复备份配置到主配置文件: 设备内的备份配置覆盖主配置。

系统配置导出: 将设备中的配置文件导出。

拷贝主配置文件到备份配置文件: 对设备内的主配置进行备份。

83.2.6 告警邮件配置

进入**系统>配置>告警邮件配置**



SMTP 服务器：邮件服务器地址。

SMTP 服务器端口：邮件服务器的端口。

安全连接：是否启用安全连接。

发件人 E-Mail：发件人邮箱。

认证：是否启用邮件认证。

SMTP 用户：发件人邮箱登陆用户名。

密码：发件人邮箱登陆密码。

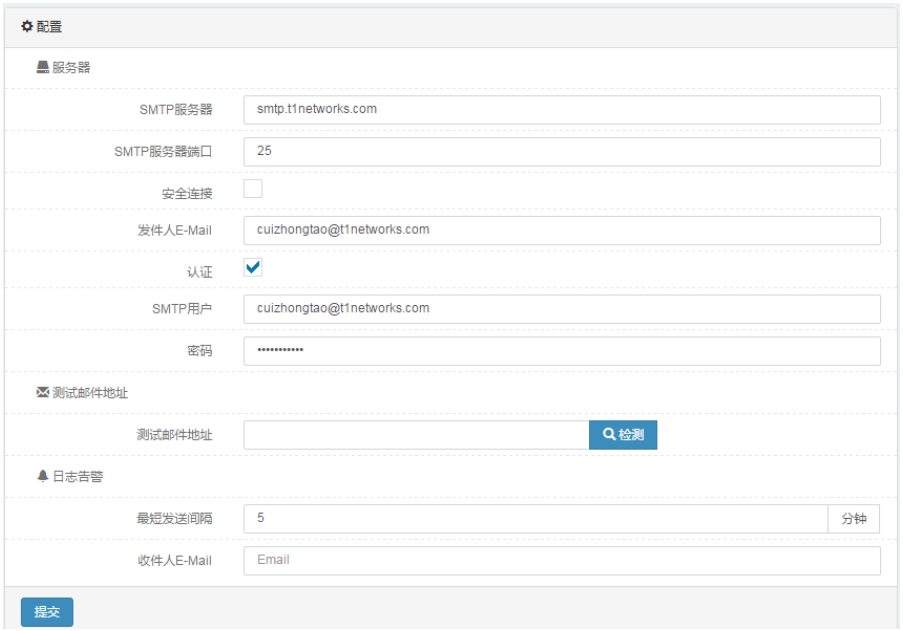
测试邮件地址：发送测试邮件到该地址，检测地址是否可达。

最短发送间隔：E-mail 日志消息最短发送的间隔时间，配置范围 1-60 分钟。

收件人 E-Mail：收件人邮箱地址。多个邮箱地址用分号隔开。

配置步骤：

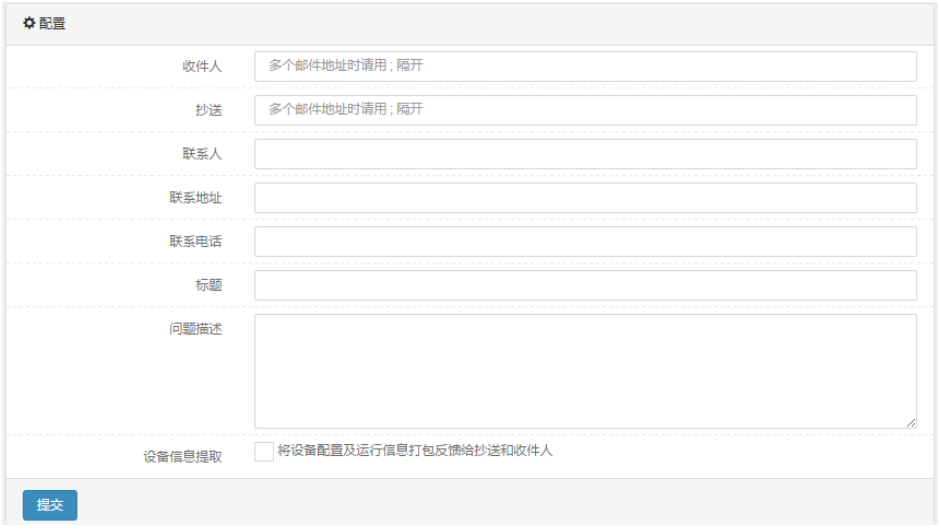
1. 输入 SMTP 服务器。
2. 输入 SMTP 服务器端口号，缺省为 25。
3. 如果 SMTP 服务器需要安全连接，勾选上启用安全连接。
4. 输入发件人 E-Mail 地址。
5. 如果您的 SMTP 服务器需要认证，勾选上启用认证。
6. 输入 SMTP 用户。
7. 输入邮箱登录密码。
8. 填写日志信息最短发送间隔。
9. 填写日志信息收件人 E-Mail。
10. 点击**提交**。



83.2.7 问题反馈

配置步骤：

进入**系统>配置>问题反馈**



收件人:收件人邮箱地址。

抄送:邮件抄送地址。

标题: 邮件标题。

问题描述:本次反馈的问题描述。

联系人:联系人姓名。

联系地址:联系人地址。

联系电话:联系人电话。

设备信息提取：是否将设备配置及运行信息打包反馈给抄送和收件人

配置步骤：

配置前提，必须配置上节描述的**告警邮件配置**，且告警邮箱可成功发送测试邮件。

1.输入**收件人**邮箱地址。

2.选择输入**抄送**地址。

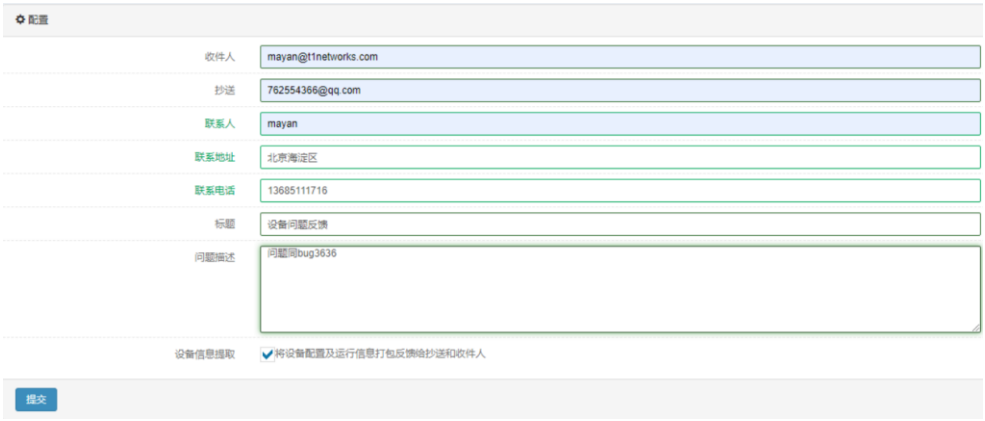
3.填写**联系人姓名，地址和联系方式**。

4.输入**标题**。

5.输入**问题描述**。

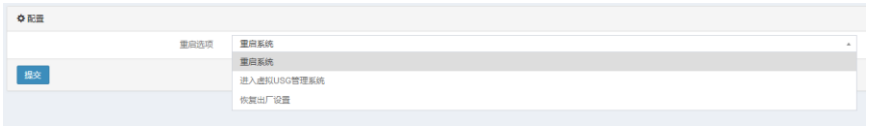
6.根据需要是否勾选设备信息提取单选框

7.点击**提交**。



83.2.8 设备重启

进入**系统>配置>设备重启**

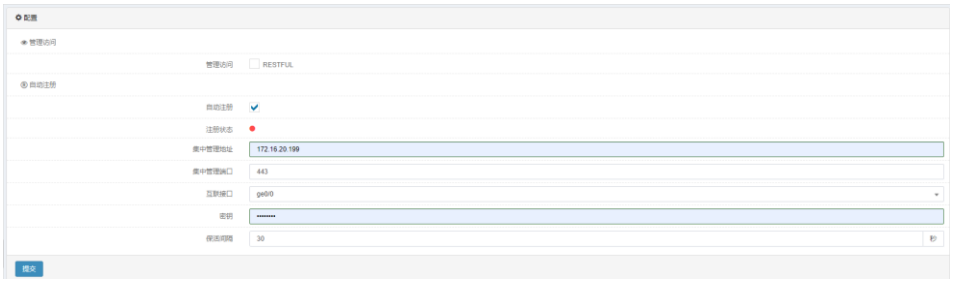


该界面可以重启设备、进入虚拟 USG 管理系统或者恢复出厂设置并重启设备。

83.2.9 集中管理

进入**系统>配置>集中管理**

集中管理功能是结合集中管理平台使用的，配置如下图所示。配置好集中管理平台的 IP，端口等参数后，就可以在集中管理平台上远程管理设备，即使设备的接口 IP 是私网 IP。



参数说明：

管理访问：是否开启 RESTFUL 接口，开启后可以通过 APIrestful 接口管理设备；

自动注册：使能开关，开启后设备自动注册到集中管理平台；

集中管理地址：集中管理平台的 ip；

集中管理端口：集中管理平台的端口；

互连接口：集中管理平台通过这个接口管理设备；

密钥：设备注册到集中管理平台的密钥；

保活间隔：设备发送保活报文的间隔；

83.2.10 设备运行记录

设备运行记录包括：设备运行记录配置、设备运行记录日志文件导出、系统运行日志导出。主要用于对设备运行的健康状态进行记录。

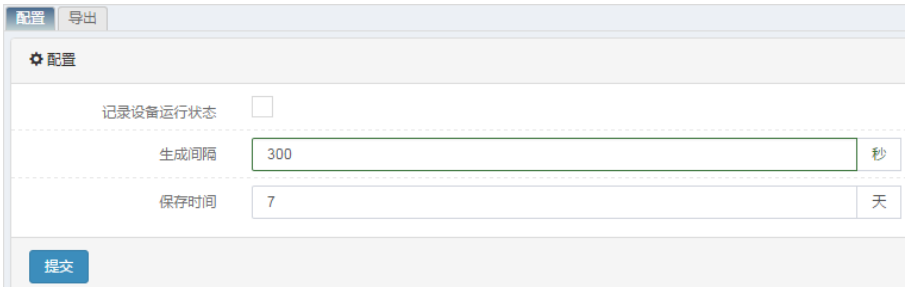
设备运行记录配置：用于对设备运行记录功能进行配置，以便形成设备运行记录日志。

设备运行记录日志文件导出：日志中记录设备的一些实时信息，包括版本信息、接口信息、流量信息等。用户可以选择性的导出日志，并导出压缩包文件。

系统运行日志导出：导出系统运行记录文件加密压缩包。

配置步骤：

1. 进入**系统>配置>设备运行记录：配置**，如下图：



参数说明：

记录设备运行状态：该功能是否使能。

生成间隔：多长时间记录一次信息，包括流量信息、接口信息、版本信息等。每天形成一个以日期为名称的新日志文件

保存时间：记录几天。若配置的是 3，代表记录连续 3 天的文件，即在磁盘中保存 3 个日志文件。新形成的文件会覆盖形成时间最早的文件。

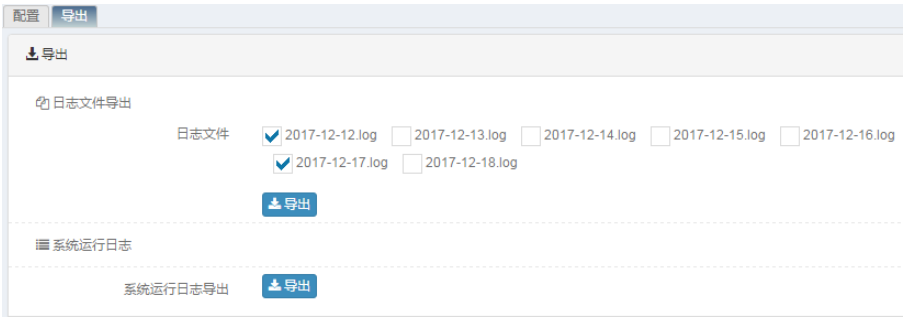
2 配置完毕后，点击**提交**。

该功能只能在有磁盘的设备上使用。

导出设备运行记录：

配置步骤：

1. 进入**系统>配置>设备运行记录：导出**，如下图：



参数说明：

日志文件导出：导出某一天及某几天的日志文件。

系统运行日志导出：导出系统运行日志。

83.2.11 配置自动备份

进入**系统>配置>配置自动备份**

配置自动备份可以具体按每周或者每月定期备份当前配置文件，防止设备因异常导致配置文件丢失，设备最多可以备份 32 份配置文件，其中无硬盘设备备份的配置文件大小不能超过 10M，总配置文件大小不能超过 10M。

参数说明：

配置自动备份：配置自动备份开关。

每周：每周定期备份配置文件。

每月：每月定期备份配置文件。

时间：每周、每月具体时分备份配置文件。

导出：将备份配置文件导出。

83.3 配置案例

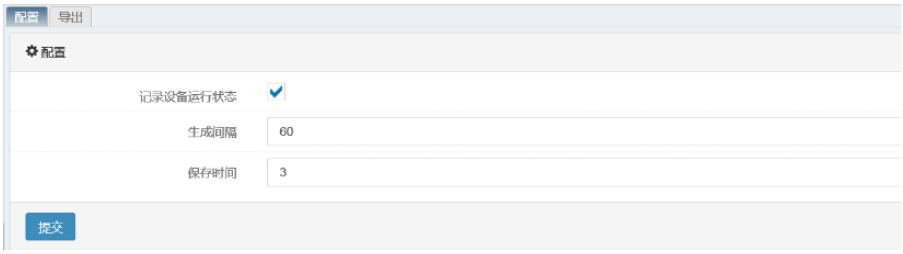
83.3.1 配置案例1：对设备运行记录进行配置并导出

案例描述

将生成间隙配置成 60，保存时间设置成 3 天，并使能设备运行记录功能。最后导出所生成的日志文件。

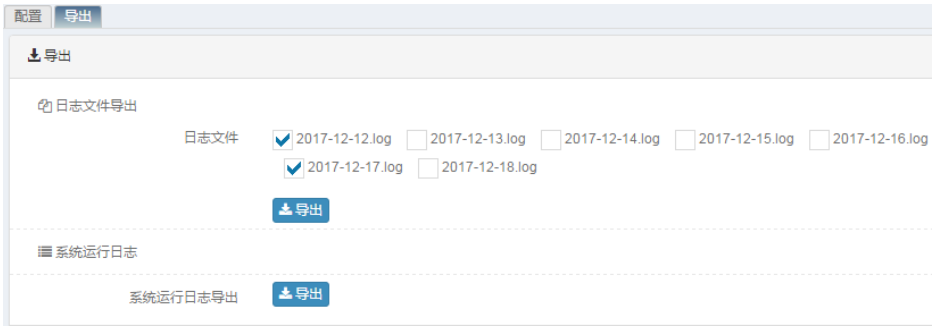
配置步骤：

1. 进入**系统>配置>设备运行记录：配置，**如下图所示：

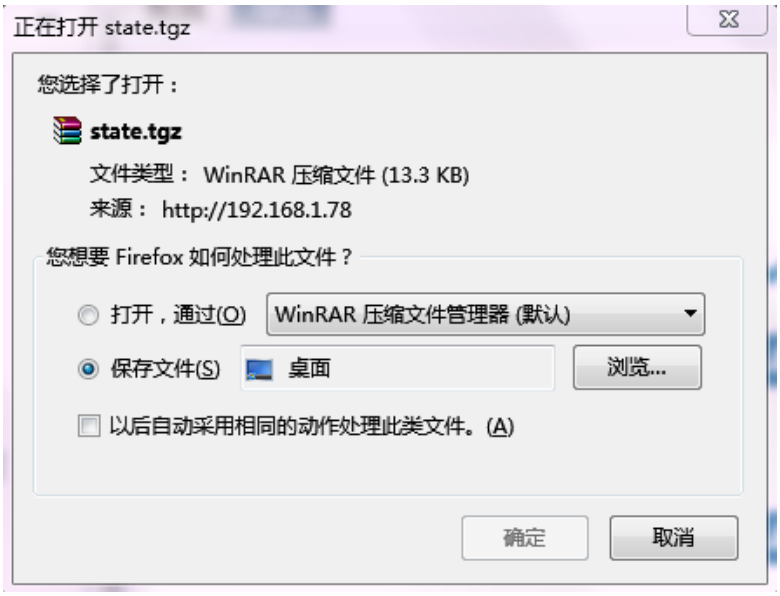


2. 点击**提交**

3. 进入**系统>配置>设备运行记录：导出，**如下图所示：



4. 选择要导出的日志文件，点击**导出，**如下图所示：



83.3.2 配置案例2：设置每个月10号进行配置自动备份

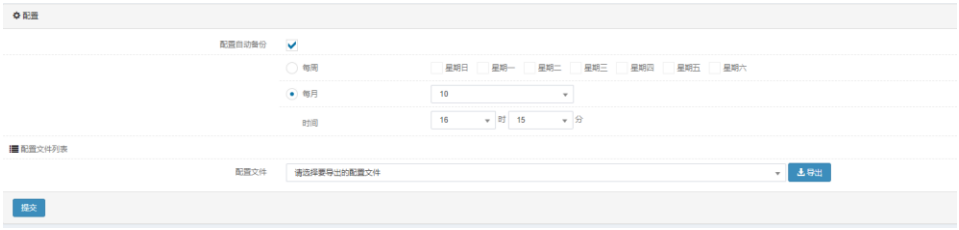
案例描述

设置配置自动配置，按照每个月 10 号进行配置自动配置，时间设置为 16 点 15 分。导出对应的配置文件

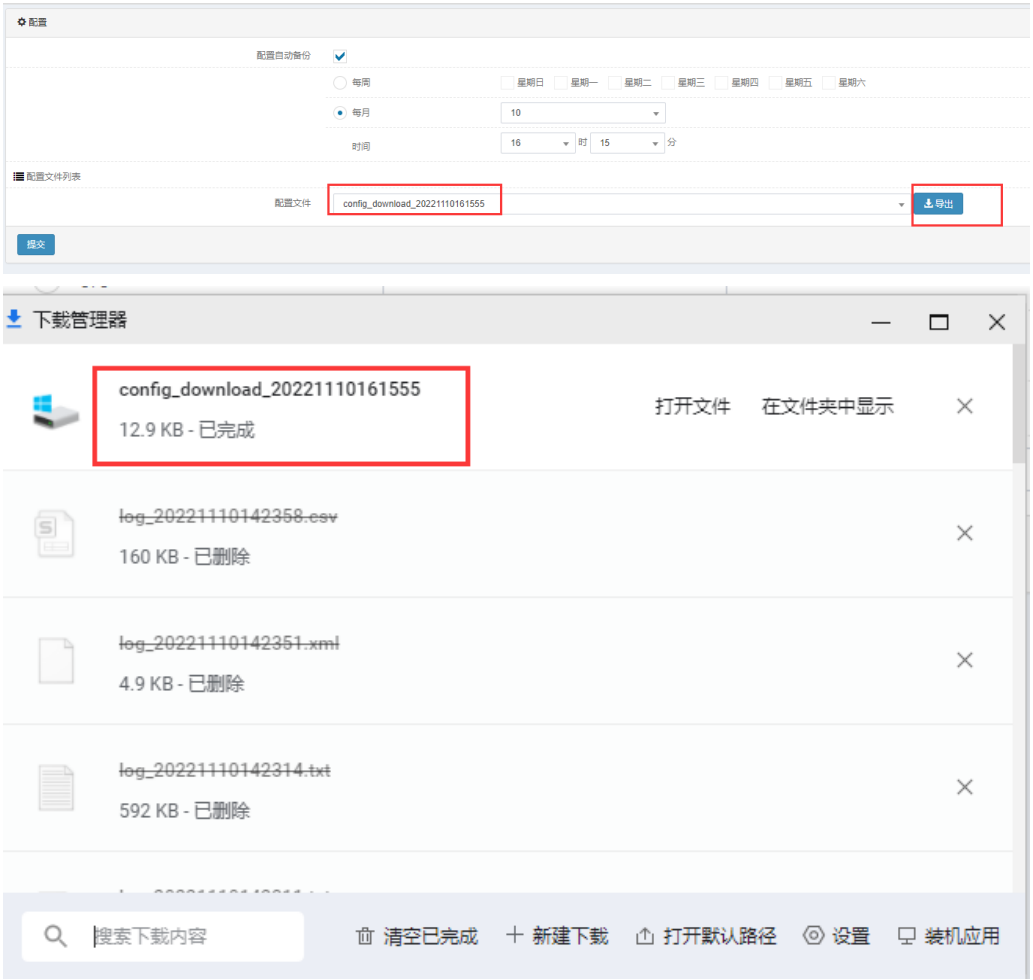
配置步骤：

1. 进入系统>配置>配置自动备份，设置每个月 10 号进行配置自动配

置，时间设置为 16 点 15 分。



2. 选择对应的日期配置文件，点击**导出**按钮导出配置文件。



84 第84章 管理员

84.1 管理员概述

T 系列防火墙支持使用本地用户数据库，支持使用 RADIUS 服务器、LDAP 服务器的用户认证。（1）可以把用户名添加到 T 系列防火墙用户数据库中，然后为用户设置一个密码以允许用户使用这个内部的数据库进行认证。（2）可以添加一个 RADIUS 服务器并且选择 RADIUS，以允许用户使用选定的 RADIUS 服务器进行认证。（3）可以添加一个 LDAP 服务器并且选择 LDAP，以允许用户使用选定的 LDAP 服务器进行认证。当一个用户输入用户名和密码时，如果这个用户设置了密码并且密码匹配，则认证通过。

如果选择的是 RADIUS，用户名和密码与 RADIUS 服务器中的用户名和密码相匹配，则认证通过。

如果选择的是 LDAP，而且配置了 LDAP 支持，用户名和密码与 LDAP 服务器中的用户名和密码相匹配，则认证通过。

84.2 配置管理员

84.2.1 配置管理员

配置用于认证的管理员用户。

进入**系统>管理员>管理员**

用户名：管理员的名称。

描述：对管理员的描述。

访问权限：管理员使用的访问权限列表，默认的权限表有 audit、admin、useradmin 三项，已配置的自定义权限表也可以在此处被选择。

类型：管理员认证的类型，包括、密码】、RADIUS、LDAP。

注意

密码*：**选择该域表示对于创建的用户，其用户名和密码都保存在本地，然后在密码***和***确认密码***中输入你设置的本地用户的密码。

RADIUS：选择该域表示对于创建的用户，本地只保存用户名，不保存密码，用户需要到指定的 RADIUS 服务器上去认证，该用户需要在 radius 服务器上存在。下拉列表中列出了当前已经配置了的 RADIUS 服务器。

LDAP：选择该域表示对于创建的用户，本地只保存用户名，不保存密码，用户需要到指定的 LDAP 服务器上去认证，该用户需要在 ldap 服务器上存在。下拉列表中列出了当前已经配置了的 LDAP 服务器。

管理 IP/掩码 #1：允许哪些网段的用户登录。

管理 IP/掩码 #2：允许哪些网段的用户登录。

管理 IP/掩码 #3：允许哪些网段的用户登录。

84.3 配置RADIUS服务器

如果您配置了 RADIUS，当某个用户被配置为要求使用 RADIUS 服务器认证的时候，T 系列防火墙将连接 RADIUS 服务器以获得认证。

84.3.1 配置RADIUS服务器

进入**对象>认证服务器>RADIUS**，点击**新建**

名称：RADIUS 服务器名称，标识 RADIUS 服务器。

服务器 IP：RADIUS 服务器的 IP 地址。

服务器密码：RADIUS 服务器的共享密钥。

认证端口：RADIUS 服务器用于认证的端口。默认 1812。

提示

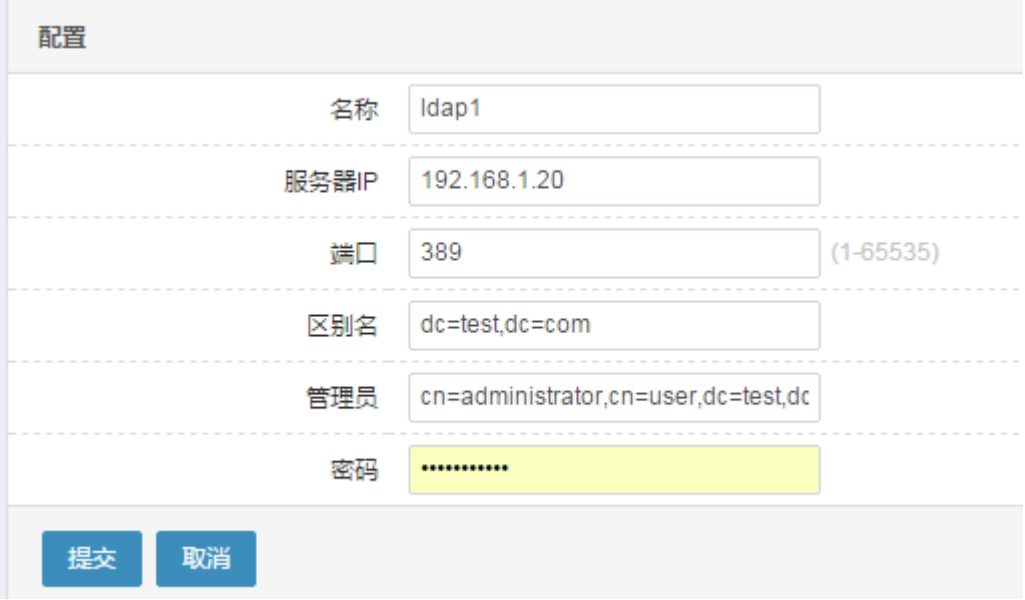
点击**认证服务器**下的 **RADIUS 配置**标签页，显示当前系统中配置的所有 RADIUS 服务器。

84.4 配置LDAP服务器

如果您配置了 LDAP，当某个用户被配置为要求使用 LDAP 服务器认证的时候，T 系列防火墙将连接 LDAP 服务器以获得认证。

84.4.1 配置LDAP服务器

进入**对象>认证服务器>LDAP**，点击**新建**



名称：LDAP 服务器名称，标识 LDAP 服务器。

服务器 IP：LDAP 服务器的 IP 地址。

端口：LDAP 服务器用于认证的端口。缺省为 389

区别名：用来指明在 LDAP 服务器上查找数据的起始位置。如，ldap 服务器上，在路径 test.com 中，容器 users 下有用户 user2。则区别名中配置为”dc=test，dc=com”。

管理员：LDAP 服务器的管理员用户。如，登陆 ldap 服务器的系统用户名为 administrator，密码为 111111，且该系统用户也存在于 ldap 服务器下，处于 test.com 中容器 users 下。则此管理员配置为”cn=administrator,cn=users,dc=test,dc=com”密码为”111111”。

密码：LDAP 服务器的管理员密码。

点击**认证用户**下的 **LDAP** 标签页，显示当前系统中配置的所有 LDAP 服务器。

84.5 认证用户监控与维护

84.5.1 查看管理员信息

进入**系统>管理员>管理员**，查看管理员信息。

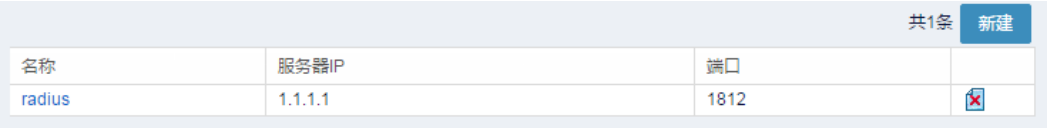
共3条 新建

用户名	管理地址	访问权限	描述	
audit		audit	default audit administrator	
admin	0.0.0.0/0	admin	default super administrator	
useradmin		useradmin	default user administrator	

可以查看用户的用户名，管理地址，访问权限，描述。

84.5.2 查看RADIUS服务器信息

进入**对象>认证服务器>RADIUS**，查看 RADIUS 服务器信息。



共1条 新建

名称	服务器IP	端口	
radius	1.1.1.1	1812	

可以查看 RADIUS 服务器名称，服务器 IP，端口。

84.5.3 查看LDAP服务器信息

进入**对象>认证服务器>LDAP**，查看 LDAP 服务器信息。

共1条 新建

名称	服务器IP	端口	区别名	
ldap1	192.168.1.20	389	dc=test,dc=com	

可以查看 LDAP 服务器名称，服务器 IP，端口，区别名。

84.5.4 查看在线管理员信息

进入**系统>管理员>在线信息**，查看在线管理员信息。

在线用户 共2条 刷新

用户名	管理地址	访问方式	登录时间	
admin		CONSOLE	2016-11-24 15:00:07	
admin	192.168.1.116	WEB	2016-11-24 15:00:33	

阻断用户 共0条

登录地址	最近登录用户名	最近登录方式	最近登录时间	解除阻断时间	

可以查看在线的管理员信息，阻断的管理员用户。

84.6 常见故障分析

84.6.1 故障现象：系统用户使用radius认证失败

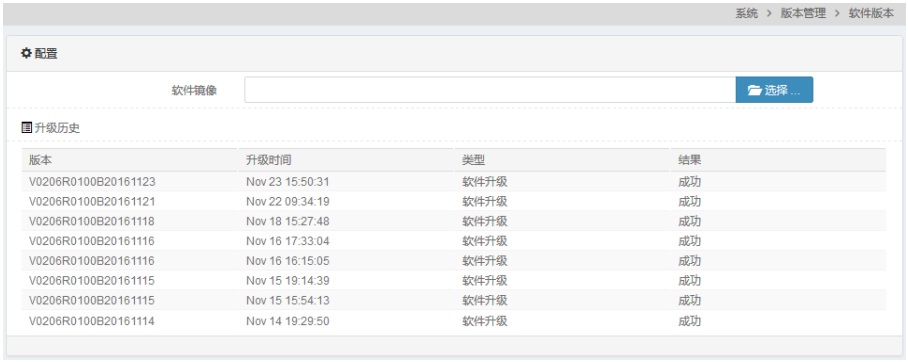
现象	使用radius用户登陆T系列防火墙系统失败。	
分析	1.	密码错误
	2.	RADIUS服务器配置错误（比如：共享密钥，IP等）
	3.	RADIUS服务器连接不上（比如：PING不通）
	4.	RADIUS服务器上没有这个用户
解决	1.	检查用户密码，输入正确的用户名和密码
	2.	修改该RADIUS服务器的配置
	3.	首先确保T系列防火墙和RADIUS服务器能通讯，能PING通
	4.	为该RADIUS服务器添加该用户

85 第85章 版本管理

85.1 版本管理

85.1.1 版本管理

1. 进入**系统>版本管理>软件版本**：



点击**选择**按钮，选择正确的升级包，点击**升级**进行版本升级。升级历史会显示最近的 10 条升级记录。

配置步骤：

1. 通过**选择**选择需要的升级包。
2. 点击**升级**或者**移除**按钮。
3. 点击**升级**后系统开始升级，没有升级成功之前，如果不想升级了，也可以点击**取消按钮取消**升级。

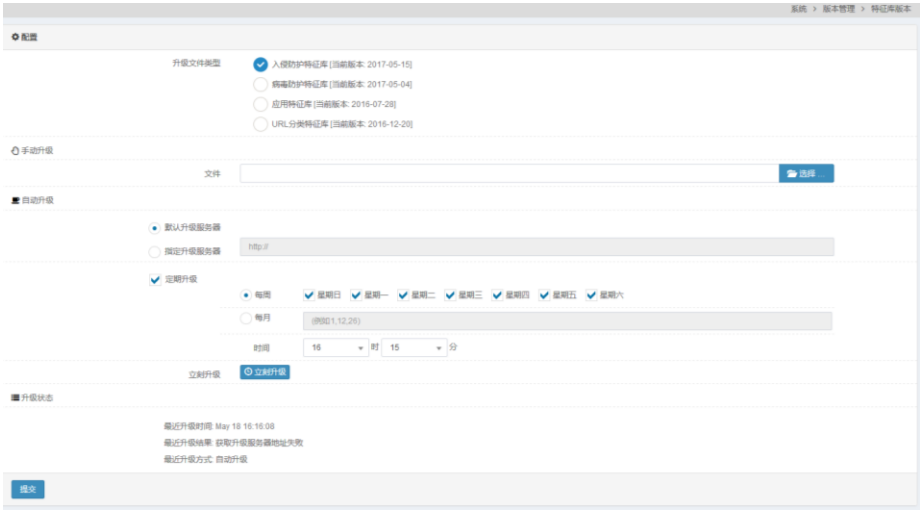
85.1.2 特征库升级

设备可以手动、自动升级特征库版本。


提示

出厂时，已经默认加载了最新版本的特征库。

选择**系统>版本管理>特征库版本**，如下图：



升级文件类型：选择需要升级的特征库类型。

手动升级:

文件：点击**选择**按钮，选中对应的特征库文件，点击“**升级**”即可

提示

采用手动升级功能时，需要保证升级文件为合法的特征库文件。

自动升级：

默认升级服务器: 升级服务器设为默认升级服务器。

指定升级服务器: 设置升级服务器地址。

定期升级: 启用定期自动升级。

每周: 设置每周星期几。

每月: 设置哪些月份。

时间: 设置自动升级的当天时间点。

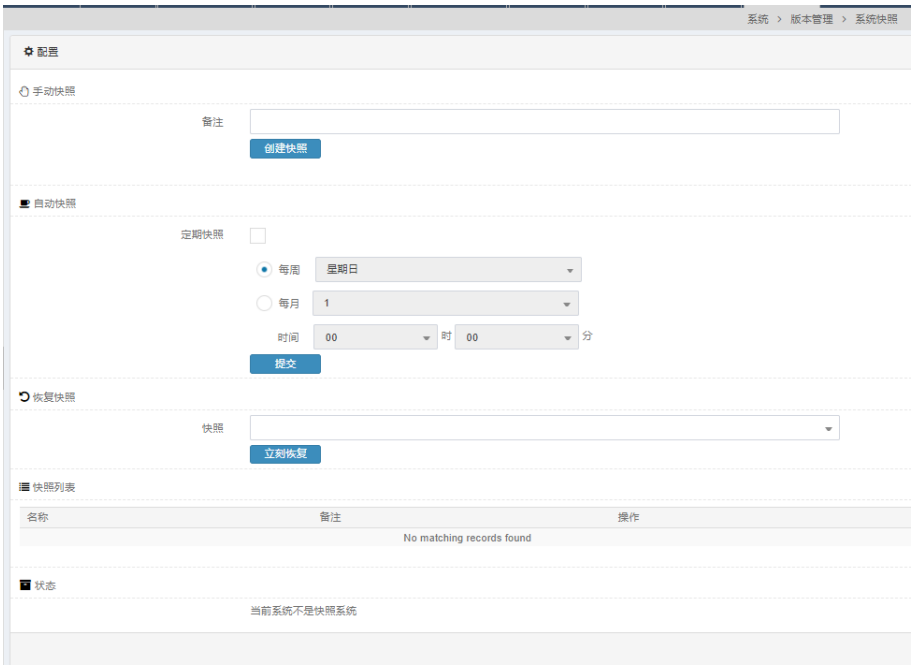
配置好后，点击**提交**。

立即升级：点击此按钮后，系统立即自动升级。

1.1.3 系统快照

设备可以创建、删除、恢复、显示系统快照。

选择**系统>版本管理>系统快照**，如下图：



手动快照:

备注：输入想要创建快照的备注，点击“**创建快照**”即可

提示

快照的备注不是快照的名称。自动快照的备注都是 auto，手动快照不可以备注为 auto。

自动快照：

启用:自动快照的开关，选中，才能配置快照的周期。

周期：

每周：设置每周星期几。

每月：设置每月几号。

时间：设置每次自动快照的时间点。

配置好后，点击**提交**。

恢复快照：选择已创建的快照，点击**立即恢复**，恢复成当时的系统，系统会自动重启。

快照列表：已经创建的快照，列表包含快照的名称，备注，操作。点击操作处的  可以删除快照

状态：显示当前系统状态是否是快照系统，当前不是恢复快照的系统会显示**当前系统不是快照系统**，恢复快照系统重启后会显示**当前系统是 xxx 的快照系统**（xxx 表示快照的名称）。

提示

恢复快照的系统,修改配置或者重新下载版本之后状态会显示**当前系统不是快照系统**

86 第86章 许可管理

86.1 许可管理概述

设备的一些附加模块受许可(license)管理控制，如果没有导入许可，这些模块将无法配置及生效。目前受许可管理的模块包含：**入侵防护特征库升级、病毒防护特征库升级、应用特征库升级、URL 分类特征库升级、虚拟化、威胁情报**。

86.2 许可导入

选择**系统>许可管理**，如下图：

点击“**更新授权**”，将通过通过正常商务渠道获得的授权码粘贴到输入框中：

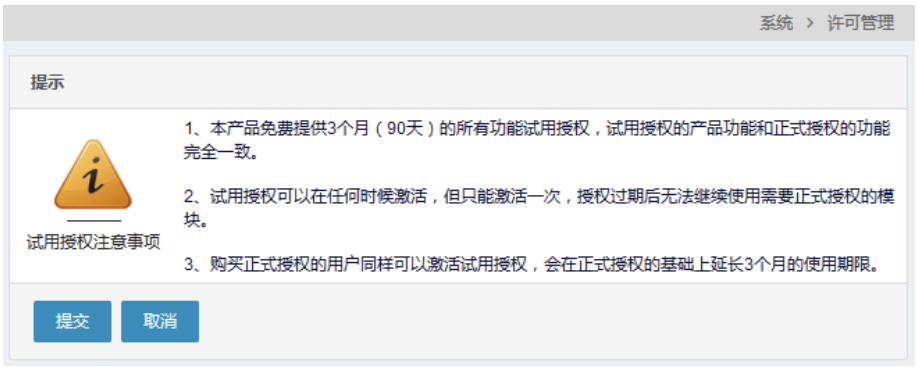
点击“**提交**”。

提示

如果输入的授权码无效，系统会提示失败。如果输入的授权码生效，返回页面会显示相关模块的许可信息。

86.3 许可试用

在“许可管理”中可点击“试用”，可以激活试用授权。试用授权的注意事项请参考点击后弹出的页面。



87 第87章 高可用性

87.1 HA概述

高可用性即 HA（High-Availability），是保证网络高可靠的一种技术方案，支持两台防火墙设备以主-备或主-主两种工作模式运行，可以满足不同的组网需要。

在主-备工作模式下，只有状态为“主”的防火墙设备转发流量，所有流量都被主设备转发，“备”设备不工作，但保持和“主”同样的配置，同时实时监测“主”设备的运行状态，一旦检测到“主”设备出现故障，比如掉电，设备死机等。“备”设备会自动接管“主”设备承担网络流量的转发工作，以保持网络的不中断运行。

在主-主工作模式下，两台防火墙设备同时转发流量，流量的分配比例取决于相邻网络设备的路由配置，以及防火墙上的相关配置，如浮动 IP 等。在主-主工作模式下，每台设备转发和自己单元 ID 相同的流量。

两台防火墙设备通过用户设置 IP 地址发送心跳报文来检测对端防火墙的工作状态，同时防火墙产品支持另外三个附加因素可选项：“网关监控”，“接口监控”和“链路聚合监控”作为切换条件。正在工作中的防火墙设备，如果检测到自己的监控状态比对端的优先级低，则会主动使自己变为“备”状态，所有流量被另外的防火墙设备接管。在主备工作模式下，具有抢占模式，可以指定主备设备，在正常的情况下，由指定的主备配置决定主备状态。

本章涉及 HA 功能的配置，阐述了如何通过 Web 管理界面配置 HA，实现 HA 功能。

87.2 HA基本配置

防火墙设备 HA 的基本配置包括工作模式，心跳地址、单元 ID 等。

配置步骤：

进入**系统管理>高可用性>配置**，进入**配置**界面。

工作模式：HA 工作模式，支持主备模式、主主模式。

首选通信地址：HA 心跳通信地址，用于发送和接收心跳报文。本地地址必须指定为设备本地的接口地址，推荐使用非业务口地址。

备选通信地址：HA 心跳备用通信地址，可选配置。指定备选通信地址后，首选地址和备选地址同时发送和接收心跳报文，为设备间通信提供保证。

单元 ID：设备的 ID 号，用于标识双机模式下的两台设备。取值范围 1-2，默认设备 ID 为 1。

抢占模式：HA 主备模式下的抢占状态。启用后，选择抢占主或抢占备，在监控对象的状态完全正常的情况下，由该选项决定设备的主备状态。默认禁用。

心跳发送间隔：两台设备的心跳发送间隔。取值范围 1-3 秒，默认配置为 3 秒。

点击**提交**。

注意

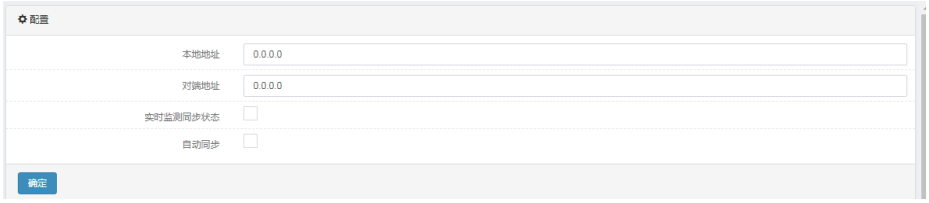
1. 两台设备的通信地址必须成对配置，并且不能指定为接口的浮动 IP。
2. 主主模式下，两台设备的单元 ID 必须指定为不同。
3. 主备模式下，两台设备的抢占模式必须成对配置。
4. 两台设备的心跳发送间隔必须配置为相同。

87.3 配置同步

防火墙设备 HA 功能可实现配置的手动同步、自动同步，当配置完一台设备后，用户可以把本设备上的配置同步到另一台设备上，既减少了用户配置的工作量，又保证了两台设备配置相同。

配置步骤：

进入**系统>高可用性>配置同步**，进入**配置同步**界面



本地地址：配置接收的本地地址，设备会在该地址上监听，用于接收配置。

对端地址：配置发送的对端地址，设备会往该地址发送本地配置。

实时检测同步状态：启用后，设备定时探测对端配置和本地配置是否相同。默认的探测间隔为 1 分钟。

自动同步：启用后，配置会自动同步到对端

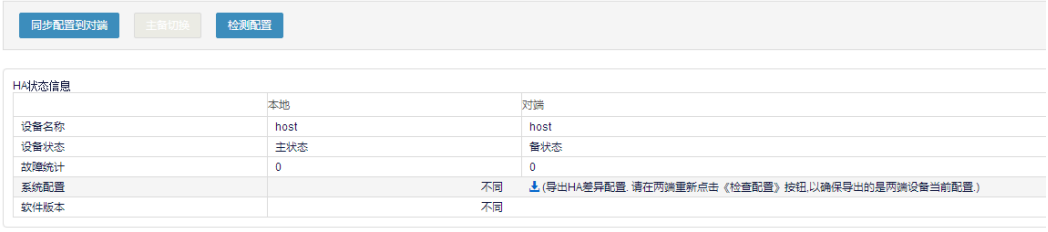
点击**确定。**

提示

1. 本地和对端地址可以和 HA 通信地址相同，不能指定为接口的浮动 IP。
2. 指定本地和对端地址后，可以在 HA 监控页面进行手动同步配置。
3. 启用实时监测同步状态后，可以在 HA 监控页面查看检测结果。
4. 两台设备中，只要有一台启用实时监测即可。
5. 配置同步功能，不会同步 HA 本身的配置，动态路由，CA 证书，VRRP，以及网络配置→接口、网络配置→设备 IP 相关的配置。

87.4 差异配置导出

HA 两端设备先分别点击系统>>高可用性>>监控页面下的“检测配置”按钮，当两端 HA 配置不同时，会在系统>>高可用性>>监控页面的系统配置显示栏后面会出现一个差异配置导出按钮，点击导出按钮即可导出两端设备的 HA 差异文件。



87.5 配置数据同步

数据同步包括四层连接同步和 FDB 表项同步。

为了保证故障切换时，已经建立的连接不中断，就必须进行连接同步。

在桥模式下，为了保证故障切换时，上下游交换机的 FDB 表项也及时切换，可以进行 FDB 表项同步。

配置步骤：

进入**系统>高可用性>数据同步**，进入**数据同步**界面。

首选通信地址：

本地：发送连接同步报文时的源地址

对端：发送连接同步报文时的目的地址

备选通信地址：

本地：发送连接同步报文时的源地址

对端：发送连接同步报文时的源地址

该地址为可选项，当首选地址发送失败时，使用备选通信地址，提高了连接同步的可靠性。

如果设备开启了连接同步，当需要同步的连接数量非常大时，会严重影响设备的性能。

FDB 表项同步，仅在透明模式下根据需求开启，路由模式下不应该启用。

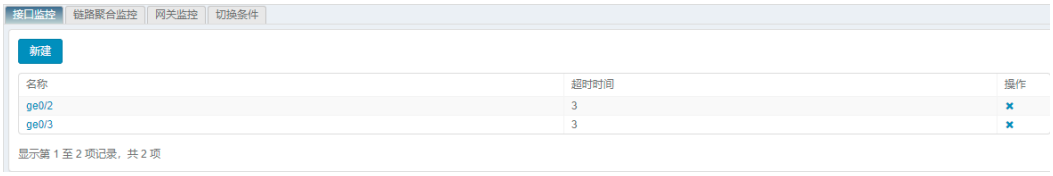
87.6 配置HA监控

HA 监控分网关监控、接口监控和链路聚合监控，实时监控设备上的运行状况，当出现监控故障时，会引起设备的状态切换，保证业务不中断。

87.6.1 配置接口监控

配置步骤：

进入**系统>高可用性>故障检测**，进入**接口监控**界面。



点击**新建**。

接口：需要监控的物理接口或 vlan 名称，可以监控用户认为重要的所有 vlan 和除了管理口之外的物理接口，监控基于物理接口或 VLAN 的 UP/DOWN。建议监控设备上下游直连的接口，这些接口的故障会造成业务的中断，必须进行故障切换。

超时时间：监控故障后，等待的超时时间，避免接口短时间内多次 up/down，引起 HA 状态频繁切换，造成设备不稳定。

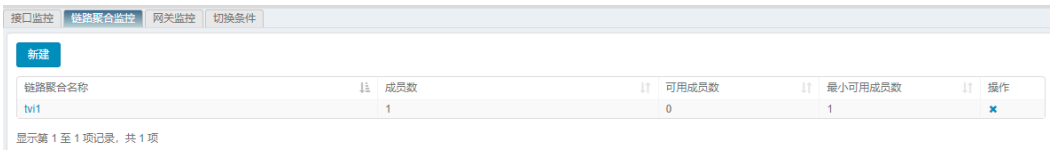
1. 选择需要监控的接口
2. 配置超时等待时间

点击**提交**。

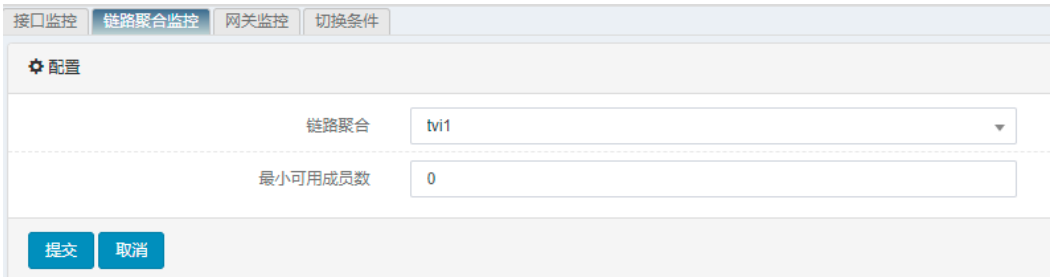
87.6.2 配置链路聚合监控

配置步骤：

进入**系统>高可用性>故障检测**，进入**链路聚合监控**界面。



点击**新建**。



链路聚合：需要监控的链路聚合名称。

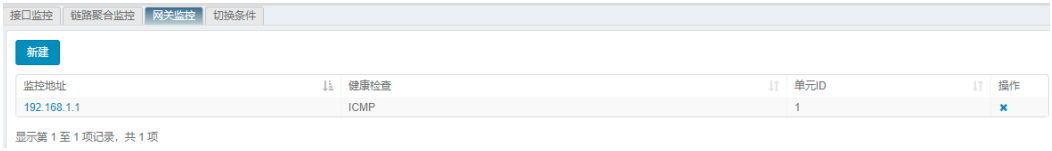
最小可用成员数：设置链路聚合接口中最少可用成员数，当可用成员数少于该值时，链路聚合接口故障。

1. 选择需要监控的链路聚合接口
2. 配置最小可用成员数
3. 点击**提交**

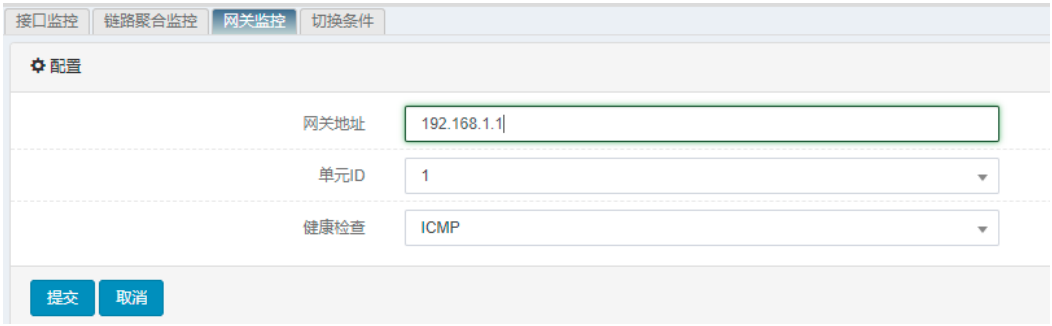
87.6.3 配置网关监控

配置步骤：

进入**系统>高可用性>故障检测**，进入**网关监控**界面。



点击**新建**。



网关监控：要监控的网关地址。

单元 ID：单元 ID 在主主模式下使用，标识网关监控所属的设备 ID，当该 ID 与设备的 ID 相同时，监控生效；当该 ID 与设备 ID 不相同时，只在主 A 状态下生效。

健康检查：下拉选择要配置的健康检查模板。健康检查模板的配置，参照**健康检查**一节

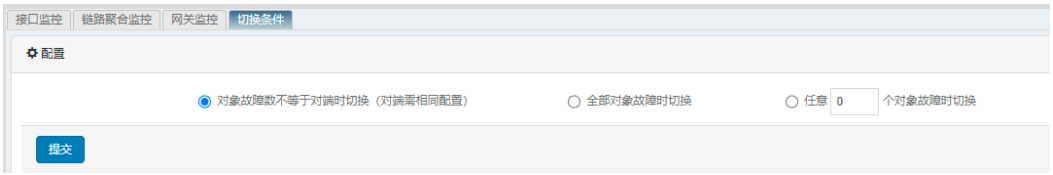
1. 选择要监控的网关地址
2. 选择监控所属的设备 ID
3. 选择健康检查模板
4. 点击**提交**

87.6.4 配置切换条件

配置步骤：

进入**系统>高可用性>故障检测**，进入**切换条件**界面，选择切换条件，点击

提交。



对象故障：是指接口监控、链路聚合监控和网关监控故障数之和。

87.7 HA状态控制

进入**系统>高可用性>监控**，可以查看当前本地和对端的 HA 状态。

同步配置到对端：当本地设备配置完毕后，点击同步配置到对端，可以将本地的配置同步到对端。

主备切换：主备模式下，当对端存在，主设备上可以点击主备切换按钮，进入备状态，同时使备设备进入主状态。

检测配置：可以点击该按钮，探测两端配置是否同步。

注意

1. 点击同步配置到对端，一段时间后页面会返回同步结果，此过程中请不要离开页面。
2. 同步配置到对端后，需要重启对端设备，配置才能生效。
3. 主主模式下不支持主备切换。
4. 主备模式下配置了抢占模式，不支持主备切换。

87.8 配置案例

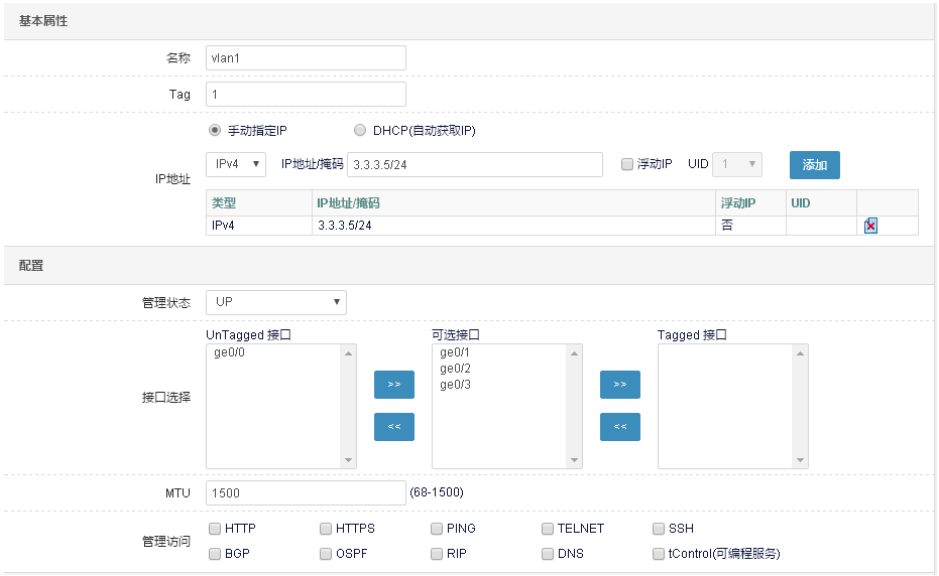
87.8.1 案例1：配置主备模式基本配置

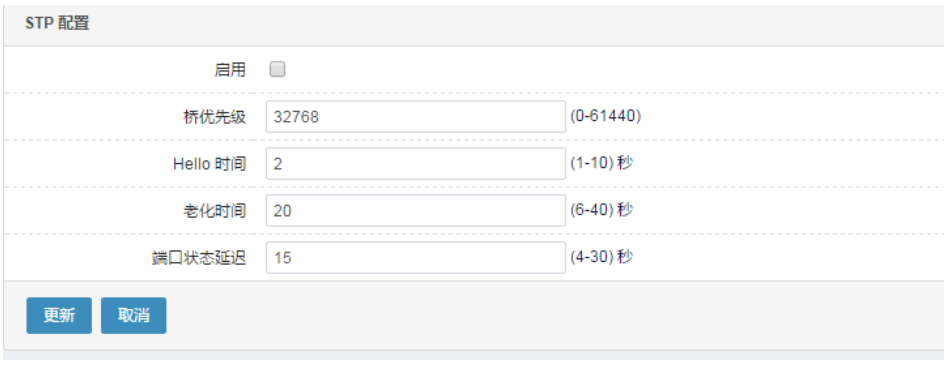
案例描述：

两台设备，FW_A,FW_B，分别配置，使之工作在主备模式下，并正确协商出主备状态。配置时可以选择 FW_A 为主设备，在 FW_A 上完成所有的配置后，再配置 FW_B 上 HA 模块相关配置，然后手工同步配置，这样 FW_B 上将拥有和 FW_A 一样的配置信息，开启实时监控同步状态.

配置步骤：

1. 配置 FW_A 进入**网络>接口>VLAN**，进入 **VLAN 列表**界面，点击**新建**，配置 HA 所需的接口 IP。





Tag：配置相应 VLAN 号，此处配置为 1

IP 地址：配置 IP 地址 3.3.3.5，**掩码：**24 位网络掩码，**浮动 IP：**不勾选

接口选择：选择相应物理接口以 tag/untag 方式加入 VLAN

其他相关参数请见具体章节

2. 点击**更新**，完成新建设备 **IP3.3.3.5** 重复以上操作创建接口 IP9.9.9.7。创建设备 IP**3.3.3.5** 绑定在 VLAN1 上，设备 IP**9.9.9.7** 绑定在 VLAN2 上，分别用于首备心跳地址。

3. 配置 FW_A,进入**系统>高可用性>配置**，进入**配置**界面。

工作模式：主备模式

首选通信地址：步骤 1 和 **2** 中创建的 3.3.3.5 地址，作为本地通信地址，对端设备需要创建 IP 地址 3.3.3.3。

备选通信地址：步骤 1 和 2 中创建的 9.9.9.7 地址，作为本地通信地址，对端设备

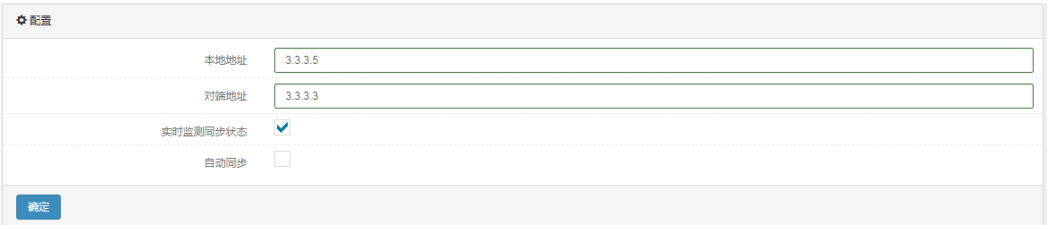
需要创建 IP 地址 9.9.9.7。

单元 ID：配置设备 ID 号为 1。

抢占模式：抢占主，本设备优先成为主设备。

心跳发送间隔：3 秒，每隔 3 秒发送一次心跳报文。

4. 配置 FW_A,进入**系统>高可用性**，进入**配置同步**界面。



本地地址：配置同步地址选择和首选通信地址相同的 IP 地址。如果用户想配置不同的 IP 地址，可重复**步骤 1** 和 **2** 创建新 IP 地址。

对端地址：对端设备需要创建设备 IP：3.3.3.3。

实时监测同步状态：勾选，实时探测两边的配置是否存在差异。

5. 配置 FW_A,进入**系统>高可用性**，进入**数据同步**界面。

首选通信地址：复用心跳备选通信地址 9.9.9.7 为本地地址，对端设备需要配置设备 IP9.9.9.9。

备选通信地址：可选配，本实例中没有配置。

连接同步：勾选，实时同步连接信息

FDB 表项同步：根据需要开启，开启后，同步 FDB 表项

6. 配置 FW_B，配置步骤请参照设备 FW_A，这里不再重复介绍。

到此 HA 主备工作模式配置完成。

7. 查看 HA 监控，进入**系统>高可用性>监控**页面。

8. HA 状态管理，进入**系统>高可用性>监控**页面。

同步配置到对端：当对端存在时，本地配置完毕后，同步本地配置到对端设备，确保两台设备的配置一致，同步配置后，需要重启设备才会生效。

主备切换：该操作会使主设备进入备状态，对端备设备进入主状态。主要用于手动进行状态切换。如果开启了抢占模式，此选项不可用。

检测配置：探测两边的配置是否一样，如果不一样，建议进行同步配置。

以上是 HA 主备模式的基本配置过程，如果需要添加故障监控，请按照本章中介绍故障监控的步骤配置相应的故障监控接口、链路聚合监控或者网关监控。需要让设备实现业务转发功能，还需要配置接口、路由、NAT 等其他相关的功能，具体配置步骤请参照对应模块的介绍。

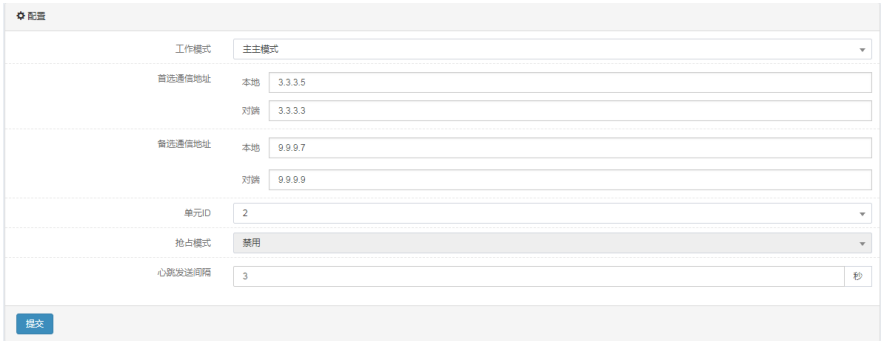
87.8.2 案例2：配置主主模式基本配置

案例描述：

两台设备，FW_A,FW_B，分别配置，使之工作在主主模式下，并正确协商出主主状态。在主主模式下两台设备均转发各自的业务流量，通过单元 ID 来区分，且开启配置自动同步功能

配置步骤：

1.主主模式所需设备 IP 配置步骤与主备模式一致，请参照主备模式配置过程。2.配置 FW_A，进入**系统>高可用性>配置**，进入**配置**界面。



工作模式：选择主主模式；

首先通信地址：步骤 1 中配置的地址。

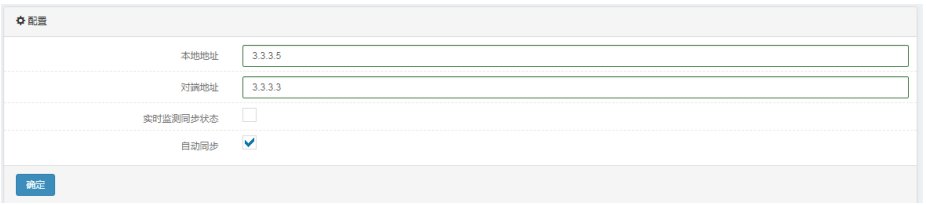
备选通信地址：步骤 1 中配置的地址。

单元 ID：设置设备单元 ID 号为 2，两台设备必须不一样。浮动 IP 也会有自己的 ID 号，只有与设备单元 ID 号相同的浮动 IP 才会在本设备上生效，否则不会生效。

抢占方式：主主模式下，抢占方式不生效。

心跳发送间隔：每 3 秒发送一次心跳。

3.配置 FW_A，进入**系统>高可用性**，进入**配置同步**界面，开启自动同步功能，如下图：



4.配置 FW_A，进入**系统>高可用性**，进入**数据同步**界面。配置步骤同主备模式一致，请参照主备模式配置步骤。

5.配置 FW_A，如果设备配置了浮动 IP，通过设置浮动 IP 的 ID 与设备单元 ID 相同，让浮动 IP 在本设备生效。进入**网络>接口>VLAN 列表**，选择需要配置的浮动 IP。

6.HA 状态管理，进入**系统>高可用性>监控**页面

同步配置到对端：同步本地配置到对端，配置同步后需要重启设备才会生效。

主备切换：主主模式下，主备切换按钮置灰为不可用状态，不能进行手动状态切换。

检测配置：检测两端的配置是否一致，不一致建议同步配置。

7.配置 FW_B，配置步骤请参照设备 FW_A，这里不再重复介绍。


注意

主主模式下，设备通过单元 ID，区分两台设备上的业务和配置，如果配置不正确，会造成业务无法正常工作。在修改设备单元 ID 时，对应的浮动 IP 也需要修改。

以上是 HA 主主模式的基本配置过程，如果需要添加故障监控，请按照本章中介绍故障监控的步骤配置相应的故障监控接口、链路聚合监控或者网关监控。，需要让设备实现业务转发功能，还需要配置接口、路由、NAT 等其他相关的功能，具体配置步骤请参照对应模块。

88 第88章 VRRP

88.1 VRRP概述

VRRP 简介

通常，同一网段内的所有主机都设置一条相同的以网关为下一跳的缺省路由。主机发往其他网段的报文将通过缺省路由发往网关，再由网关进行转发，从而实现主机与外部网络的通信。当网关发生故障时，本网段内所有以网关为缺省路由的主机将无法与外部网络通信。

缺省路由为用户的配置操作提供了方便，但是对缺省网关设备提出了很高的稳定性要求。增加出口网关是提高系统可靠性的常见方法，此时如何在多个出口之间进行选路就成为需要解决的问题。

VRRP（Virtual Router Redundancy Protocol，虚拟路由器冗余协议）将可以承担网关功能的路由器加入到备份组中，形成一台虚拟路由器，由 VRRP 的选举机制决定哪台路由器承担转发任务，局域网内的主机只需将虚拟路由器配置为缺省网关。

VRRP 是一种容错协议，在提高可靠性的同时，简化了主机的配置。在具有多播或广播能力的局域网（如以太网）中，借助 VRRP 能在某台设备出现故障时仍然提供高可靠的缺省链路，有效避免单一链路发生故障后网络中断的问题，而无需修改动态路由协议、路由发现协议等配置信息。

VRRP 备份组

VRRP 将局域网内的一组路由器划分在一起，称为一个备份组。备份组由一个 Master 路由器和多个 Backup 路由器组成，功能上相当于一台虚拟路由器。

虚拟 IP

虚拟路由器具有 IP 地址。局域网内的主机仅需要知道这个虚拟路由器的 IP 地址，并将其设置为缺省路由的下一跳地址，网络内的主机通过这个虚拟路由器与外部网络进行通信。

备份组中路由器的优先级

VRRP 根据优先级来确定备份组中每台路由器的角色（Master 路由器或 Backup 路由器）。优先级越高，则越有可能成为 Master 路由器。

备份组中路由器的工作方式

备份组中的路由器具有以下两种工作方式：

非抢占方式：如果备份组中的路由器工作在非抢占方式下，则只要 Master 路由器没有出现故障，Backup 路由器即使随后被配置了更高的优先级也不会成为 Master 路由器。

抢占方式：如果备份组中的路由器工作在抢占方式下，它一旦发现自己的优先级比当前的 Master 路由器的优先级高，就会对外发送 VRRP 通告报文。导致备份组内路由器重新选举 Master 路由器，并最终取代原有的 Master 路由器。相应地，原来的 Master 路由器将会变成 Backup 路由器。

备份组中路由器的认证方式

VRRP 提供了两种认证方式：

Text：简单字符认证。在一个有可能受到安全威胁的网络中，可以将认证方式设置为 Text。发送 VRRP 报文的路由器将认证字填入到 VRRP 报文中，而收到 VRRP 报文的路由器会将收到的 VRRP 报文中的认证字和本地配置的认证字进行比较。如果认证字相同，则认为接收到的报文是真实、合法的 VRRP 报文；否则认为接收到的报文是一个非法报文。

MD5：MD5 认证。在一个非常不安全的网络中，可以将认证方式设置为 MD5。发送 VRRP 报文的路由器利用认证字和 MD5 算法对 VRRP 报文进行加密，加密后的报文保存在 Authentication Header（认证头）中。收到 VRRP 报文的路由器会利用认证字解密报文，检查该报文的合法性。

在一个安全的网络中，用户也可以不设置认证方式。


注意

在 VRRPv3 版本模式下，不支持认证。

VRRP 定时器

1. VRRP 通告报文时间间隔定时器

用户可以通过设置 VRRP 定时器来调整 Master 路由器发送 VRRP 通告报文的时间间隔。如果 Backup 路由器在等待了 3 个间隔时间后，依然没有收到 VRRP 通告报文，则认为自己是 Master 路由器，并对外发送 VRRP 通告报文，重新进行 Master 路由器的选举。

2. VRRP 抢占延迟时间定时器

在性能不够稳定的网络中，Backup 路由器可能因为网络堵塞而无法正常收到 Master 路由器的报文，导致备份组内的成员频繁的进行主备状态转换。用户可以通过设置 VRRP 抢占延迟时间的方法来解决这个问题。

设置了 VRRP 抢占延迟时间后，Backup 路由器会在等待了 3 倍的通告报文时间间隔后，再等待 VRRP 抢占延迟时间。如在此期间还是没有收到 VRRP 通告报文，则此 Backup 路由器将认为自己是 Master 路由器，对外

发送 VRRP 通告报文，触发备份组内路由器进行 Master 路由器的选举。

VRRP 报文格式

支持 VRRPv2 和 VRRPv3 两种格式的报文。

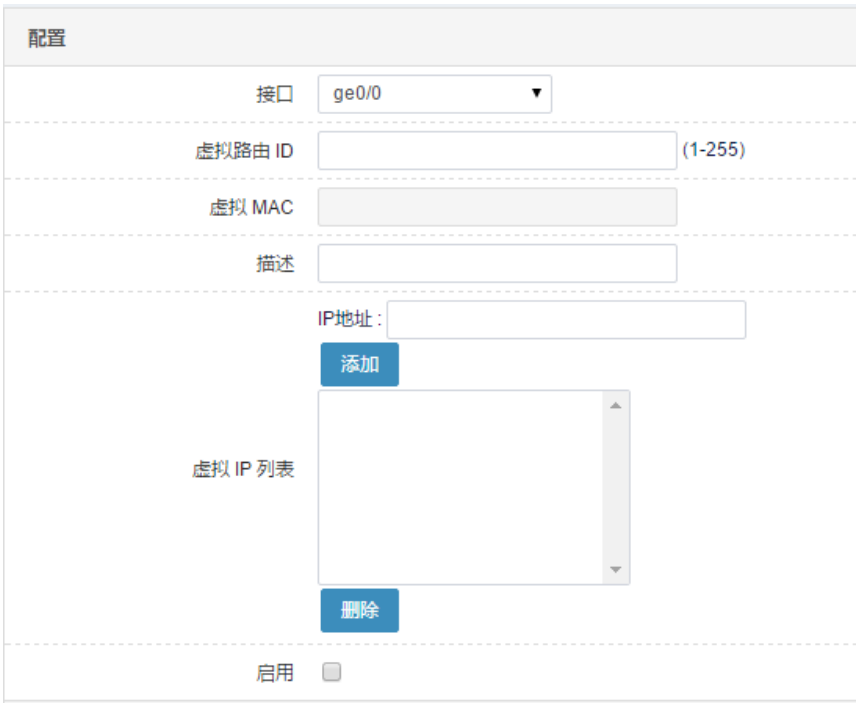
88.2 配置VRRP

88.2.1 配置VRRP

配置步骤：

1. 在**网络>接口>VLAN** 列表中，为一个 VLAN 接口配置好 IP 地址。
2. 新建 VRRP 备份组。

进入**系统> VRRP**，点击“新建”按钮。如下图：



接口：接口列表中包含所有可用接口。

虚拟路由 ID：设置 VRRP 备份组的组号，取值范围 1~255。

在一个接口下，VRID 必须唯一，不能重复；但在不同接口下，可以重复使用。

虚拟 MAC：配置虚拟路由 ID 之后自动生成。

描述：用于管理目的的说明性信息。

虚拟 IP 列表：设置备份组的虚拟 IP 地址。

- 虚拟路由器的 IP 地址可以是备份组所在网段中未被分配的 IP 地址，

也可以和备份组内的某个路由器的接口 IP 地址相同。

- 接口 IP 地址与虚拟 IP 地址相同的路由器被称为“IP 地址拥有者”，优先级被强制为 255（最高优先级）。
- 在同一个 VRRP 备份组中，只允许配置一个 IP 地址拥有者。
- 如果接口连接多个子网，则可以为一个备份组配置多个虚拟 IP 地址，以便实现不同子网中路由器的备份。
- 虚拟 IP 地址不能为全零地址(0.0.0.0)、广播地址(255.255.255.255)、环回地址、非 A/B/C 类地址和其它非法 IP 地址(如 0.0.0.1)。
- 只有配置的虚拟 IP 地址和接口 IP 地址在同一网段，且为合法的主机地址时，备份组才能够正常工作；否则，如果配置的虚拟 IP 地址和接口 IP 地址不在同一网段，或为接口 IP 地址所在网段的网络地址或网络广播地址，虽然可以配置成功，但是备份组不会生效。

启用：是否开启该 VRRP。

高级选项：高级选项中包含了一些高级功能。如下图：

优先级：VRRP 优先级的取值范围为 0 到 255（数值越大表明优先级越高），可配置的范围是 1 到 254，优先级 0 为系统保留给特殊用途来使用，255 则是系统保留给 IP 地址拥有者。当路由器为 IP 地址拥有者时，其运行优先级始终为 255。因此，当备份组内存在 IP 地址拥有者时，只要其工作正常，则为 Master 路由器。

VRRP 版本：使用 VRRPv2 或 VRRPv3 格式的报文。

抢占模式与抢占延迟：在使能抢占模式的前提下，抢占延迟的可选范围为 0~255 秒。

通告间隔：可选范围为 10~25500 亚秒（1 亚秒=1/100 秒）。

认证方式：在 VRRPv2 版本下，有“None”（不认证），“Text”（简单字符

认证）与“MD5”（MD5 认证）三种选择；在 VRRPv3 版本下，没有认证选项。

是否可 Ping：按照 VRRP 协议的规定，如果虚拟 IP 与接口上任何真实 IP 都不相同，那么虚拟 IP 是无法 Ping 通的。但很多用户都有 Ping 网关的习惯，所以如果想让虚拟 IP 可以被 Ping，就使能这个选项。

3. 点击“提交”按钮，新建完成。

88.2.2 编辑VRRP备份组

在已经建立好的备份组的操作选项中，点击虚拟路由 ID 下面的蓝色字符串按钮。如下图：

状态	虚拟路由 ID	描述	虚拟IP	接口	优先级	
■	1	vrrp1	10.10.10.10	vlan	100	✖

各选项的意义与“新建”时相同，唯一区别是“**接口**”和“**虚拟路由 ID**”不能修改。

88.2.3 删除VRRP备份组

在已经建立好的备份组的操作选项中，点击“✖”按钮，经确认后删除。

注意

如果备份组所属的接口被“注销”，如 vlan 下的物理接口被热拔除或者 vlan 接口被删除，那么该接口下所有的备份组都将自动被删除。

88.2.4 查看VRRP备份组

进入 VRRP 配置页面，如下图：

状态	虚拟路由 ID	描述	虚拟IP	接口	优先级	
■	1	vrrp1	10.10.10.10	vlan	100	✖

状态：显示■ - “Initialize”，○ - “Backup”或● - “Master”三种状态中的一种，其中“Backup”和“Master”属于工作状态。

虚拟路由 ID：显示备份组组号。

虚拟 IP：显示多个虚拟 IP 地址。

接口：VRRP 所属 VLAN 接口。

优先级：显示优先级。

88.3 配置案例

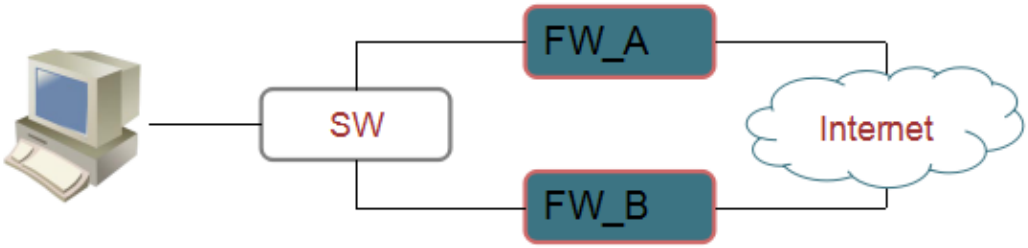
88.3.1 配置案例1（单备份组）

案例描述：

单备份组方式表示业务仅由 Master 路由器承担。当 Master 路由器出现故障时，才会从其他 Backup 路由器选举出一个接替工作。主备备份方式仅需要一个备份组，不同路由器在该备份组中拥有不同优先级，优先级最高的路由器将成为 Master 路由器。

在 LAN 中，主机使用 192.168.31.1 这个 IP 地址作为它们的默认网关。把 FW_A 和 FW_B 两台路由器组成一个备份组 1。

拓扑描述：



配置步骤：

1. 在 FW_A 进入**系统>VRRP**，点击**新建**按钮，如下图配置：

VRID 设置为 1，优先级为 100，虚拟 IP 为 192.168.31.1，启用备份组后提交。

2. 在 FW_B 进入**系统>VRRP**，点击“新建”按钮，如下图配置：

VRID 设置为 1，优先级为 50，虚拟 IP 为 192.168.31.1，启用备份组后提交。

3. 配置好后，查看两台设备的 VRRP 状态，一个为 Master，一个为

Backup。

88.3.2 配置案例2（多备份组负载分担）

案例描述：

在一个接口上可以创建多个备份组，使得该路由器可以在一个备份组中作为 Master 路由器，在其他的备份组中作为 Backup 路由器。

负载分担方式是指多台路由器同时承担业务，因此负载分担方式需要两个或者两个以上的备份组，每个备份组都包括一个 Master 路由器和若干个 Backup 路由器，各备份组的 Master 路由器可以各不相同。

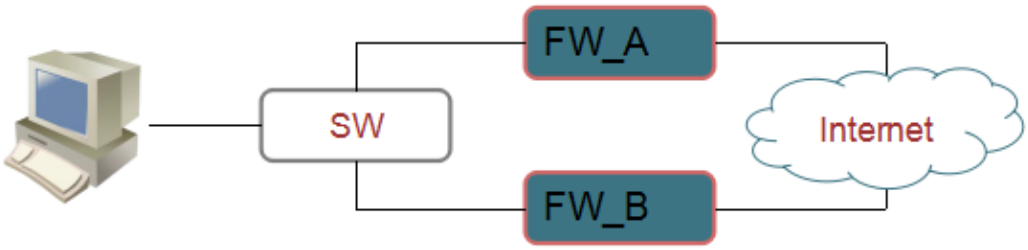
在 LAN 中，用 FW_A 和 FW_B 两台路由器创建两个备份组：

备份组 1：FW_A 作为 Master 路由器，FW_B 作为 Backup 路由器，虚拟 IP 为 192.168.31.1。

备份组 2：FW_A 作为 Backup 路由器，FW_B 作为 Master 路由器，虚拟 IP 为 192.168.31.2。

为了实现业务流量在 FW_ A、和 FW_B 之间进行负载分担，需要将局域网内的主机的默认网关分别设置 192.168.31.1 和 192.168.31.2。在配置优先级时，需要确保两个备份组中各路由器的 VRRP 优先级形成交叉对应。

拓扑描述：



配置步骤：

1. 在 FW_A 进入**系统管理>VRRP**，点击**新建**按钮，如配置案例 1。

VRID 设置为 1，优先级为 100，虚拟 IP 为 192.168.31.1，启用备份组后提交。

2. 在 FW_A 上继续配置备份组 2，如下图配置：

VRID 设置为 2，优先级为 50，虚拟 IP 为 192.168.31.2，启用备份组后提交。

3. 在 FW_B 进入**系统管理>VRRP**，点击“新建”按钮，如配置案例 1。

VRID 设置为 1，优先级为 50，虚拟 IP 为 192.168.31.1，启用备份组后提交。

4. 在 FW_B 上继续配置备份组 2，如下图配置：

VRID 设置为 2，优先级为 100，虚拟 IP 为 192.168.31.2，启用备份组后提交。

88.4 常见故障

故障现象：配置好的备份组在启用后一直不工作

现象	配置好了一个备份组，在启用后一直显示处于“Initialize”状态
分析	备份组所属接口没有处于UP状态，或者网线没有插好。
解决	有时候备份组即使被启用了，但仍然无法工作，因为备份组进入工作状态的前提条件是： 1.接口处于 UP 状态 2.接口网线上能检测到载波信号 3.接口上至少配置了一个真实 IP 地址 4.备份组至少配置了一个虚拟 IP 地址 5.备份组被启用 以上条件如果任何一个没有被满足，该备份组都无法进入工作状态。

89 第89章 SNMP

89.1 SNMP概述

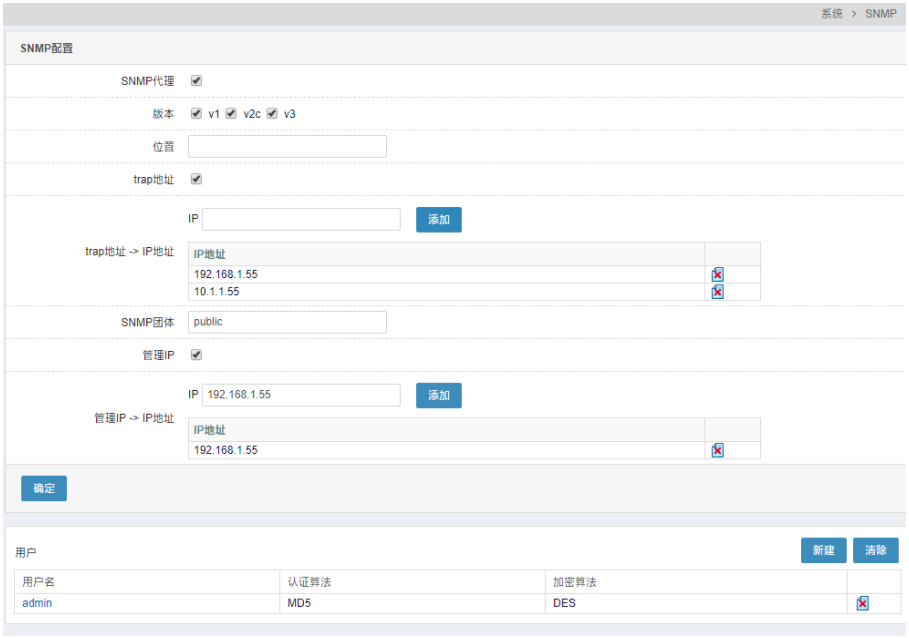
简单网络管理协议（SNMP），由一组网络管理的标准组成，该协议能够支持网络管理系统，用以监测连接到网络上的设备是否有任何引起管理上关注的情况。

89.2 SNMP配置

89.2.1 配置SNMP

配置步骤：

1. 进入**系统>SNMP：**



SNMP 代理：选中为启动 SNMP 代理。

版本：选择是否启用 v1、v2c、v3 版本的 SNMP。

位置：输入系统所在的物理位置描述字串。

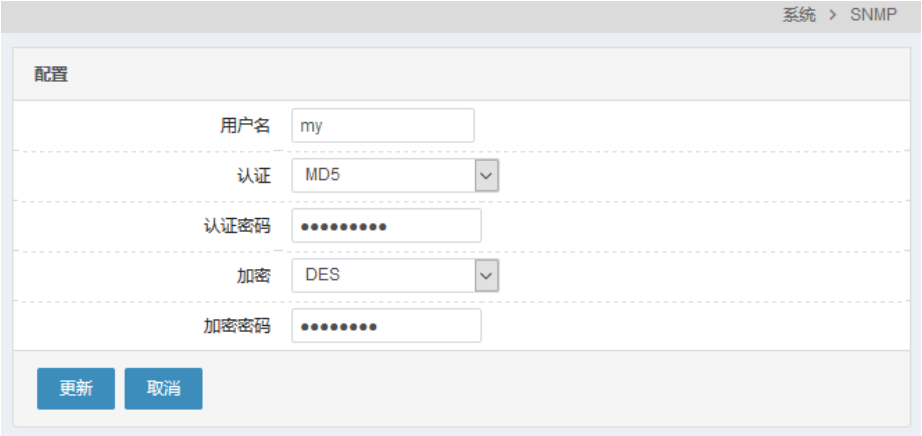
Trap 地址：添加 trap 信息接收端 IP 地址。

SNMP 团体：输入 SNMP 代理认证口令,默认为 public。

管理 IP：选中并添加 IP 地址，则启动管理 IP 过滤。

IP 地址：添加管理 IP 地址，用于对管理 IP 过滤

用户：建立管理用户，用于对 V3 版本的权限设置。



用户名：SNMP V3 认证所需要的用户名。

认证：选择认证方式，可以选择 none、MD5 和 SHA。

认证密码：输入认证密码。

加密：选择加密方式，可以选择 none、DES 和 AES。

加密密码：当加密方式不为 none 时，需要输入加密密码。

注意

该 snmp v3 认证用户的认证方式及密码，需要同 snmp 客户端上配置的用户保持一致。

配置步骤：

1. 勾选启用 **SNMP 代理。**
2. 选择是否启用 **v1、v2c、v3** 版本的 SNMP
3. 输入**位置**。
4. 添加 **trap 地址**。
5. 输入 **SNMP 团体**。
6. 点击**确定**。
7. 如果是 V3 版本需要用户认证，点击**新建**。
8. 在弹出框中配置**用户名**、**认证**方式、**认证密码**、**加密方式**、**加密密码**。
9. 点击**更新**。

89.2.2 配置案例

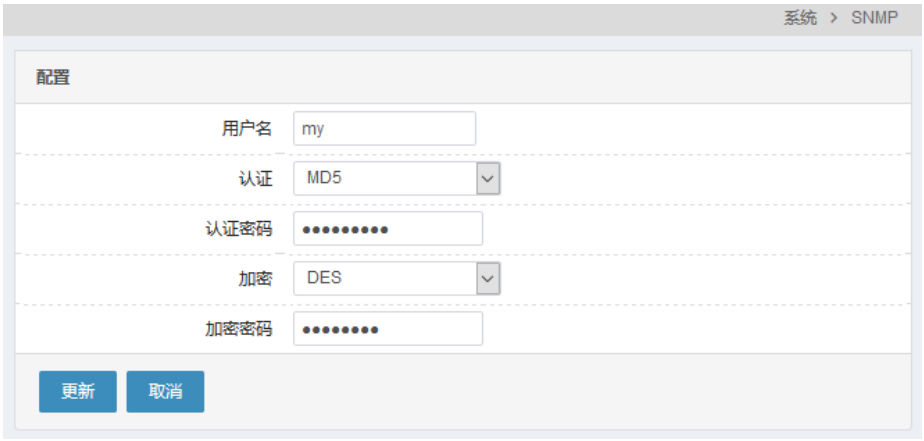
配置案例：配置 SNMP

案例描述:

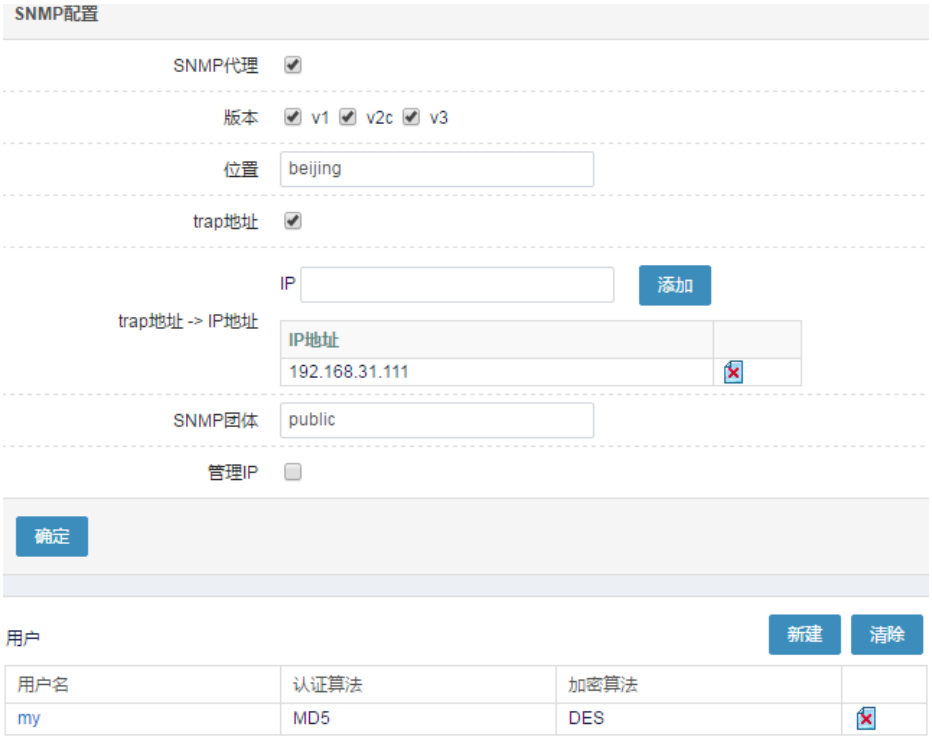
设置启动 snmp 代理，物理位置为 beijing，trap 地址为 192.168.31.111，snmp 团体为 public，建立一个 V3 认证用户，用户名为 my，采用 MD5 认证算法和 DES 加密算法，认证密码与加密密码均为 1234578。

配置步骤:

1. 进入**系统管理>SNMP**，配置 v3 认证用户：



2. 输入其他参数，启用 snmp 代理，启用 v3 版本，如下图：



通过如上配置，可以使用 mib browser 等 snmp 客户端工具访问设备的 snmp 功能，在该工具上要配置相应的 snmp v3 用户信息，可获取设备相应信息。

默认 snmp 客户端工具中自带 RFC1213 mib 库，若要读取设备私有信息，

需要导入公司私有 mib 库文件。

90 第90章 无线配置

90.1 无线网络概述

部分型号的防火墙添加了 Wi-Fi 功能模块和蜂窝移动网络功能模块。Wi-Fi 功能支持 802.11n 协议，能够让移动终端通过 Wi-Fi 连接到防火墙，进而实现无线网络的访问策略控制。蜂窝移动网络功能模块，通过插入运营商提供的 4G SIM 卡，可以让防火墙、及其下的网络通过蜂窝网络访问互联网。通过这两项功能，能够保障企业无线网络、物联网的信息安全。

90.2 配置无线网络

90.2.1 配置Wi-Fi

1. 配置 Wi-Fi 之前，需要配置 Wi-Fi 接口相应的 IP 地址、DHCP 服务器。
2. 进入**网络>无线配置>Wi-Fi**。

参数说明：

名称：即 Wi-Fi 的 SSID。

国家：可以指定防火墙工作的国家或地区，以兼容不同国家或地区的信道。

频段：指定防火墙 Wi-Fi 工作在 2.4GHz 或 5.0GHz 频段。

信道：指定防火墙 Wi-Fi 工作的信道。

认证方式：指定防火墙 Wi-Fi 的认证方式，如果选择 none，则不需要密码。

密码：指定防火墙 Wi-Fi 的认证密码。

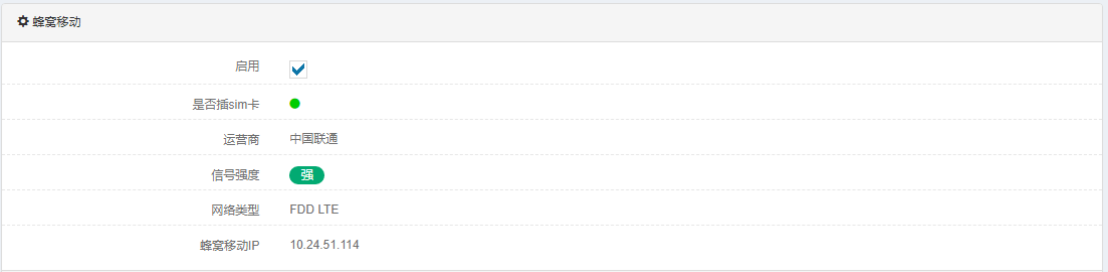
3. 点击**提交**。

注意

1. 防火墙上，Wi-Fi 所对应的物理接口为 ge_wlan。
2. 防火墙 Wi-Fi 只能工作在一种频段下。
3. 认证的密码至少需要 8 位。

90.2.2 配置蜂窝移动网络

1. 进入**网络>无线配置>蜂窝移动。**



参数说明：

启用：即开启、关闭蜂窝网络。

是否插 SIM 卡：检测防火墙是否插入了 SIM 卡。正确插入了 SIM 卡，此处显示为绿色，否则为红色。

运营商：如果注网成功，此处会显示蜂窝移动网络的提供商。

信号强度：显示当前蜂窝移动网络的信号强度，绿色为强，黄色为中，红色为差。

网络类型： 显示网络类型，如 FDD LTE 等

蜂窝移动 IP：防火墙从蜂窝移动网络运营商处获得的 IP 地址。

注意

1. 防火墙所支持的 SIM 卡为标准卡 Standard SIM，而非 Mini SIM、Nano SIM、Micro SIM。
2. SIM 卡不支持热插拔。请在防火墙断电的情况下，插拔 SIM 卡
3. 防火墙上，蜂窝移动网络所对应的物理接口为 ge_lte。
4. ge_lte 接口获取运营商 IP 地址的方式为 PPPoE。

90.3 配置案例

90.3.1 无线网络配置案例

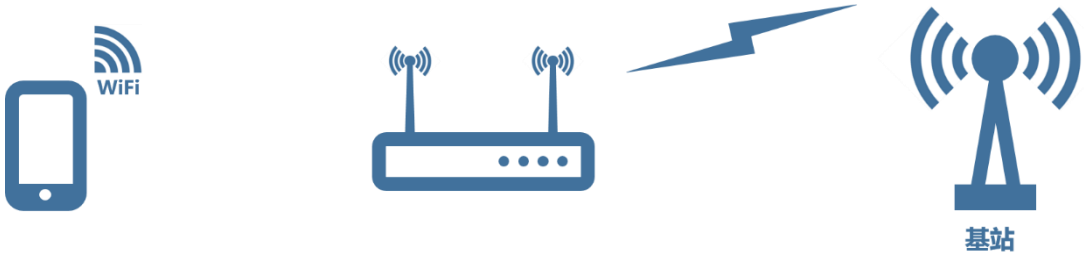
案例描述：

企业的移动终端和物联网终端需要能够访问互联网。但由于没有铺设线缆，无法通过有线网络组网。并且为了信息安全，需要一台防火墙来隔离内外网络。此时配置了无线功能模块的防火墙正好可以用来解决这个需求。

用户需求如下：

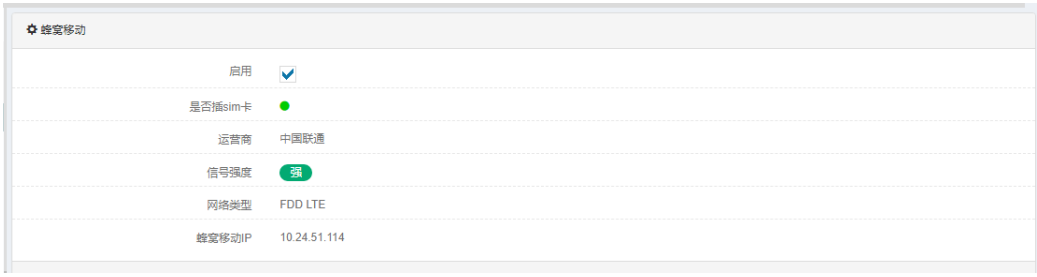
1. 企业内网的移动终端、物联网终端经过防火墙的访问控制策略，可以访问互联网。而外网试图访问企业内网的行为则被阻断。
2. 由于没有布置互联网专线，需要使用联通 4G 蜂窝网络来访问互联网。

配置案例组网图：

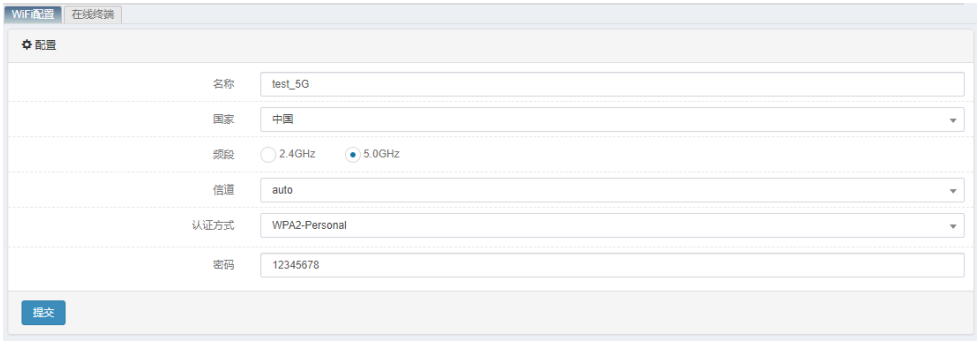


配置步骤：

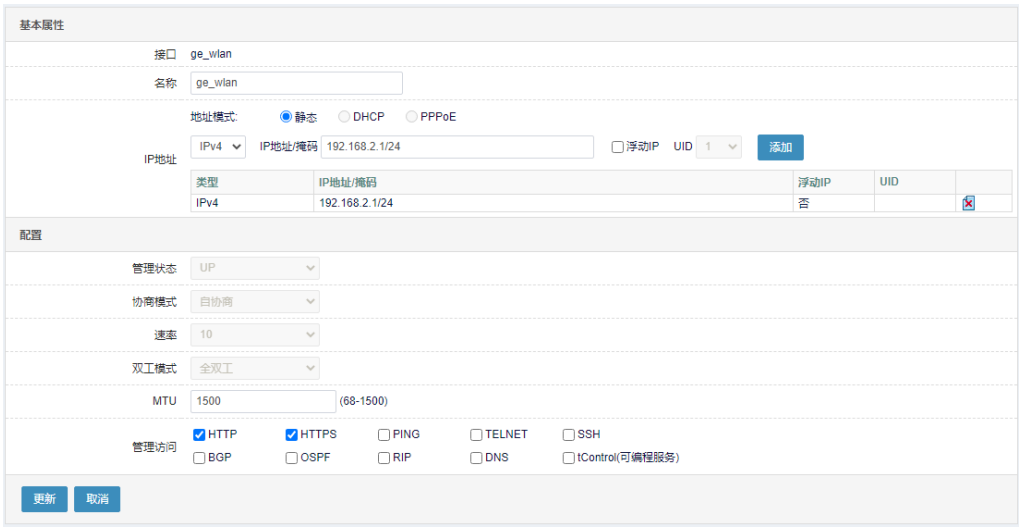
1. 在防火墙断电的情况下，将 SIM 插入防火墙的 SIM 卡槽。
2. 进入**网络>无线配置>蜂窝网络**，启用蜂窝网络。



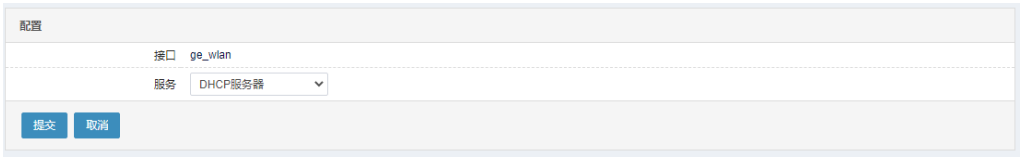
3. 进入**网络>无线配置>Wi-Fi**，根据需求配置**名称、频道、认证方式**和**密码**，点击**提交**。



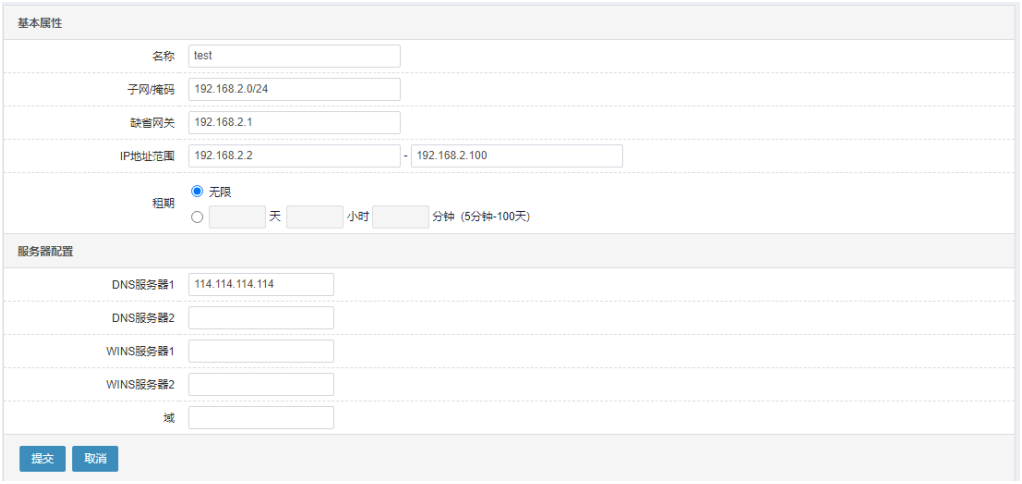
4. 进入**网络>物理接口**，给 ge_wlan 配置 IP 地址。点击**更新**。



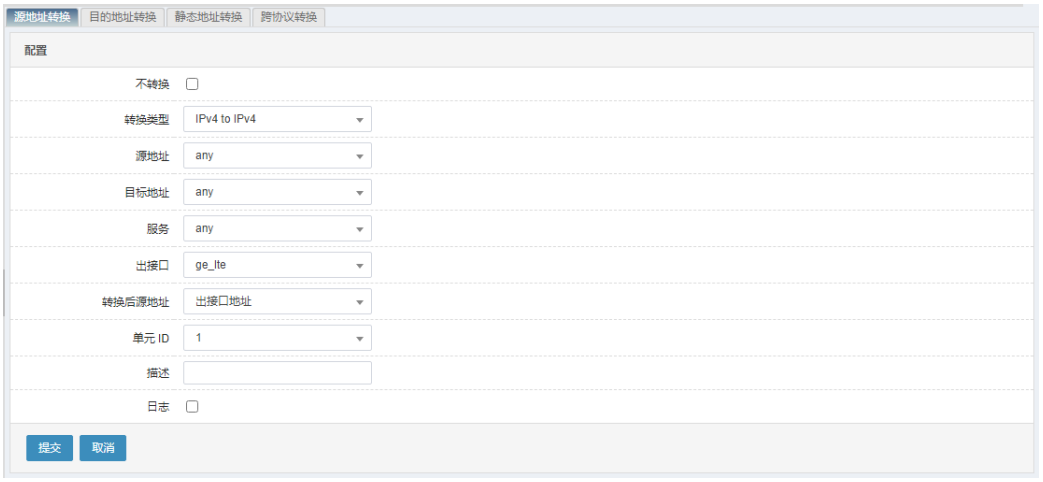
5. 进入**网络>DHCP>服务**，将 ge_wlan 接口开启 DHCP 服务器。点击**提交**。



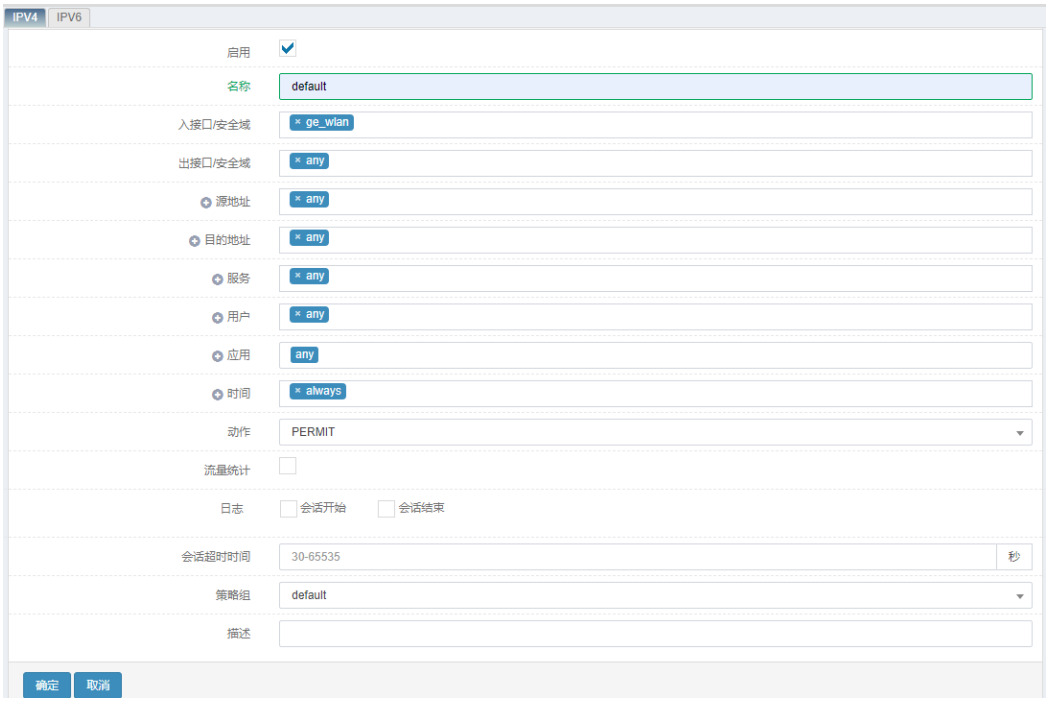
6. 进入**网络>DHCP>服务器**，配置 DHCP 服务器。配置 DHCP 服务器**名称、子网/掩码、网关、IP 地址范围、DNS 服务器**，点击**提交**。



7. 进入**网络>NAT>源地址转换**，配置一条出接口为 ge_lte，转换后源地址为出接口地址的源 NAT。点击**提交**。



8. 进入**策略>防火墙>策略>新建策略**，新建一条入接口为 ge_wlan、出接口为 ge_lte 的允许策略。只允许从 Wi-Fi 向蜂窝网络访问的流量通过。点击**确定**。



至此，案例配置完成。移动终端可以通过 Wi-Fi 连接防火墙，经过防火墙的防护策略保护后，再通过 4G 蜂窝移动网络访问互联网。

90.4 常见故障分析

90.4.1 Wi-Fi连接失败

现象	配置Wi-Fi后，移动终端连接Wi-Fi失败。
分析	分析可能为以下几种情况： 1. Wi-Fi名称即SSID错误。 2. 移动终端不支持5G频段。 3. 移动终端的不支持所设国家的信道。 4. 未配置DHCP服务器。
解决	1. 确认移动终端所连接的SSID是否正确。 2. 修改防火墙的Wi-Fi频段为2.4GHz。 3. 修改防火墙Wi-Fi的信道，使之与移动终端所支持的信道相匹配。 4. 将ge_wlan开启DHCP服务，并配置DHCP服务器。

90.4.2 移动终端无法访问互联网

现象	移动终端成功连接防火墙Wi-Fi后，却无法访问互联网。

分析	分析可能为以下几种情况： 1. 未启用蜂窝移动网络。 2. 蜂窝移动网络信号弱。 3. 所配置的其它路由与通过蜂窝网络所获得的网关冲突。 4. 未配置源NAT。 5. 防火墙策略未生效。
解决	1. 开启蜂窝网络，查看是否能正确获得运营商分配的IP地址。 2. 观察蜂窝网络的信号状态，调整防火墙的位置，以获得更好的网络信号。 3. 调整其它路由及所获得的网关距离，使蜂窝网络的网关生效。 4. 配置出接口为ge_lte，转换后源地址为出接口地址的源NAT。 5. 检查防火墙策略是否启用，匹配是否正确。