神州云科 Yunke China | DCN

DCFW-1800E-X 系列下一代防火墙 WEB 管理手册

---201902

目录

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**下一代防火墙设备（NGFW）**。在进行 Web 管理前，必须配置下一代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、Mozilla22.0 及以上版本、chrome27.0 浏览器，最佳显示分辨率为 1024×768。

1.2 Web管理

Web 管理界面由**导航条、菜单、**和**主内容区**页面组成，每个导航标签里有相应的一个或多个子项目。当点击一个导航页，如统计，左侧显示菜单项目，右侧为主内容区。

1.2.1 导航

导航提供了下一代防火墙设备的信息统计和主要配置选项。

概况：系统相关的一些关键信息展示。包括状态、接口、流量、在线用户等概要信息显示，方便直接查看。

统计：一些数据统计结果的显示，包括用户流量、设备健康信息等。

策略：策略相关配置。包括用户策略、应用策略、防护策略、协议、流量策略等。

网络：网络相关配置。接口、路由、DNS、IPSEC 等。

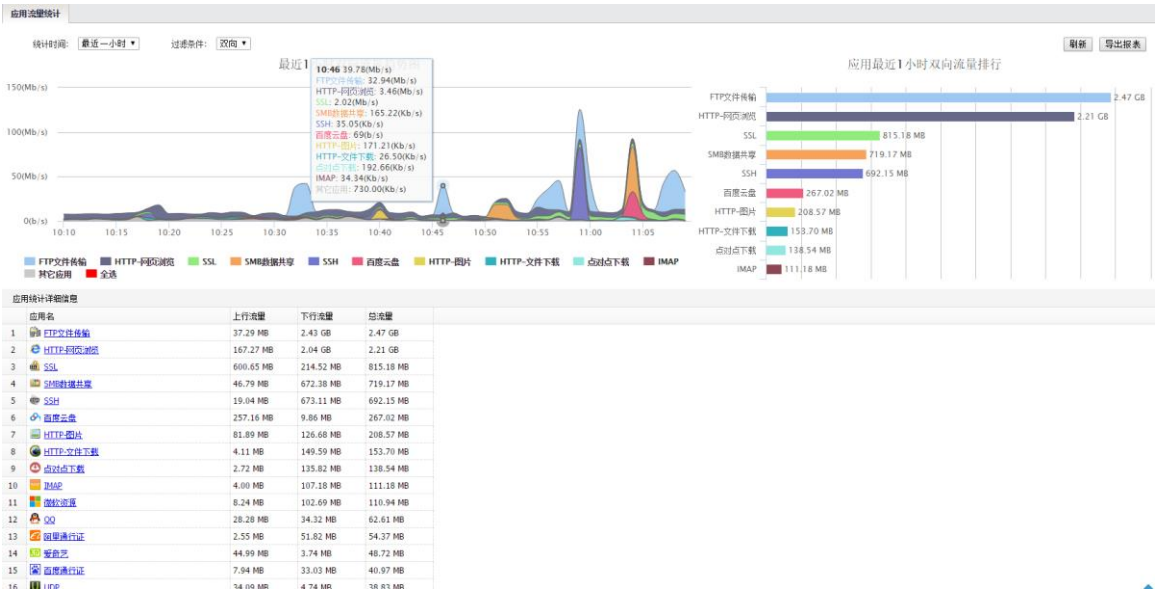
对象：对象相关配置。包括用户、关键字，应用、服务、地址、时间，设备健康检查、CA 证书等。

日志：类别日志查询。包括系统、安全、NAT、应用控制、入侵防御、病毒防护日志。

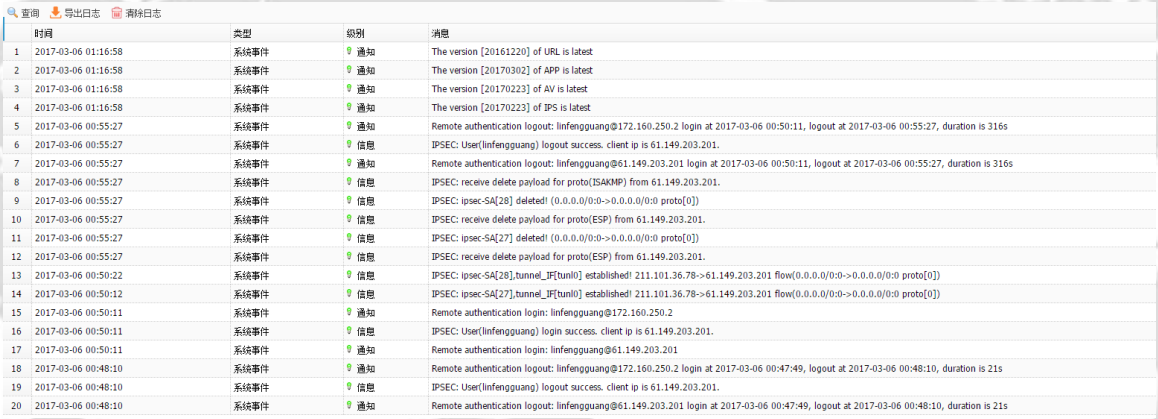
系统：系统功能配置。包括管理员配置、可用性、系统维护等。

1.2.2 主内容区

主内容区是显示配置和信息的界面，在不同导航项目中有不同的表现形式。在“**统计**”导航标签下，统计信息主要以图表的形式直观的展现出来，不同项目信息以不同颜色加以显示，方便查看。



在**“日志”，“策略”，“网络”**等导航标签下，信息主要以表格的形式展现，更加贴近用户的使用习惯。



1.2.3 菜单

除“**概况**”之外，其他导航页面左侧都有可折叠的浮动**菜单栏**。菜单栏中可以选择不同的配置项目进行细节配置或查看。

1.3 设备默认配置

出厂的设备有默认的配置。这些默认配置保证了用户不需要进行额外配置就能够通过 Web 对下一代防火墙设备进行管理、配置。

1.3.1 管理接口的默认配置

管理接口（MGT）的默认地址配置为 192.168.1.200/24。

1.3.2 默认管理员用户

系统默认的管理员用户为 admin，密码为 admin。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 admin.audit。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 admin.user。用户可以使用这个账号用于配置系统管理员。

第2章 系统信息

2.1 系统信息概述

通过 Web 登录设备后默认进入“**概况**”页面，该页面显示系统当前运行状态和高级别日志信息。本章介绍该页面中各个部分。

2.2 概况

进入**“概况”**，可以查看系统概况。

2.2.1 查看主机信息

进入**概况**，可以看到系统主机信息。

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：下一代防火墙设备的唯一标识，是设备出厂时设定好的。
版本号：当前设备运行的系统软件的版本号。
系统时间：表示系统当前时间。
应用特征库：应用特征库版本信息
入侵防御特征库：入侵防御特征库版本信息
病毒防护特征库：病毒防护特征库信息
系统运行时间：表示系统从上次启动已经运行的时间。

2.2.2 修改主机名

为了方便区分设备，有时候需要修改主机名。

配置步骤：

1、**系统>系统设置>设备**，在配置里修改主机名称，修改之后点击“**确定**”即可修改成功。

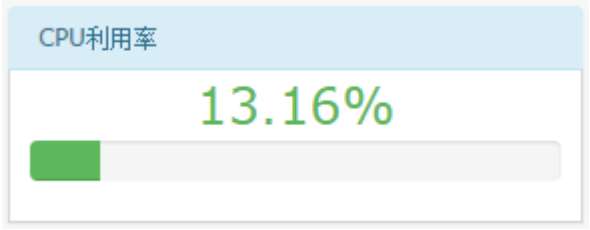
2.2.3 查看接口信息

进入**概况**，可以查看当前下一代防火墙的产品接口示意图。

图中，设备的物理接口示意图，当前在线的接口显示为蓝色，没有连接网线的接口则显示为灰白色。当鼠标位于接口图上时，可以显示接口的信息，包括接口名称、链路状态等。虚线框表示接口板卡位置，设备插上接口板时，会显示接口板状态。

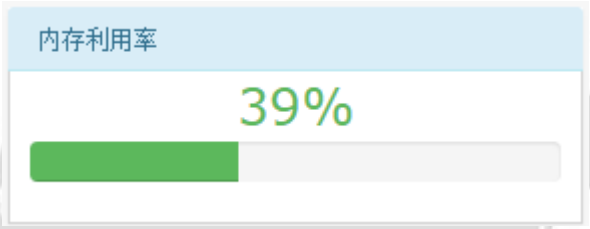
2.2.4 查看 CPU 使用情况

进入**概况**，可以查看当前 CPU 当前使用情况。



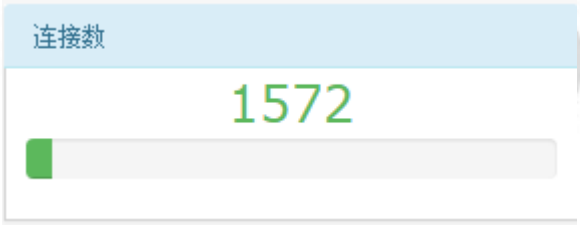
2.2.5 查看内存使用情况

进入**概况**，可以查看当前系统内存当前使用情况。



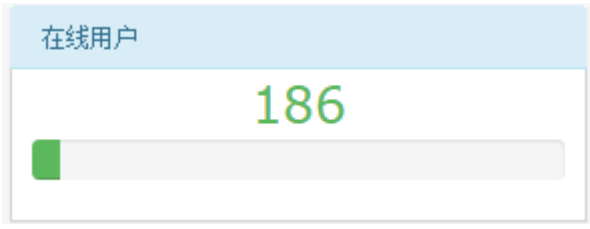
2.2.6 查看总连接数

显示当前连接数。



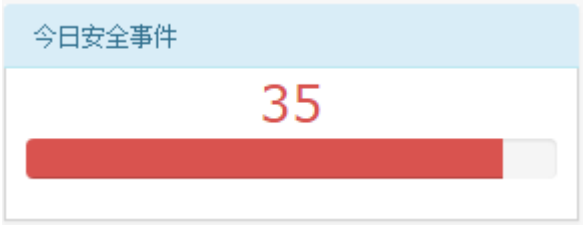
2.2.7 查看在线用户数

显示当前在线用户总数。

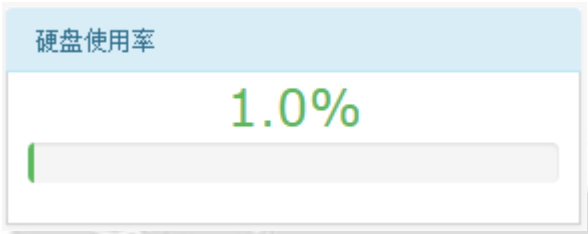


2.2.8 查看今日安全事件数

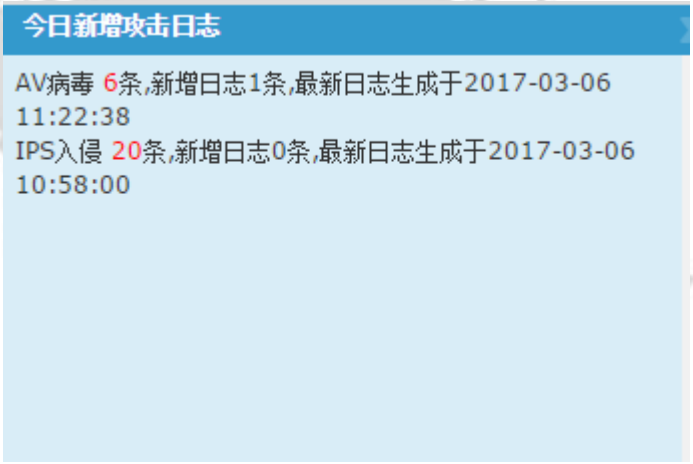
显示今日安全事件总数



2.2.9 查看硬盘利用率



2.2.10 告警弹窗



第3章 统计信息

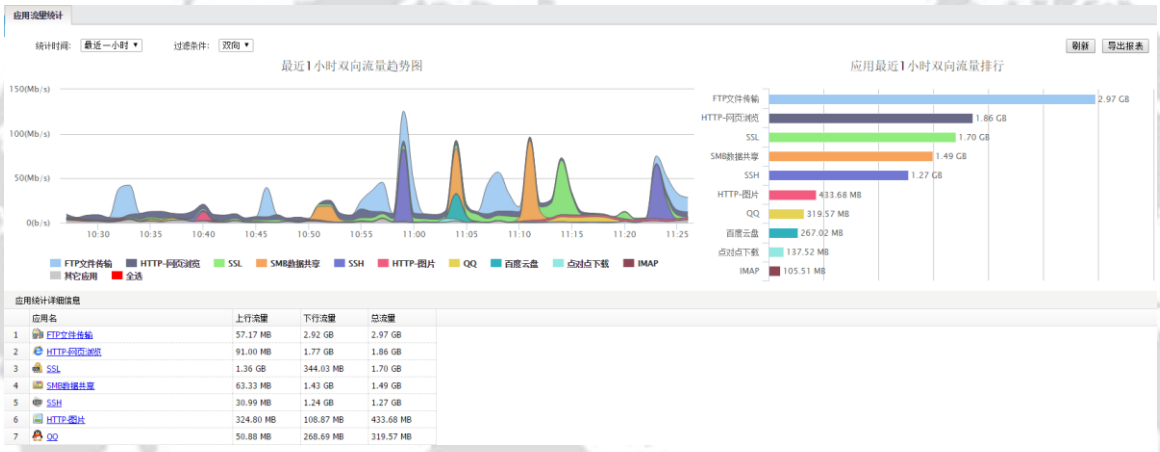
3.1 统计信息概述

通过统计信息，可以查看应用流量、用户流量、Web 访问统计、设备健康统计、入侵防御统计、病毒防护统计、在线用户统计、接口信息统计、会话信息监控的曲线图信息，通过这些信息可以判断其工作状况是否正常，给排查问题、进行大数据分析提供必要的信息。

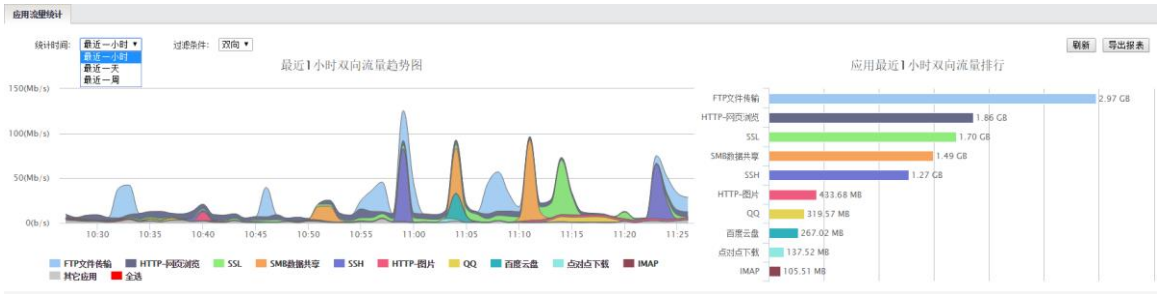
3.2 应用流量统计

查看步骤：

1、点击**统计**导航页，该页面根据左侧菜单中的选项，查看不同的子类项目。下图为应用流量统计内容页面。



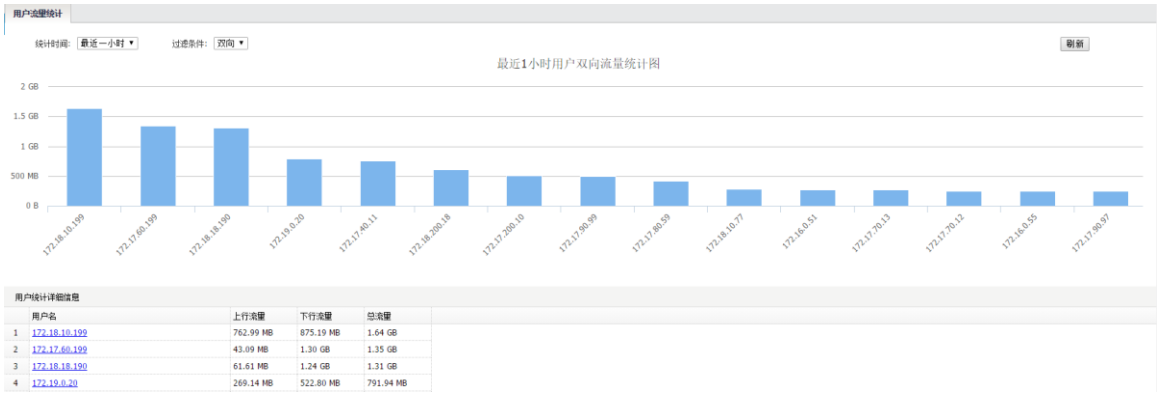
2、通过下拉框选择统计时间间隔，其中包括最近 1 小时、最近 1 天、最近 1 周。过滤条件也可以选择**单向/双向**。



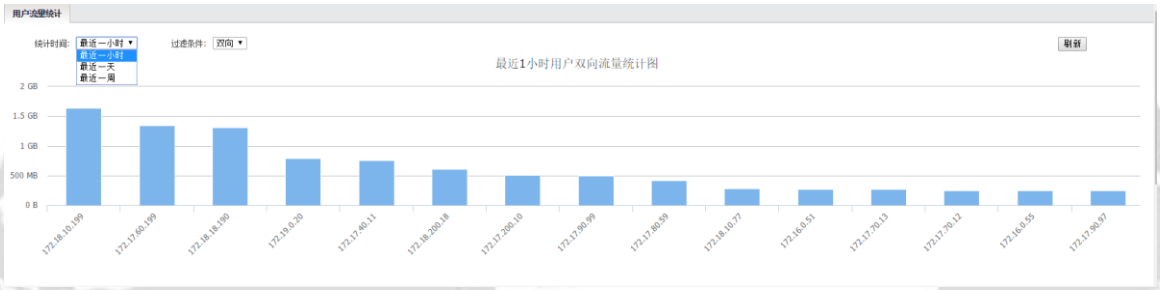
3.3 用户流量统计

查看步骤：

1、点击**统计**导航页，该页面选择左侧菜单中**用户流量统计**。

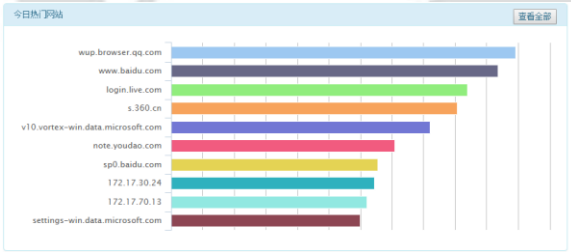


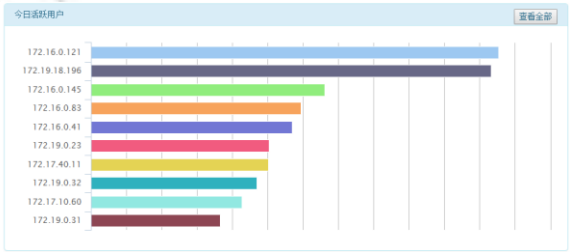
2、通过下拉框选择统计时间间隔，其中包括最近 1 小时、最近 1 天、最近 1 周。过滤条件也可以选择**单向/双向**。

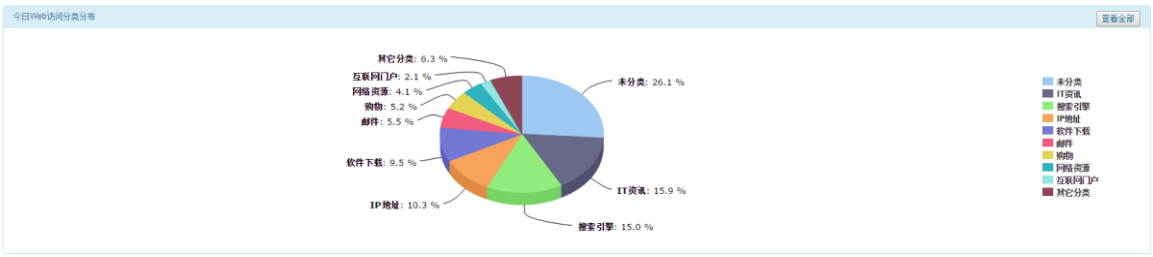


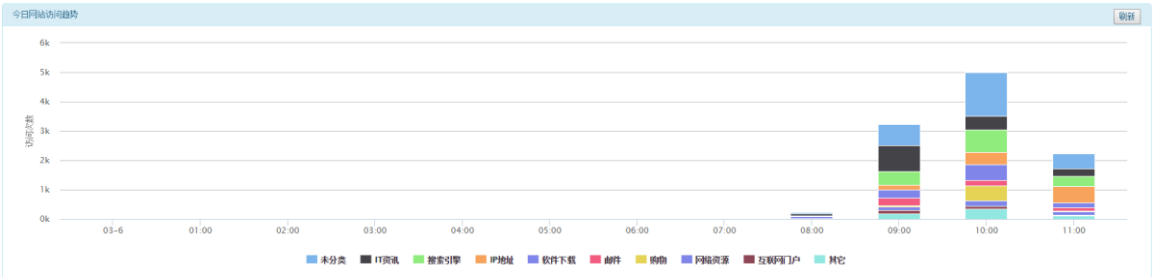
3.4 Web访问统计

可以查看今日热门网站、今日活跃用户、web 访问分类分布、网站访问趋势等。





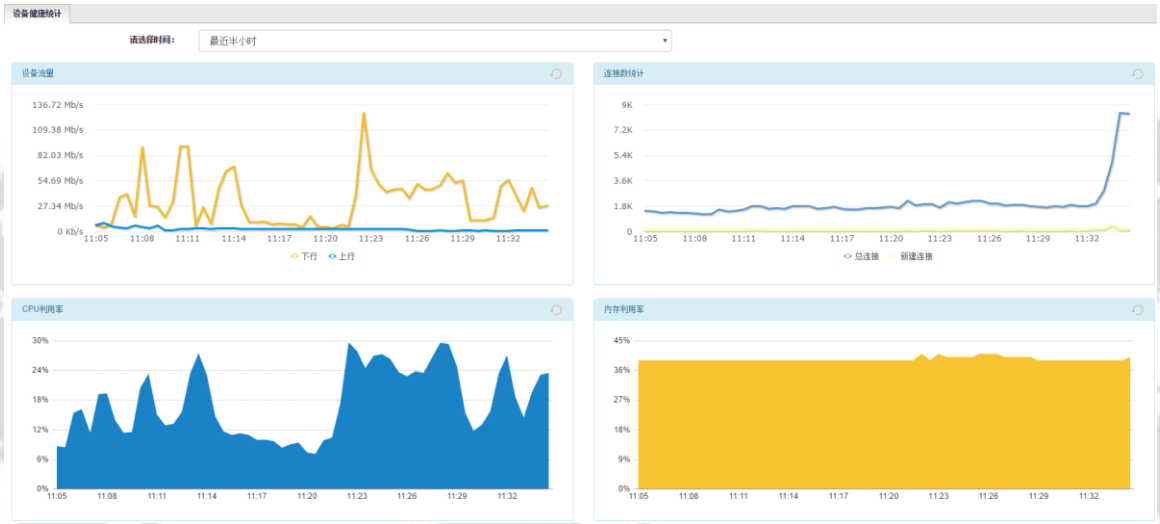




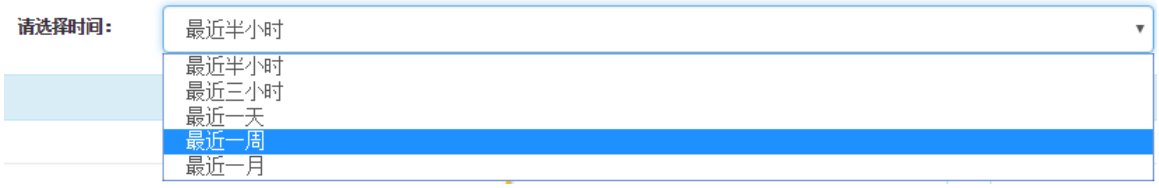
3.5 设备健康统计

查看步骤：

1、点击**统计**导航页，该页面选择左侧菜单中**设备健康统计**。分别列出了设备流量、连接数、CPU 利用率、内存利用率信息。



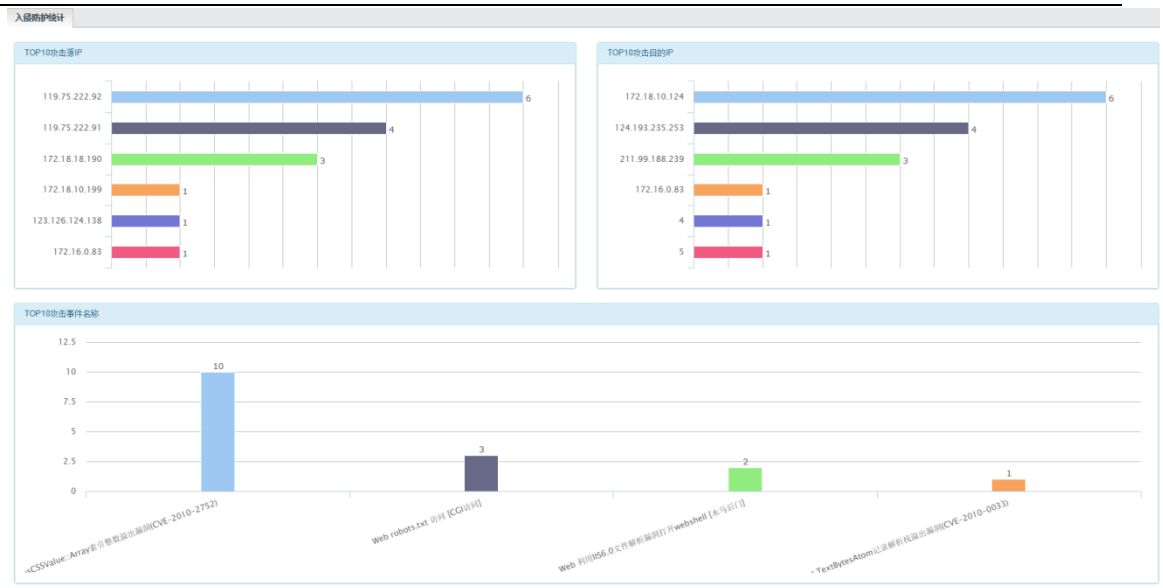
2、通过下拉框选择统计时间间隔，其中包括最近半小时、最近 3 小时、最近 1 天、最近 1 周、最近 1 周。

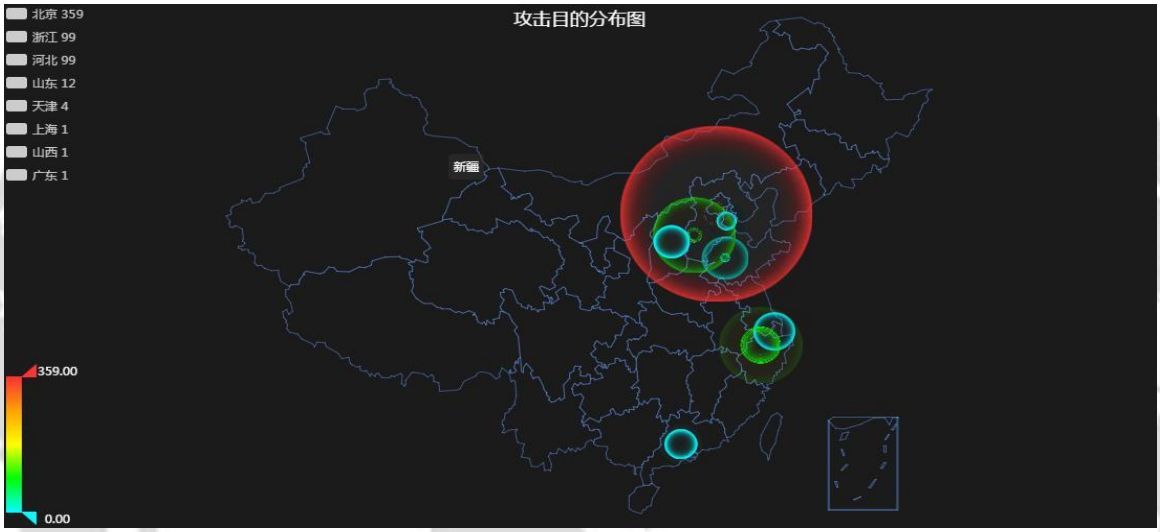


3.6 入侵防护统计

查看步骤：

1、点击**统计**导航页，该页面选择左侧菜单中**入侵防护统计**。分别列出了 TOP10 攻击源 IP、TOP 攻击目的 IP、 TOP10 攻击事件名称信息。

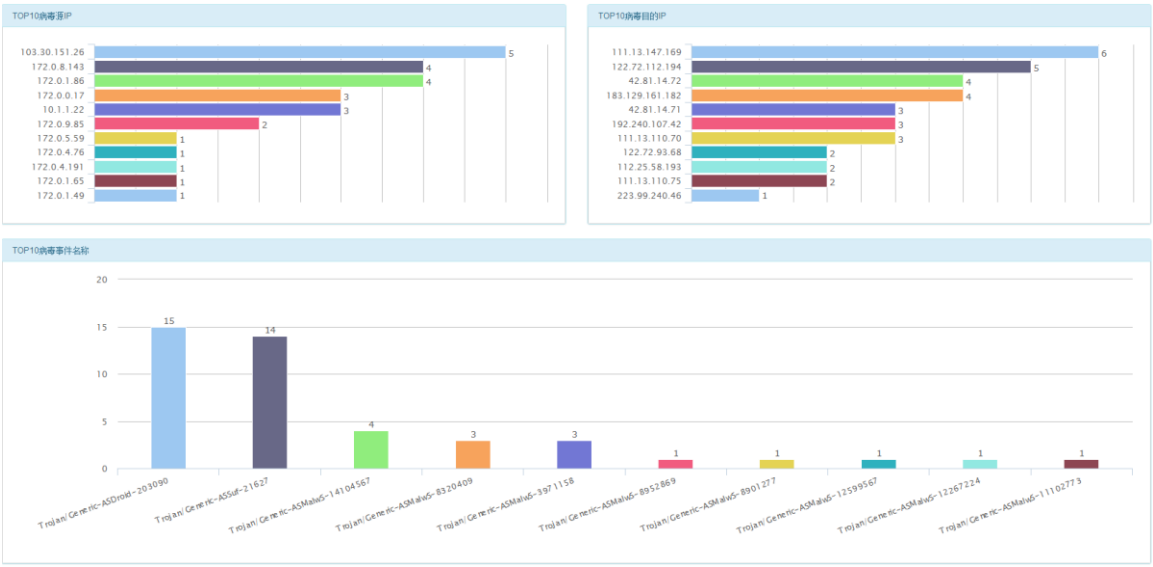




3.7 病毒防护统计

查看步骤：

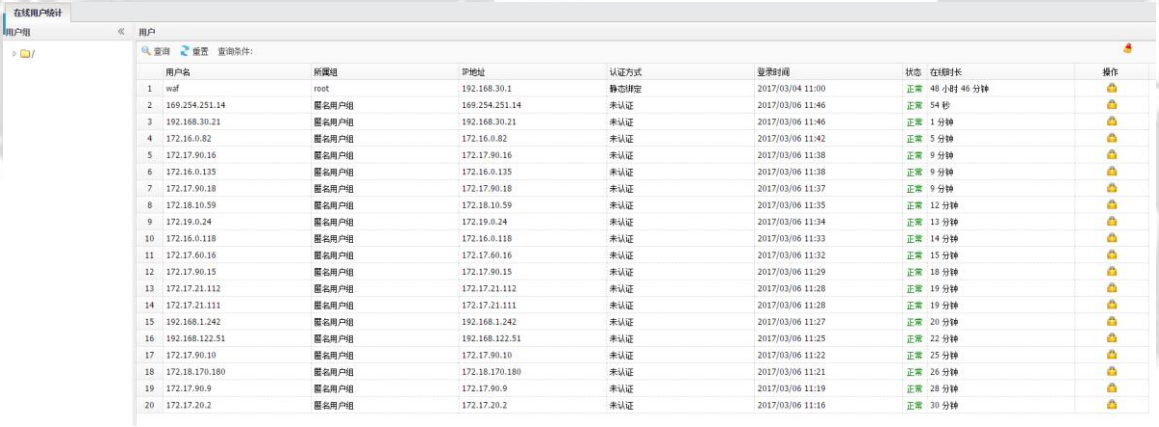
1、点击**统计**导航页，该页面选择左侧菜单中**病毒防护统计**。分别列出了 TOP10 病毒源 IP、TOP 病毒目的 IP、 TOP10 病毒事件名称信息。



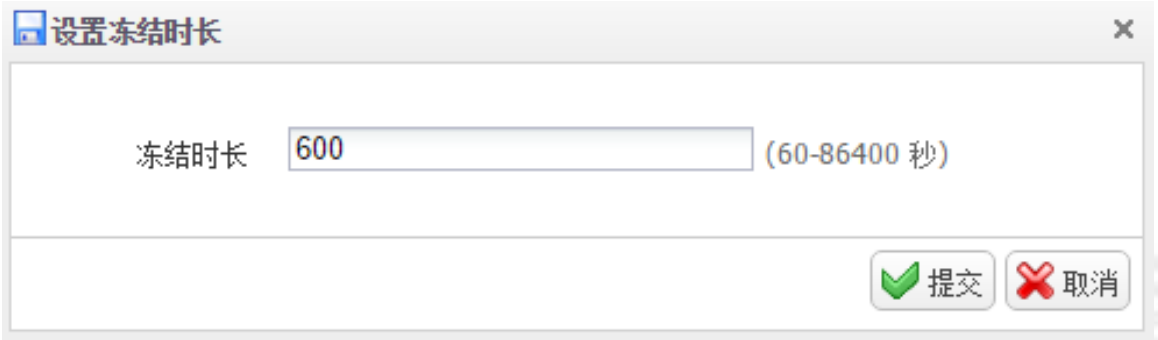
3.8 在线用户统计

查看步骤：

1、点击**统计**导航页，该页面选择左侧菜单中**在线用户统计**。



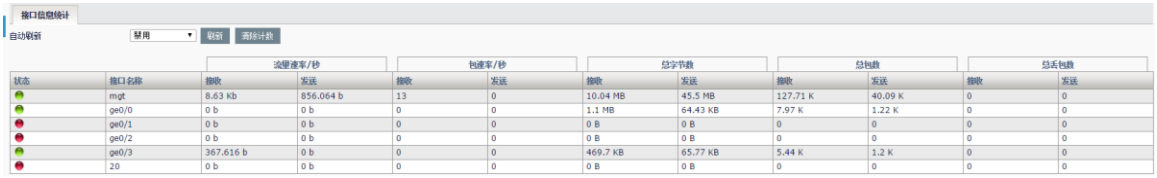
2、左侧折叠文件夹中可以选择显示匿名用户和认证用户，点击右侧锁形图标可以冻结该用户。



3.9 接口信息统计

查看步骤：

1、点击**统计**导航页，该页面选择左侧菜单中在**接口信息统计**。



2、可以选择自动刷新的时间间隔：禁用、10s 、30s 、300s。

3、点击清除计数可以清除全部接口计数

第4章 会话信息监控

4.1 会话监控信息概述

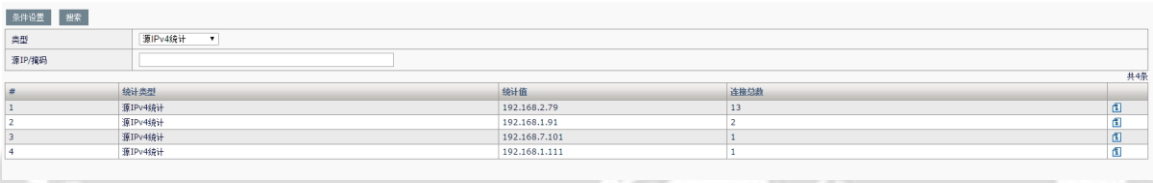
通过会话监控功能，可监控统计下一代防火墙内所有连接状况;并可根据参数定制查询。

4.2 会话统计

配置步骤：

1、点击**统计>会话信息监控>会话统计**，进入会话统计页面。

2、点击**条件设置**，选择筛选条件：

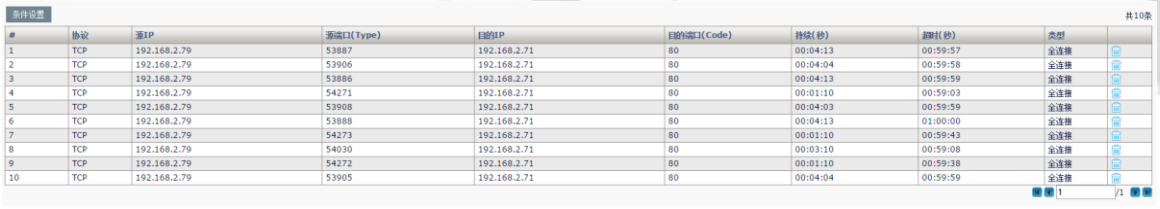


类型：源 IPv4 统计、源 Ipv6 统计、目的 IPv4 统计、目的 Ipv6 统计、目的端口统计，默认为按源 IPv4 统计。

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。

点击搜索进行统计。

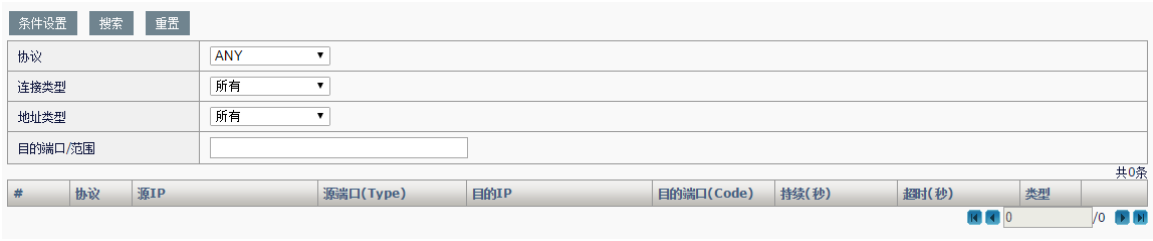
3、结果显示后，若想查看详细信息，点击 进入标准会话页面查看连接详细信息。



4.3 会话监控

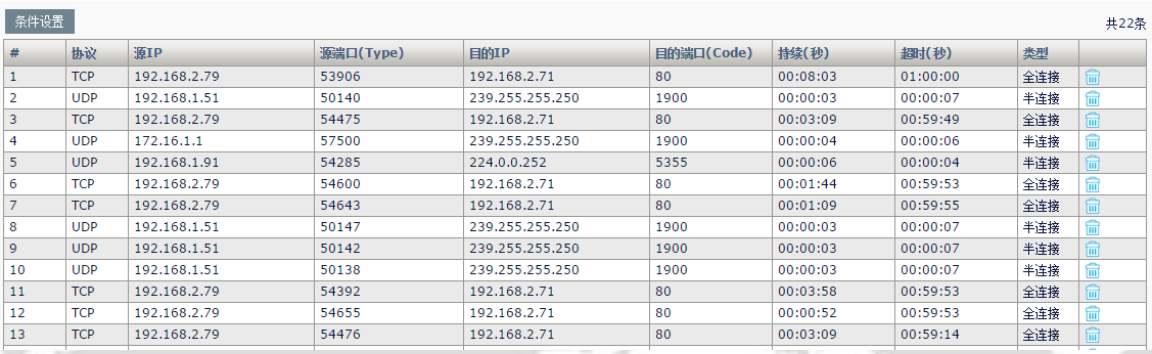
配置步骤：

1、点击**统计>会话信息监控>会话监控**，进入会话监控页面，该页面根据输入的协议、连接类型、地址类型、目的端口/范围进行组合查询，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协议、连接类型、地址类型、目的端口/范围等条件。

3、点击 搜索 进行查询。



#	协议	源IP	源端口(Type)	目的IP	目的端口(Code)	持续(秒)	超时(秒)	类型
1	TCP	192.168.2.79	53906	192.168.2.71	80	00:08:03	01:00:00	全连接
2	UDP	192.168.1.51	50140	239.255.255.250	1900	00:00:03	00:00:07	半连接
3	TCP	192.168.2.79	54475	192.168.2.71	80	00:03:09	00:59:49	全连接
4	UDP	172.16.1.1	57500	239.255.255.250	1900	00:00:04	00:00:06	半连接
5	UDP	192.168.1.91	54285	224.0.0.252	5355	00:00:06	00:00:04	半连接
6	TCP	192.168.2.79	54600	192.168.2.71	80	00:01:44	00:59:53	全连接
7	TCP	192.168.2.79	54643	192.168.2.71	80	00:01:09	00:59:55	全连接
8	UDP	192.168.1.51	50147	239.255.255.250	1900	00:00:03	00:00:07	半连接
9	UDP	192.168.1.51	50142	239.255.255.250	1900	00:00:03	00:00:07	半连接
10	UDP	192.168.1.51	50138	239.255.255.250	1900	00:00:03	00:00:07	半连接
11	TCP	192.168.2.79	54392	192.168.2.71	80	00:03:58	00:59:53	全连接
12	TCP	192.168.2.79	54655	192.168.2.71	80	00:00:52	00:59:53	全连接
13	TCP	192.168.2.79	54476	192.168.2.71	80	00:03:09	00:59:14	全连接

4、点击右侧 按钮可以删除选定的某条会话。

第5章 流量统计

5.1 基于转发策略流量统计

该功能是对配置开启了流量统计的安全策略进行流量统计的。

进入**统计>会话信息监控>流量统计>基于转发策略**，点击**条件设置**可看到如下界面。可输入检索条件，查询流量统计结果。

地址类型：ipv4/ipv6 地址。

服务：策略服务类型。

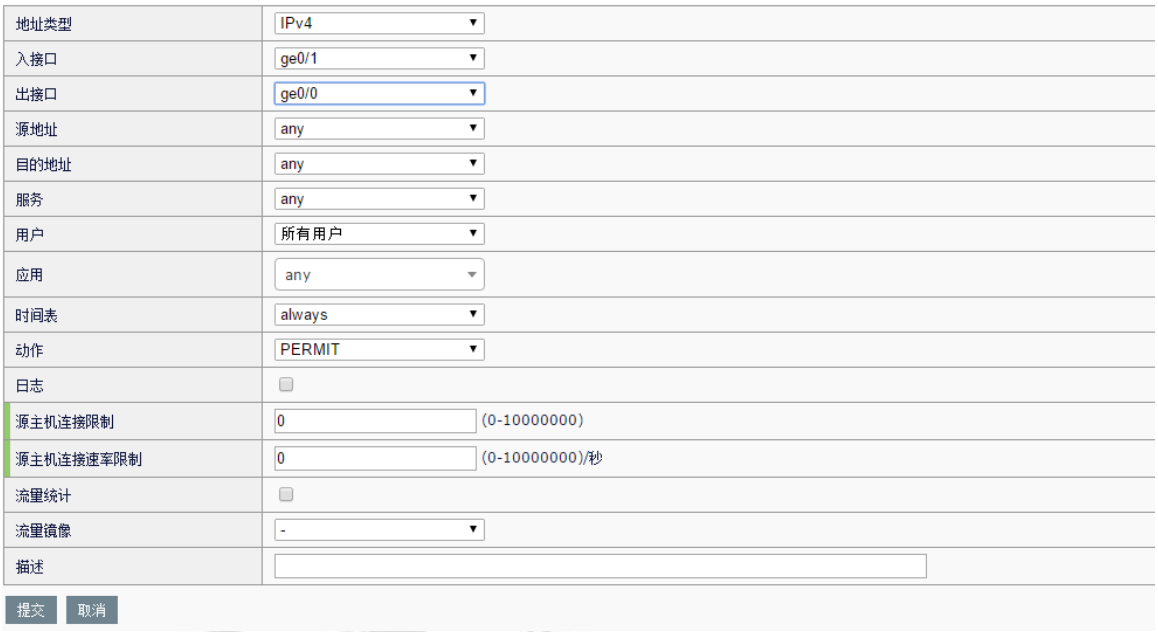
5.2 配置案例

案例描述

配置统计策略，查看统计结果。

配置步骤：

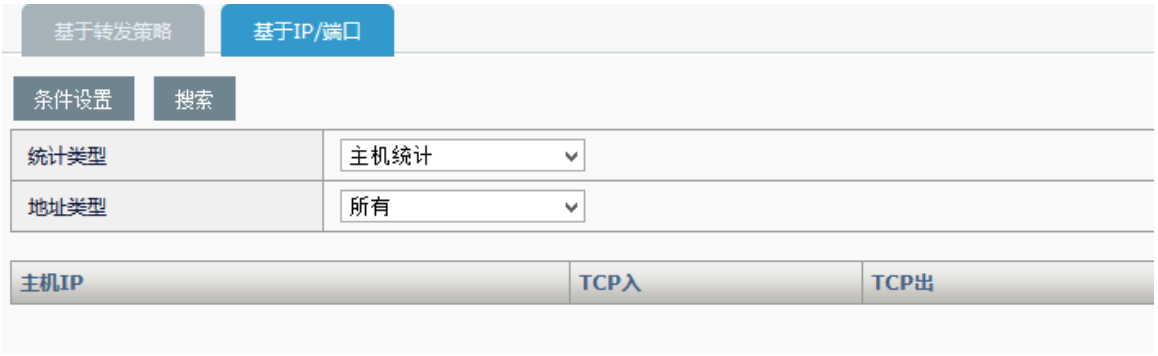
1、进入**策略>防火墙策略>访问控制>新建**，选中一条策略之后，开启策略流量统计功能：



2、进入**统计>会话信息监控>流量统计>基于转发策略**，点击条件设置，输入检索条件，查询流量统计结果。

5.3 基于IP/端口流量统计查询

进入**统计>会话信息监控>流量统计>基于 IP/端口策略**，点击**条件设置**可看到如下界面。可输入检索条件，查询流量统计结果。



统计类型：包括主机和端口

地址类型：IPv4/IPv6 地址

主机 ip：统计的主机地址

目的端口或范围：统计的目的端口或者端口范围，如 100-2410

TCP 入：TCP 协议流量

TCP 出：TCP 协议流量

UDP 入：UDP 协议流量

UDP 出：UDP 协议流量

其他入：其他协议流量

其他出：其他协议流量

总流量：所有协议双方向流量总和

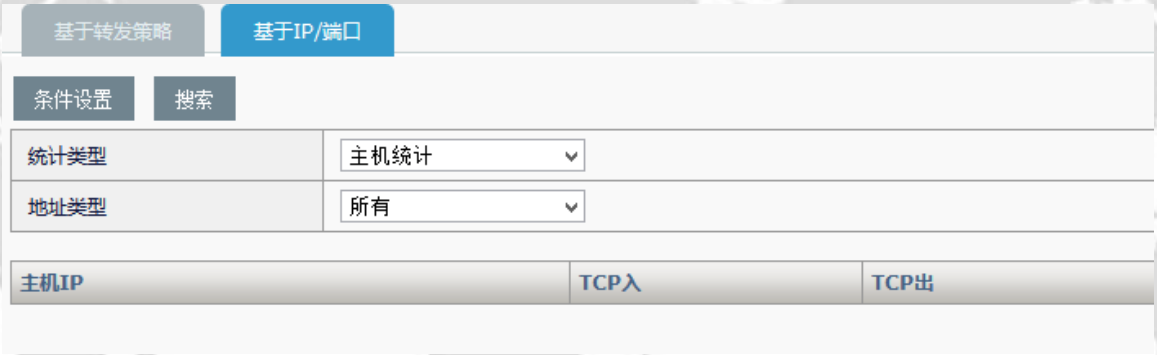
5.4 配置案例

案例描述

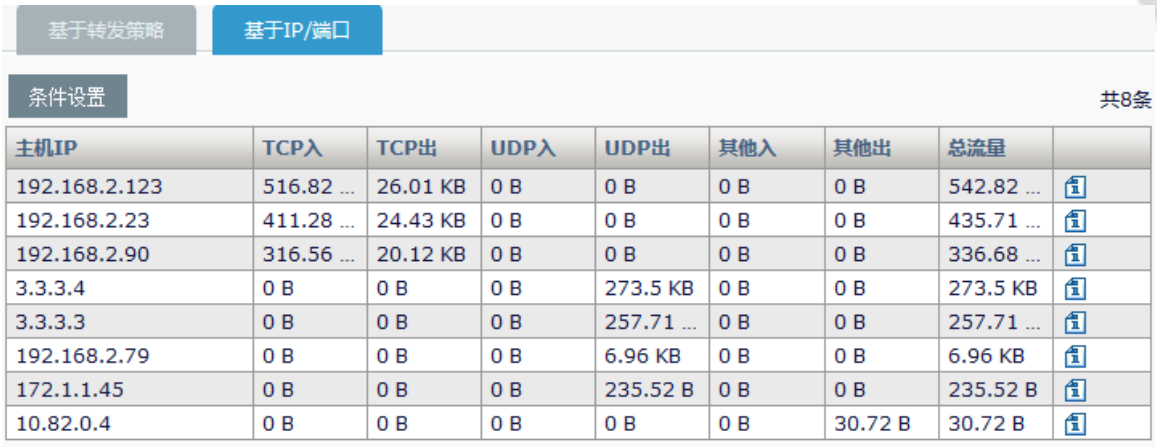
配置过滤条件，查看流量统计。

配置步骤：

1、进入**统计>会话信息监控>流量统计>基于 IP/端口策略**，点击**条件设置**，输入检索条件，查询流量统计结果。



2、点击**搜索**，可查看设备的流量统计结果:



主机IP	TCP入	TCP出	UDP入	UDP出	其他入	其他出	总流量	
192.168.2.123	516.82 ...	26.01 KB	0 B	0 B	0 B	0 B	542.82 ...	
192.168.2.23	411.28 ...	24.43 KB	0 B	0 B	0 B	0 B	435.71 ...	
192.168.2.90	316.56 ...	20.12 KB	0 B	0 B	0 B	0 B	336.68 ...	
3.3.3.4	0 B	0 B	0 B	273.5 KB	0 B	0 B	273.5 KB	
3.3.3.3	0 B	0 B	0 B	257.71 ...	0 B	0 B	257.71 ...	
192.168.2.79	0 B	0 B	0 B	6.96 KB	0 B	0 B	6.96 KB	
172.1.1.45	0 B	0 B	0 B	235.52 B	0 B	0 B	235.52 B	
10.82.0.4	0 B	0 B	0 B	0 B	0 B	30.72 B	30.72 B	

第6章 时间对象

6.1 概述

为了方便用户配置和管理，下一代防火墙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。

6.2 配置时间对象

6.2.1 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**。

6.2.2 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：

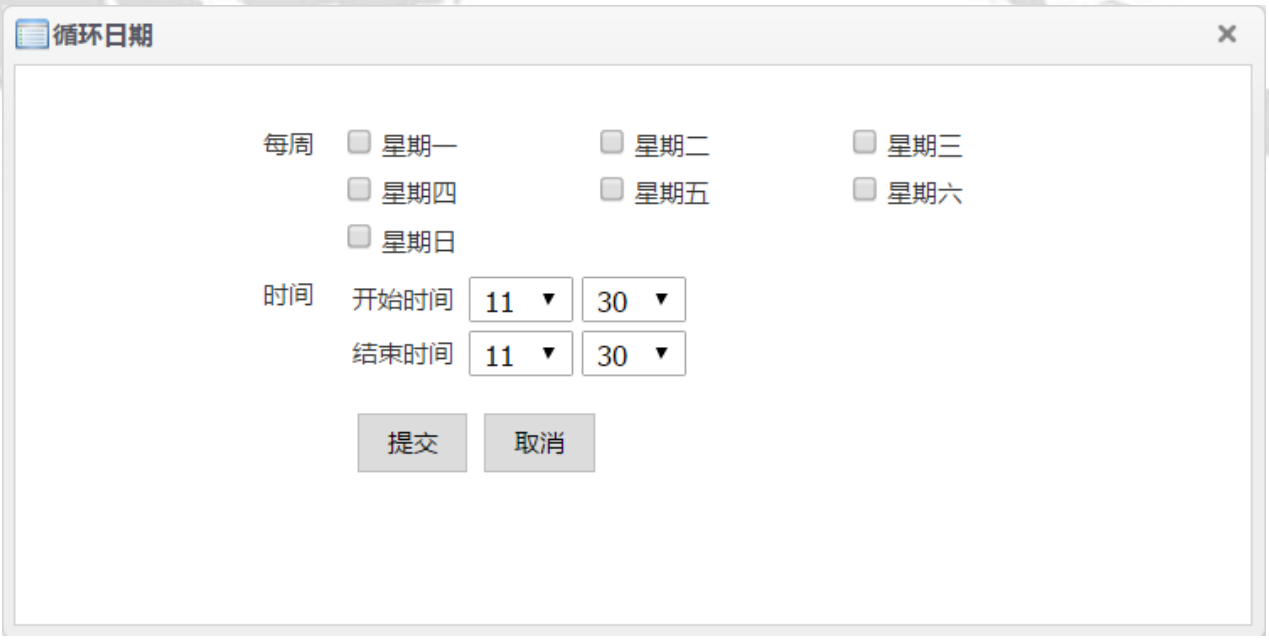
名称：为新建周期时间设置名称。

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**。

6.3 配置案例

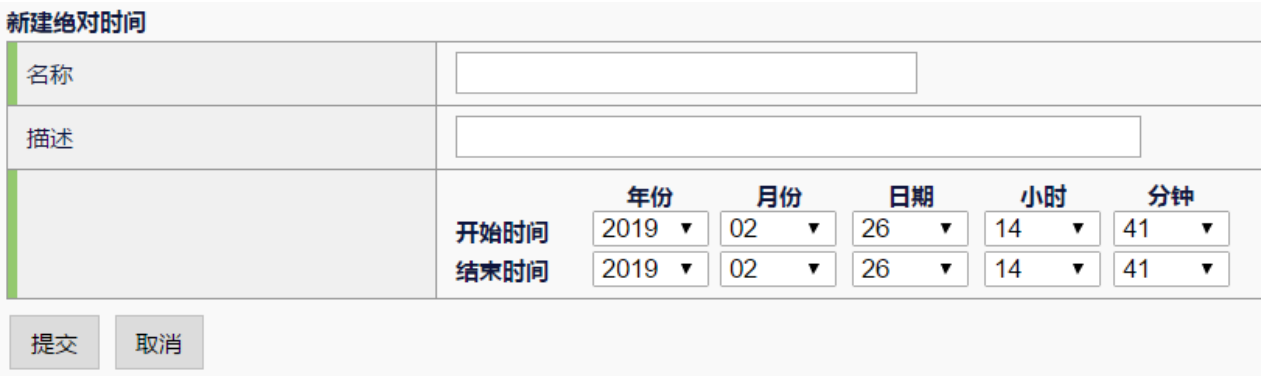
6.3.1 配置案例 1：增加绝对时间

案例描述

增加一个绝对时间对象，此对象目的是被安全策略引用，使该安全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。

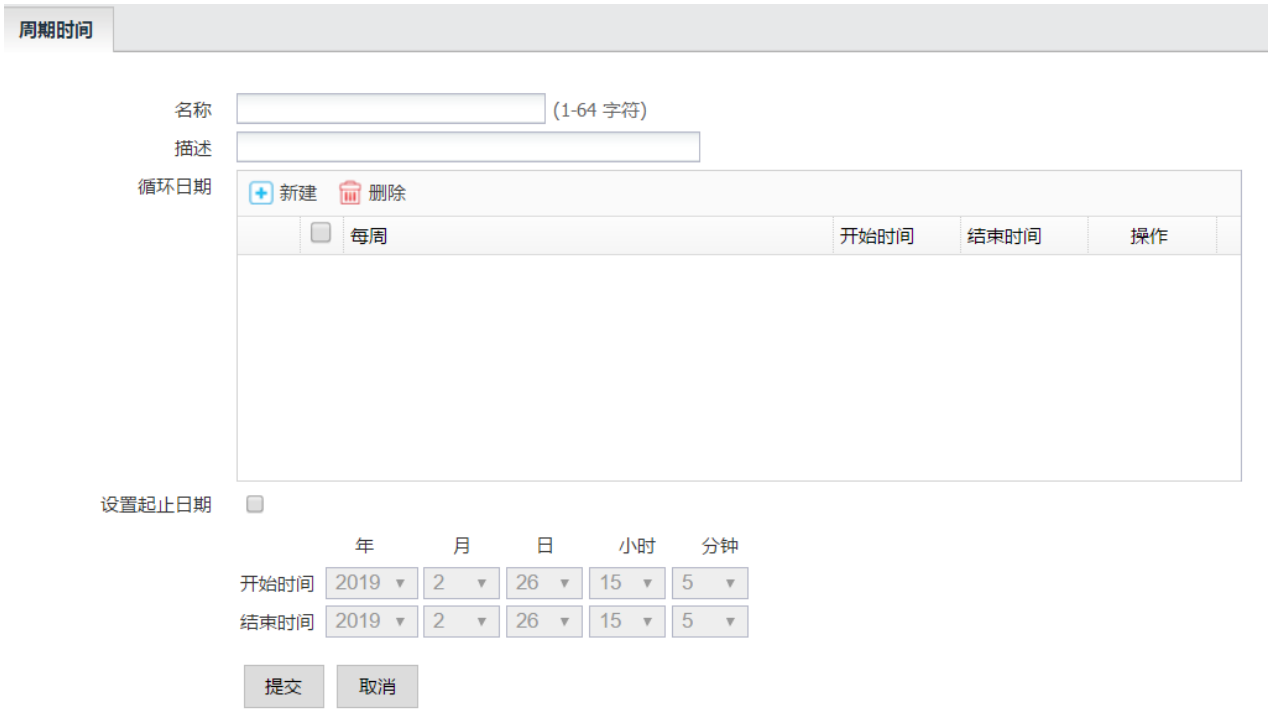
6.3.2 配置案例 2：增加周期时间

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。

6.4 绝对时间与周期时间监控与维护

6.4.1 查看绝对时间

1、点击**对象>时间对象>绝对时间**，如下图：

6.5 常见故障分析

6.5.1 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。

第7章 服务对象

7.1 概述

为了方便用户的配置和管理，下一代防火墙中引入了服务对象的概念。在其它功能(如防火墙策略、NAT 策略、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。

7.2 配置服务对象

7.2.1 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：

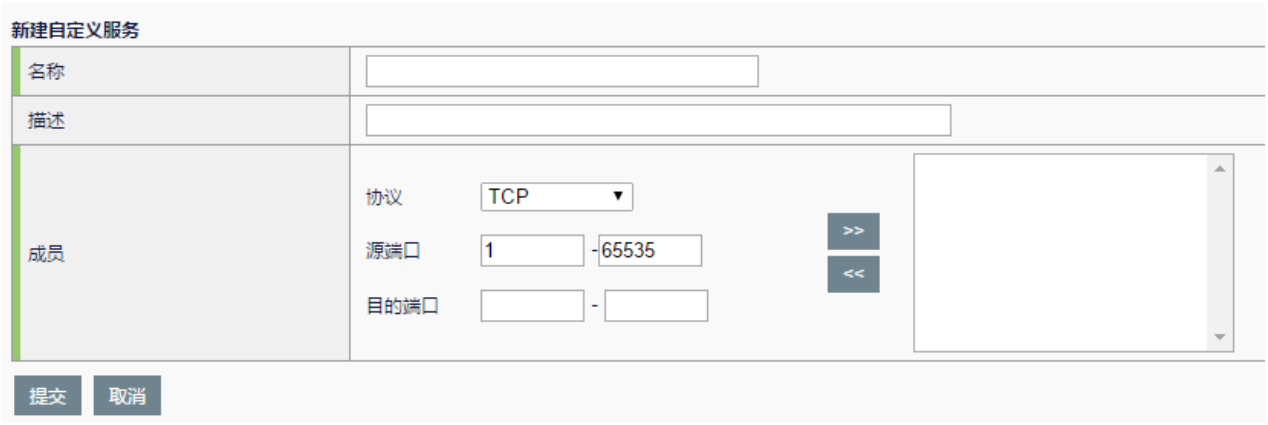
下图是部分系统预定义服务。

名称	内容(协议/源端口-目的端口)	引用
any	All	0
ah	IP/51	0
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
dns	TCP/1-65535:53,UDP/1-65535:53	0
discard	TCP/1-65535:9,UDP/1-65535:9	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	1
https	TCP/1-65535:443	0

7.2.2 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**。

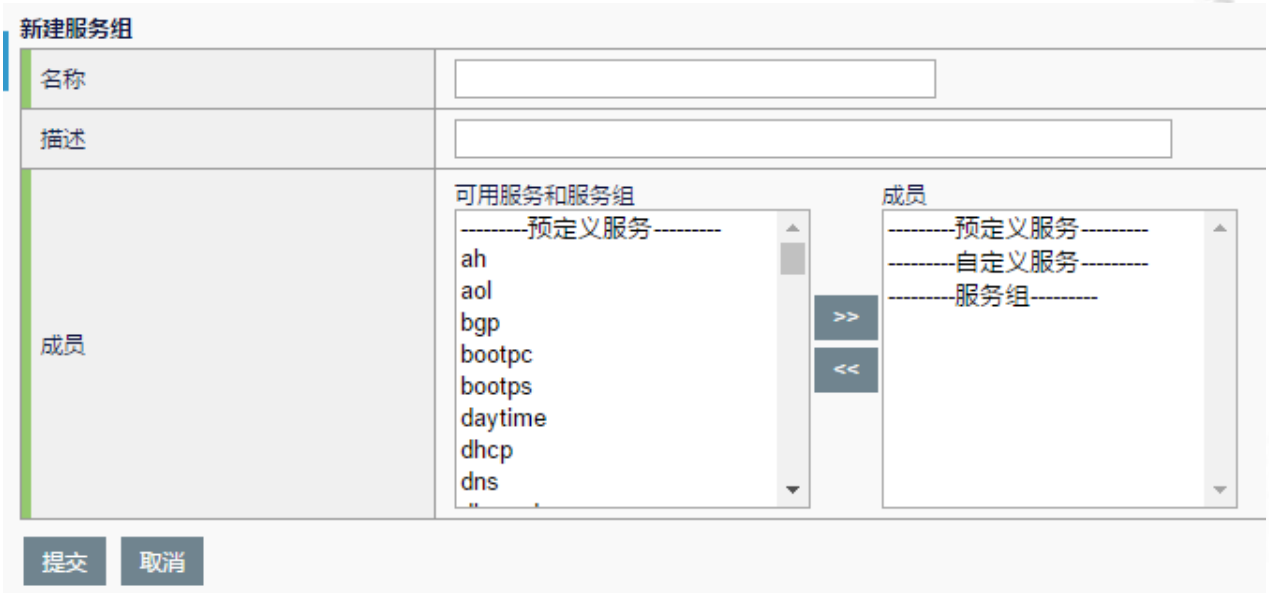
提示：

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。

7.2.3 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。

点击**提交**。

提示：

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。

7.3 配置案例

7.3.1 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、编辑目的端口 110，点击 >> 添加。

3、点击**提交**完成设置。

7.3.2 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，SMTP，TFTP 到允许访问服务组。

3、点击 >> 添加。

4、点击**提交**完成设置。

7.4 服务对象监控与维护

7.4.1 查看服务组

1、进入**对象>服务对象>服务组**，如下图：

名称	成员	引用	描述
允许服务	ftp,http,smtp	0	允许访问的服务

7.5 常见故障分析

7.5.1 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。

第8章 地址对象

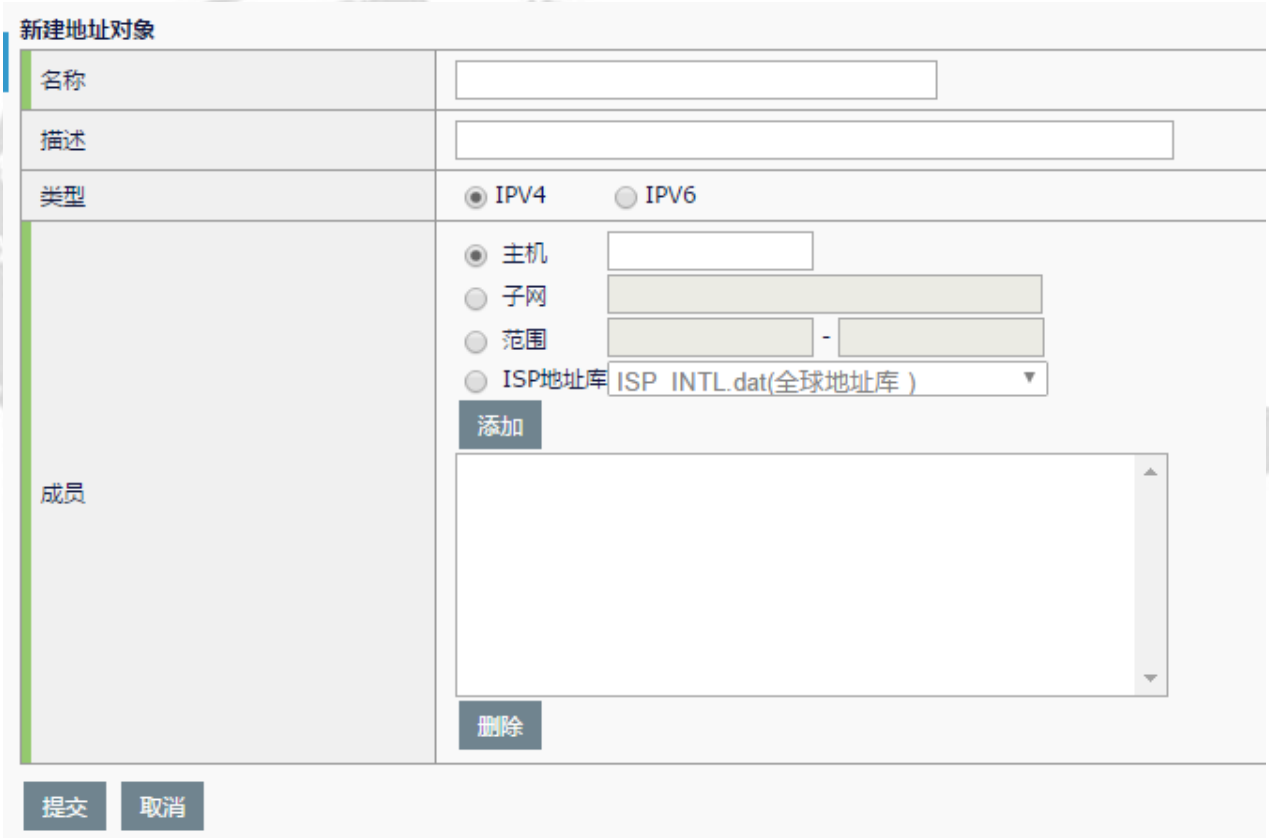
8.1 地址对象概述

为了方便用户的配置和管理，下一代防火墙中引入了地址对象的概念。地址对象分为地址节点和地址组，地址组是地址节点的集合。在其它功能的配置中(如防火墙策略、NAT 策略、路由策略)，可以引用地址对象来定义配置生效的条件。

8.2 配置地址对象

地址对象分为 IPv4 类型，IPv6 类型。

1、进入**对象- >地址对象>地址对象**，点击**新建**，如下图：



名称：为新建地址对象设置名称，不得超过 63 个字符。

描述：对新建地址对象描述，不得超过 127 个字符。

类型：地址对象可分为 IPv4 类型，IPv6 类型。

ISP 地址库：系统预置了 ISP 的主要地址信息

地址节点：IPv4 类型地址对象的内容包含：

●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 类型地址对象的内容包括：

●主机：主机 IPv6 地址

●子网：IPv6 网络地址

●范围：IPv6 地址范围

2、进入**对象>地址对象>地址对象**，查看已创建地址信息，如下图：

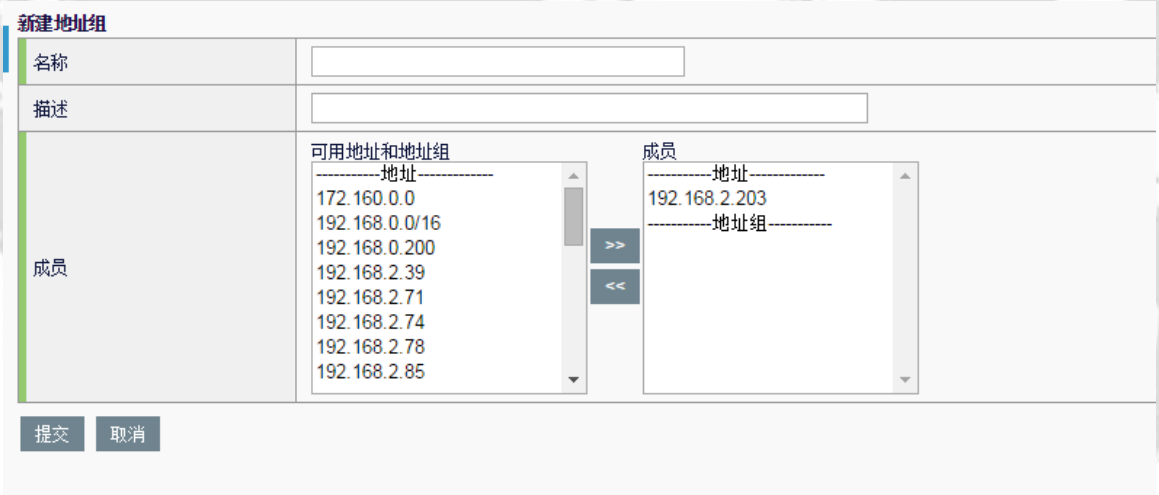
名称	成员	引用	描述
any	0.0.0.0/0,::/0	9	
sss	1.1.1.1	0	

8.3 配置地址组

地址组是地址对象的集合，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。

可用地址和地址组：已经定义好的地址对象和地址组信息。

成员：地址组成员。

2、点击**提交**。

8.4 备份恢复

备份恢复可以对当前地址对象进行导出进行本地保存，也可以导入已有的地址信息。

配置步骤：

1、进入**对象>地址对象>备份恢复**，如下图：

导入：导入已有的地址对象信息

导出：导出当前的地址对象配置信息

8.5 配置案例

8.5.1 配置案例 1：增加 IPv4 地址对象

案例描述

增加一个 IPv4 的地址对象，包含内网的某些网段。

配置步骤：

1、进入**对象>地址对象>地址对象**，点击**新建**，如下图：

2、输入参数。

3、点击**提交**完成设置。

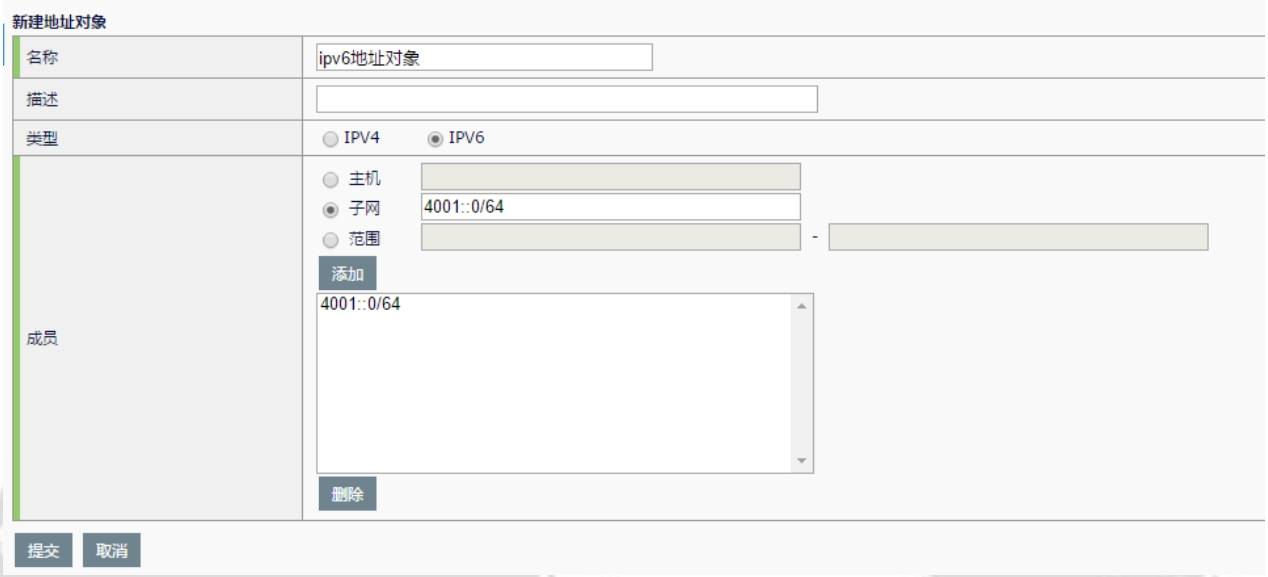
8.5.2 配置案例 2：增加 IPv6 地址节点

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>地址对象**，点击**新建**，如下图：



2、输入参数。

3、点击**提交**完成设置。

8.5.3 配置案例 3：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。

8.6 常见故障分析

8.6.1 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。

第9章 应用对象

9.1 概述

为了方便用户的配置和管理，下一代防火墙中引入了应用对象的概念。在防火墙策略、应用策略、路由策略的配置中，可以引用应用对象来定义配置生效的条件。

应用实际上包括应用对象、应用组两个部分。

●**应用对象**：具体的用户应用，如下载软件、即时通信软件，不需要用户配置。

●**应用分类**：查看预定义应用分组，不需要用户配置。

●**应用组**：需要用户自行配置。

在实际使用中，由防火墙策略、路由策略等来引用应用对象。

转发策略引用应用对象可以阻断某些应用或允许特定的应用。

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。以往多通过阻断、限速的方式，这里可以通过应用负载将 P2P 流量引入到另一条链路上。

9.2 配置应用对象

9.2.1 配置应用组

配置步骤：

1、进入**对象>应用>应用组**，点击**新建**，如下图

名称：为新建应用对象的名称。

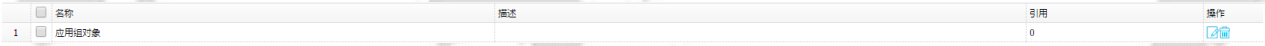
应用列表：为系统所支持的所有应用列表；如上图所示。

选中所想要的应用，点击**提交**。

9.3 监控与维护

9.3.1 查看应用对象

进入**对象>应用>应用组**，如下：



9.3.2 查看已有的预定义应用信息

进入**对象>应用对象**查看点击具体应用类别查看具体应用信息

9.4 常见故障分析

9.4.1 故障现象：第一次访问应用往往无法引流

现象	第一次访问应用，发现无法正常引流
分析	因为要有识别的过程才能确定是否是这个应用，识别出来之后，后续流量可以正常引流

第10章 用户

10.1 概述

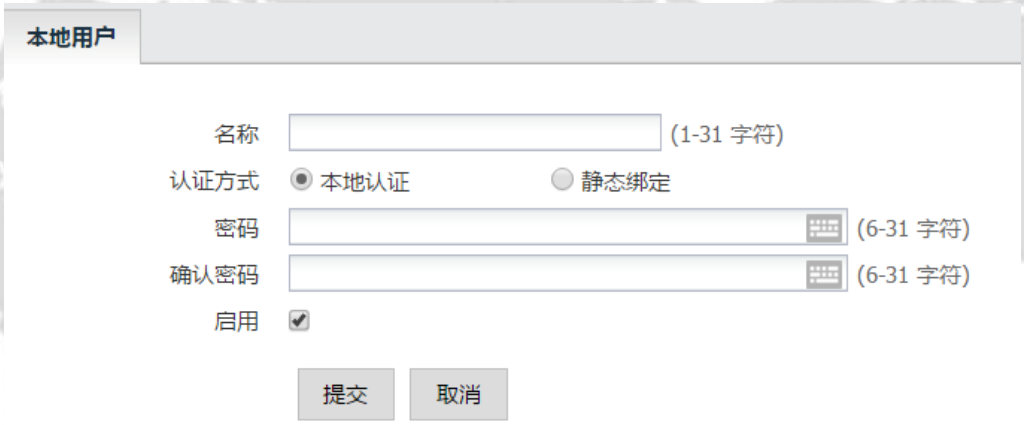
设备提供用户管理功能，支持本地认证、静态绑定和远程用户；可以配置用户组，将用户加入用户组中；在访问控制策略、应用控制策略、流控策略、审计等功能中可以引用用户/用户组。

10.2 用户配置

10.2.1 用户

本地用户

进入**对象>用户>本地用户**，点击**新建**



名称：用户名

认证方式：本地认证/静态绑定

密码：用户的密码

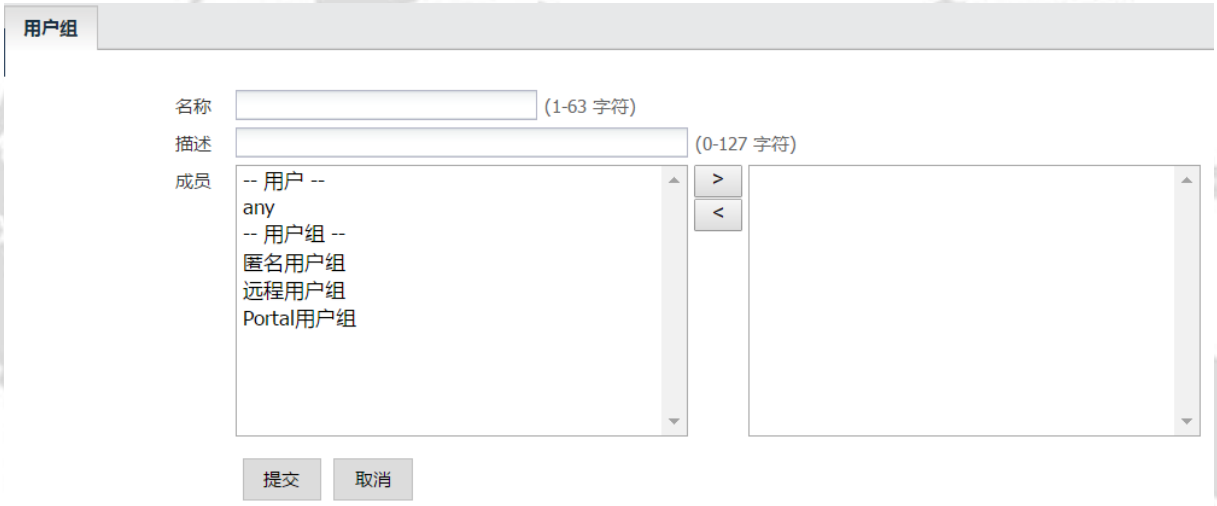
启用按钮默认勾选

静态绑定模式：为用户绑定指定的 ip 或网段

远程用户：以 RADIUS 或 LDAP 来配置用户（首先要配置 RADIUS/LDAP 认证服务器）

10.2.2 用户组

进入**对象>用户>用户组**，可以将用户加入用户组。



名称：用户组名

描述：用户组的备注

成员：左侧为可选用户，右侧是选中的用户

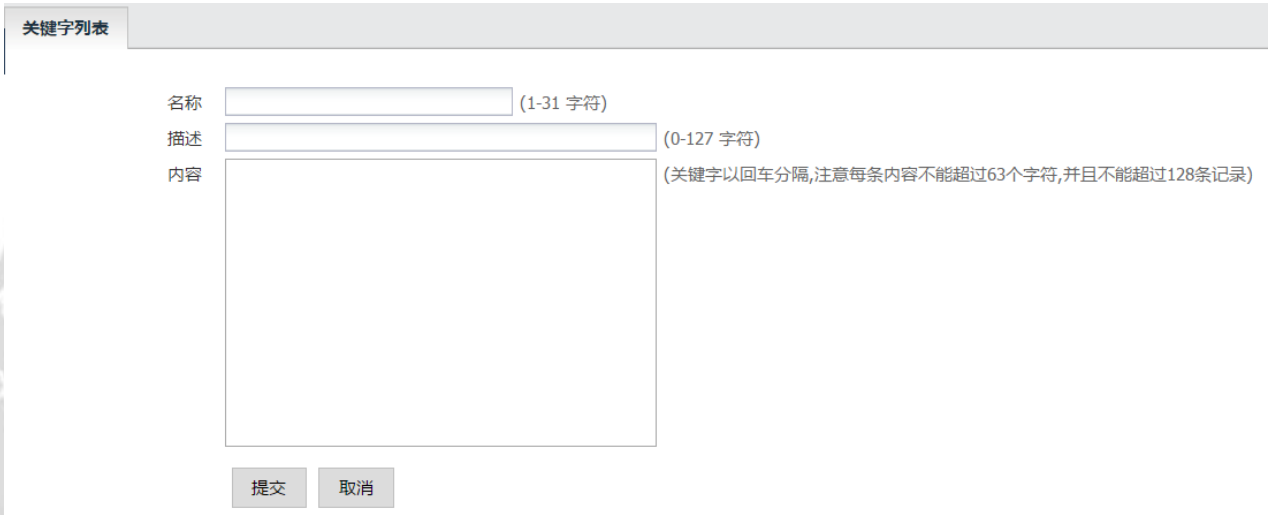
第11章 关键字

11.1 概述

关键字对象在 web 访问策略中被引用，参与策略的条件匹配

11.2 配置关键字

进入**对象>关键字>关键字对象**，点击**新建**按钮



名称：关键字名

描述：关键字的备注

内容：关键字以回车分隔,注意每条内容不能超过 63 个字符,并且不能超过 128 条记录

第12章 url 分类

12.1 概述

url 对象在 web 访问策略中被引用，参与策略的条件匹配

12.2 配置url

进入**对象>URL>URL 分类**，点击**新建**按钮

名称：url 名

描述：url 的备注

内容：url 以回车分隔,注意每条内容不能超过 127 个字符,并且不能超过 64 条记录

第13章 健康检查

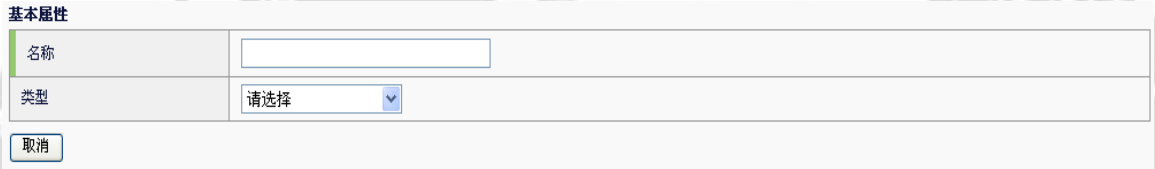
13.1 健康检查概述

健康检查用来对服务器或者链路进行探测，来获取服务器或者链路的健康状况。一旦发现服务器或链路故障，将不再往该服务器或者链路上进行流量分担。使负载均衡更加可靠。

支持的健康检查方式包括：icmp，udp，tcp-half-open，dns 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。同时根据需要，可以将多种健康检查方式组合到一起对一个服务器或者链路进行监控。

13.2 配置健康检查

进入**对象>健康检查>健康检查**，点击**新建**



名称：健康检查的名称。

类型：健康检查的类型。选择类型后弹出具体类型的配置。

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：指定新建健康检查的名称。

类型：指定新建健康检查的协议类型。

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。

平均延迟：启用该选项功能之后，则会实时统计采样区间内有效延时的平均值，如果平均值超过该阈值，则可判断健康质量为不健康。

丢包率：启用该选项功能之后，则会实时统计采样区间内的丢包数与统计总数的百分比，如果百分比超过该阈值，则可判断健康质量为不健康。

质量采样范围：平均延迟和丢包率计算的采样区间

目标 IP 地址类型：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

目标 IP：健康检查探测的设备 ip 地址。

当类型为 UDP 时，配置界面如下：

目标端口：健康检查探测的设备端口。

当类型为 TCP 时，配置界面如下：

当类型为 DNS 时，配置界面如下：

域名：健康检查探测的域名。

3、输入间隔。
4、输入最大重试次数。
5、输入超时时间。
6、输入平均延迟
7、输入丢包率
8、输入质量采样范围
9、输入域名。
10、输入目标 IP。
11、输入目标端口。
12、点击**提交**。

13.3 配置健康检查组

健康检查组由高可用性引用，将一些通用的健康检查加入到健康检查组中。

进入**对象>健康检查>健康检查组：**

名称：健康检查组名称。

健康检查方法选择：从可选列表中选取一些健康检查方法。

有效性要求：至少要通过的健康检查个数，默认为所有，建议为默认值。

配置步骤：

1、选择健康检查方法。

2、输入有效性要求。

3、点击**确定**。

13.4 配置案例

案例描述：

新建一个 icmp 类型的健康检查，然后在静态路由中引用。

配置步骤：

1、新建 icmp 类型的健康检查：

基本属性

名称	健康检查
类型	ICMP

配置

间隔	16 (1-86400)秒
最大重试次数	3 (1-10)
超时时间	5 (1-86400)秒
平均延迟	≤ 10 (0-60000)毫秒
丢包率	≤ 50 %
质量采样范围	10 (10-50)次数
目标IP地址类型	IPv4 IPv6
目标IP	192.168.100.100

更新 取消

2、新建静态路由并引用该健康检查：

配置

IP地址/掩码	172.16.0.0/16
下一跳地址	192.168.2.100
出接口	tunl0
权重	1 (1-100)
距离	1 (1-255)
健康检查方法选择	健康检查

更新 取消

当健康检查失效时，相应的路由信息中的系统状态显示为无效：

类型	目的地址	下一跳	出接口	距离	权重	持续时间	系统状态
静态	0.0.0.0/0		ge0/0	1	1	03:56:12	有效
直连	1.1.1.0/24		ge0/3	0	0	03:32:14	有效
主机	1.1.1.1/32		ge0/3	0	0	03:32:14	有效
直连	1.1.10.0/24		ge0/0	0	0	03:32:05	有效
主机	1.1.10.1/32		ge0/0	0	0	03:32:05	有效
直连	127.0.0.0/8		lo	0	0	03:57:35	有效
静态	172.16.0.0/16	192.168.2.100	ge0/1	1	1	00:00:16	无效
直连	172.17.0.0/16		mgt	0	0	03:57:15	有效
主机	172.17.70.111/32		mgt	0	0	03:57:15	有效
直连	192.168.2.0/24		ge0/1	0	0	00:01:09	有效
主机	192.168.2.1/32		ge0/1	0	0	00:01:09	有效

第14章 证书管理

14.1 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 网上验证用户的身份。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 本地证书功能是：当设备作为 PKI 客户端时，选择本地证书作为设备的身份标识，并且验证从其他主机接收到的证书的合法性。这相当于 IE 浏览器中的证书项功能。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。

14.2 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。

14.2.1 配置本地证书

上传证书配置步骤

1、进入**对象>证书>本地证书**，点击**导入本地证书**

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、证书密钥分离格式或者证书链三种。

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。

提示：

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、证书密钥分离格式或者证书链三种。

证书文件：数字证书文件位置。

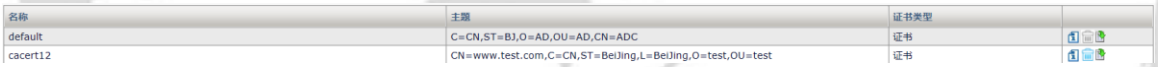
密钥文件：数字证书私钥文件位置。

密码：数字证书的密码

查看证书配置步骤

2、进入**对象>证书>本地证书**

该界面显示已导入的数字证书。



3、点击 查看某一个证书的具体信息，显示证书详细信息。

主题	C=CN,ST=BJ,O=AD,C

证书详细信息

证书名称	default
发行者	C=CN,ST=BJ,L=BJ,O=AD,OU=AD,CN=ADCA
主题	C=CN,ST=BJ,O=AD,OU=AD,CN=ADC
有效起始	Jul 29 11:33:53 2013 GMT
有效终止	Jul 27 11:33:53 2023 GMT
版本	3
序列号	01
扩展	X509v3 Basic Constraints: CA:FALSE Netscape Comment: OpenSSL Generated Certificate X509v3 Subject Key Identifier: 1B:6E:BE:D8:A1:6A:3E:90:B7:9E:4C:C0:20:E4:3F:A4:3B:CF:AA:BC X509v3 Authority Key Identifier: keyid:4B:78:A2:E2:67:4E:12:26:0D:B0:F7:00:B0:CE:50:F4:86:41:3A:FF

关闭

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

4、进入**对象>证书>本地证书**

该界面显示全部导入的数字证书列表。

名称	主题	证书类型	
default	C=CN,ST=BJ,O=AD,OU=AD,CN=ADC	证书	
cacert12	CN=www.test.com,C=CN,ST=BeiJing,L=BeiJing,O=test,OU=test	证书	

5、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

6、进入**对象>证书>本地证书**

该界面显示已导入的数字证书。

7、点击删除某一个证书。

8、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。

14.2.2 配置 CA 证书

上传证书配置步骤

1、进入**对象>证书>本地 CA 中心**，点击**导入 CA 中心证书**，可以选择两种上传 CA 证书的方式。

2、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

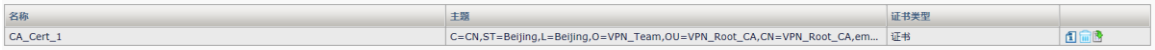
CA 证书集合文件：要上传的 CA 证书集合文件位置

3、点击提交

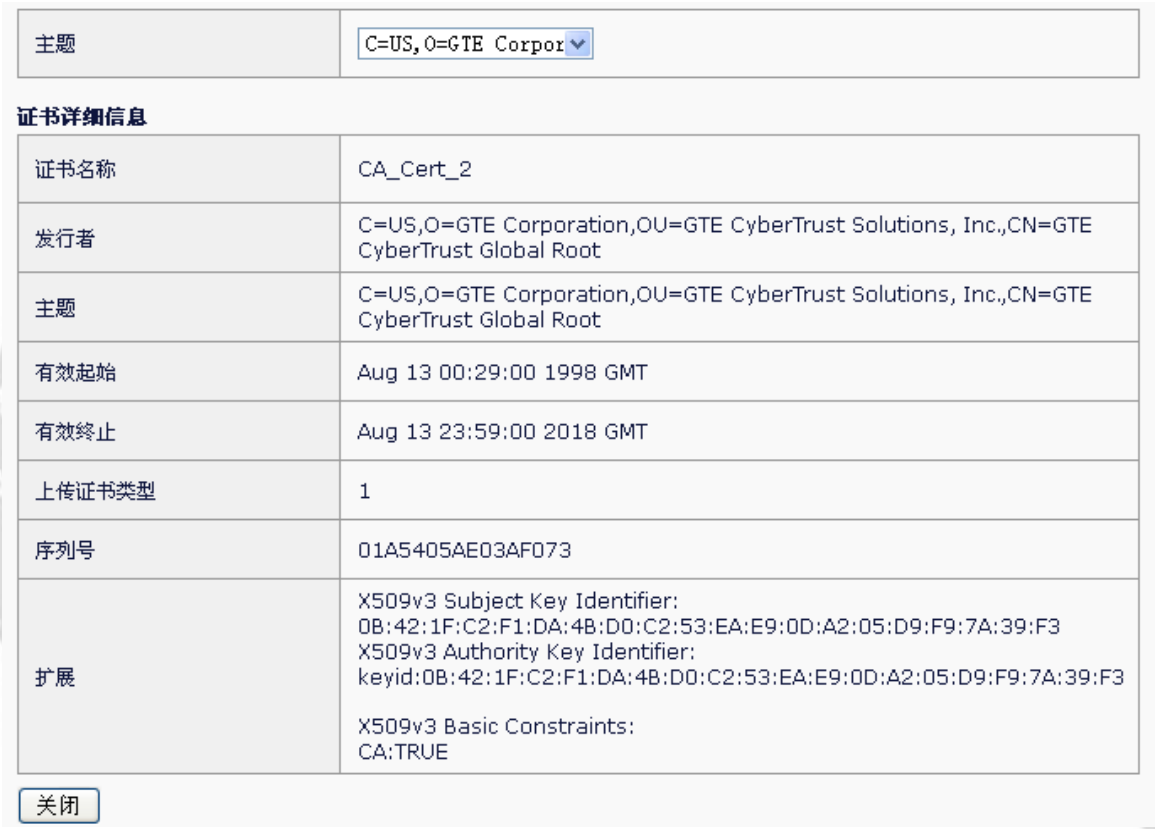
查看证书配置步骤

4、进入**对象>证书>本地 CA 中心**

该界面显示已导入的 CA 证书。



5、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

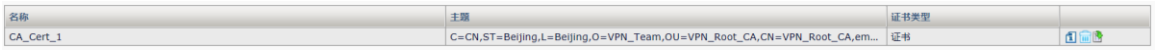
序列号：证书的序列号

扩展：证书的扩展信息

导出证书配置步骤

1. 进入**对象>证书>本地 CA 中心**

该界面显示已导入的 CA 证书。

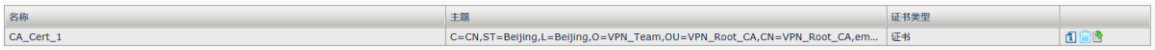


2. 点击导出某一个证书，在弹出的窗口选择导出证书存放路径，点确定导出证书。

删除证书配置步骤

6、进入**对象>证书>本地 CA 中心**

该界面显示全部导入的 CA 证书。



7、点击删除某一个证书。

8、点击确认删除证书。

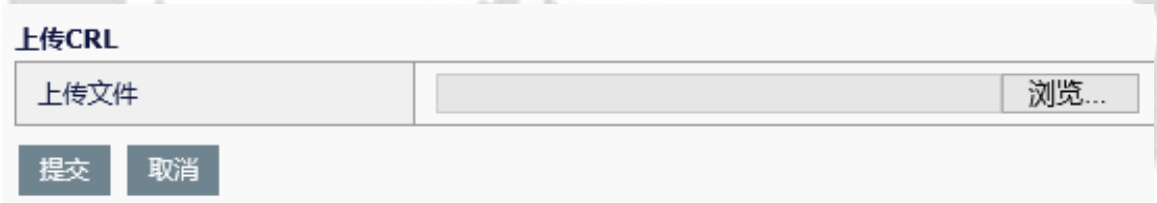
提示：

删除证书时出现时表明证书正在被引用，无法删除。

14.2.3 配置 CRL 证书

上传 CRL 配置步骤

1、进入**对象>证书>自动获取 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

3、进入**对象>证书>自动获取 CRL**

该界面显示已导入的 CRL 证书。

4、点击 查看某一个 CRL 证书的具体信息，显示证书详细信息。

CRL详细信息

证书名称	CRL_2
发行者	C=CN,CN=ADC,L=BeiJing,O=ADC
上次更新	Apr 8 11:18:08 2014 GMT
下次更新	May 8 11:18:08 2014 GMT
版本	2
扩展	X509v3 CRL Number: 1 X509v3 Authority Key Identifier: DirName:/C=CN/CN=ADC/L=BeiJing/O=ADC serial:E5:87:B6:9C:99:E9:71:16

关闭

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

扩展：证书的扩展信息

导出 CRL 配置步骤

5、进入**对象>证书>自动获取 CRL**

该界面显示已导入的 CRL 证书。

名称	主题	
CRL_1	C=CN,ST=BJ,L=BJ,O=VENUS,OU=ADC,CN=liminyiclient	

6、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，点确定导出证书。

删除 CRL 配置步骤

7、进入**对象>证书>自动获取 CRL**

该界面显示已导入的 CRL 证书。

名称	主题	
CRL_1	C=CN,ST=BJ,L=BJ,O=VENUS,OU=ADC,CN=liminyiclient	

8、点击 删除某一个 CRL 证书。

9、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。

14.2.4 配置管理根 CA 配置

生成根 CA 配置步骤

1、进入**对象>CA 中心>根 CA 管理**

该界面显示根 CA 配置中心。

2、点击 生成CA根证书 生成 CA 根证书，在弹出的窗口确认覆盖原 CA 根证书，进入证书生成界面。

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

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：

4、进入**对象>CA 中心>根 CA 管理**

该界面显示根 CA 配置中心。

5、点击 导入CA根证书 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格式两种。

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格式两种。

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格式两种。

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。

6、点击**更新**按钮，完成根 CA 证书上传。

导出根 CA 配置步骤

7、进入**对象>CA 中心>根 CA 配置**

该界面显示根 CA 配置中心。

8、点击 

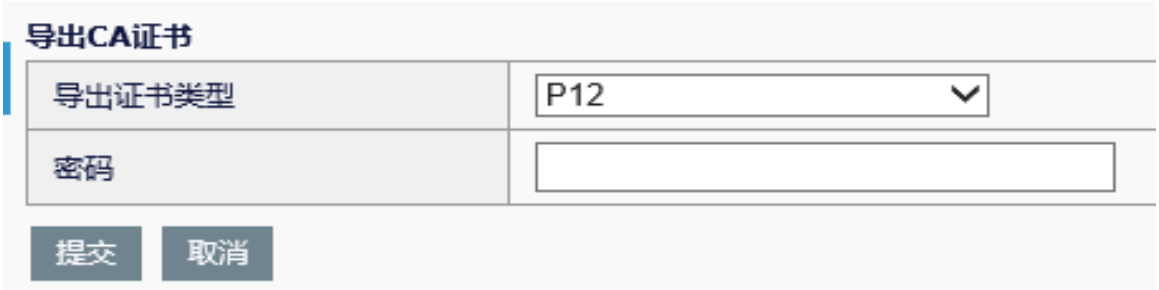
，进入根 CA 证书导出界面，可以选择导出为 PEM 格式和 P12 格式两种类型的 CA 证书。其中 PEM 格式证书不包含密钥文件。

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

9、进入**对象>CA 中心>根 CA 配置**

该界面显示根 CA 配置中心。

10、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

11、进入**对象>CA 中心>根 CA 配置**

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

12、进入**对象>CA 中心>根 CA 配置**。

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：证书生效的开始时间

下次更新：证书生效的终止时间

版本：证书的版本号

扩展：证书的扩展信息

导出 CRL 配置步骤

13、进入**对象>CA 中心>根 CA 配置**。

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

14、进入**对象>CA 中心>根 CA 配置**

该界面显示根 CA 配置中心。

在 CRL 一栏，点击手动更新 CRL。

14.2.5 配置管理用户证书

生成用户证书请求步骤

1、进入**对象>CA 中心>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

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

电子邮件：配置证书的电子邮件信息

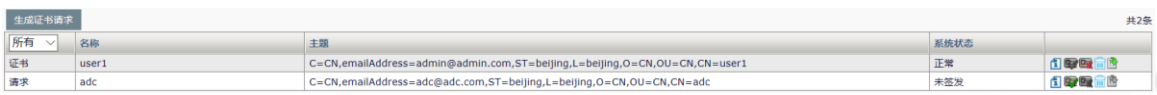
密钥大小：配置证书的密钥大小，可以选择 1024bit 或者 2048bit 的证书

3、点击**更新**，生成证书请求。

签发用户证书步骤

4、进入**对象>CA 中心>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

5、进入**对象>CA 中心>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。

6、点击**提交**，完成对证书的吊销。

删除用户证书步骤

7、进入**对象>CA 中心>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

8、进入**对象>CA 中心>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。

证书详细信息

证书名称	user1
发行者	C=CN,L=t1,ST=t1,O=t1,OU=t1,emailAddress=t1@t1.com,CN=CA_NO1
主题	C=CN,L=admin,ST=admin,O=admin,OU=admin,emailAddress=admin@admin.com,CN=user1
有效起始	Jan 13 13:14:13 2014 GMT
有效终止	Apr 23 13:14:13 2014 GMT
版本	3
序列号	C4CDE16822EDD120
扩展	X509v3 Key Usage: Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication, E-mail Protection, Code Signing, Microsoft Server Gated Crypto, OCSP Signing, Time Stamping, dvcs

关闭

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

9、进入**对象>CA 中心>用户证书管理**

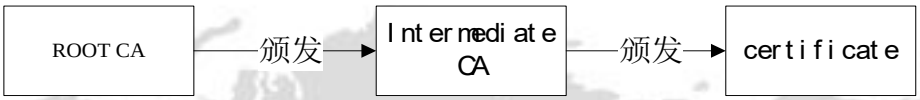
该界面显示用户证书列表。

选择系统状态为正常的证书，点击  图标导出证书。

14.3 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，结构如下图所示：



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>证书>本地证书。**

3、点击**导入本地证书**，根据 certificate 的格式导入本地证书。

4、进入**对象>证书>本地 CA 中心**。

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。

14.4 常见故障

14.4.1 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	检查各级证书链是否能够验证。 证书链应当包含根 CA。

第15章 接口

15.1 接口概述

下一代防火墙接口管理分为三种：物理接口配置管理、VLAN 配置管理、链路聚合配置管理。其中物理接口主要是对以太网接口进行属性配置。

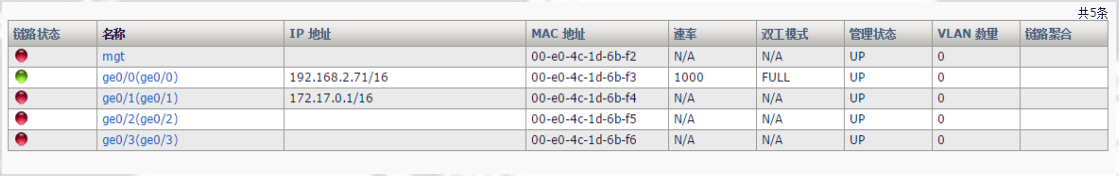
VLAN 配置包括创建 VLAN，并在 VLAN 中加入成员物理接口。加入到 VLAN 中的接口分两种方式：tag 与 untag。tag 的方式启用 802.1q 协议并能处理协议报文，untag 方式则只能处理不带 vlan 标签的普通以太报文。VLAN 支持 STP 协议，根据 STP 协议与其他 VLAN 形成生成树。

链路聚合配置则是将多个物理口成员聚合在一起，起到提高带宽的作用。链路聚合支持 LACP 协议，根据 LACP 协议可以与其他链路聚合形成动态的聚合关系。

15.2 物理接口配置管理

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。

1、进入**网络>接口配置>物理接口**，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		00-e0-4c-1d-6b-f2	N/A	N/A	UP	0	
	ge0/0(ge0/0)	192.168.2.71/16	00-e0-4c-1d-6b-f3	1000	FULL	UP	0	
	ge0/1(ge0/1)	172.17.0.1/16	00-e0-4c-1d-6b-f4	N/A	N/A	UP	0	
	ge0/2(ge0/2)		00-e0-4c-1d-6b-f5	N/A	N/A	UP	0	
	ge0/3(ge0/3)		00-e0-4c-1d-6b-f6	N/A	N/A	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 是千兆电口，xge X/X 是万兆光口

IP 地址：物理接口的 IP 地址。

MAC 地址：物理接口的 MAC 地址。

速率：物理接口实际速率，单位 Mbps。

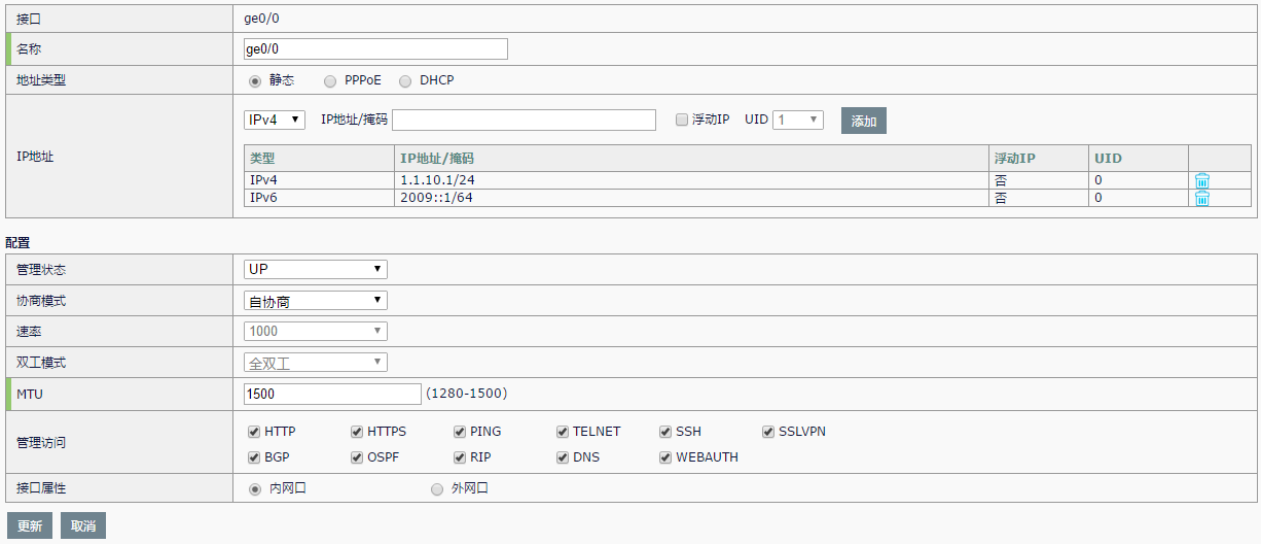
双工模式：物理接口双工模式，分为全双工/半双工两种（FULL/HALF）。

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>。

2、点击**接口名称**，进入单个物理接口配置，如下图：



基本属性显示物理接口当前状态，具体如下：

接口：物理接口名称，mgt 是管理口，ge X/X 是千兆电口，xge X/X 是万兆光口。

名称：物理接口的别名。

地址类型：接口地址的类型。

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

配置用于配置物理接口，具体如下：

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：物理接口实际速率，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。

注意：

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。

3、点击**更新**完成对物理接口的配置。

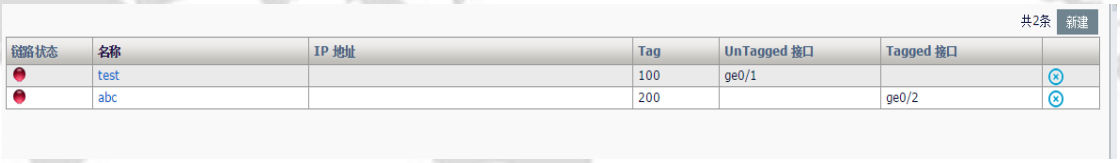
15.3 VLAN配置

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 vlan 标签的普通以太报文。

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。

15.3.1 添加 VLAN

1、进入**网络>接口配置>VLAN**，如下图：



链路状态：VLAN 的状态

名称：VLAN 名称

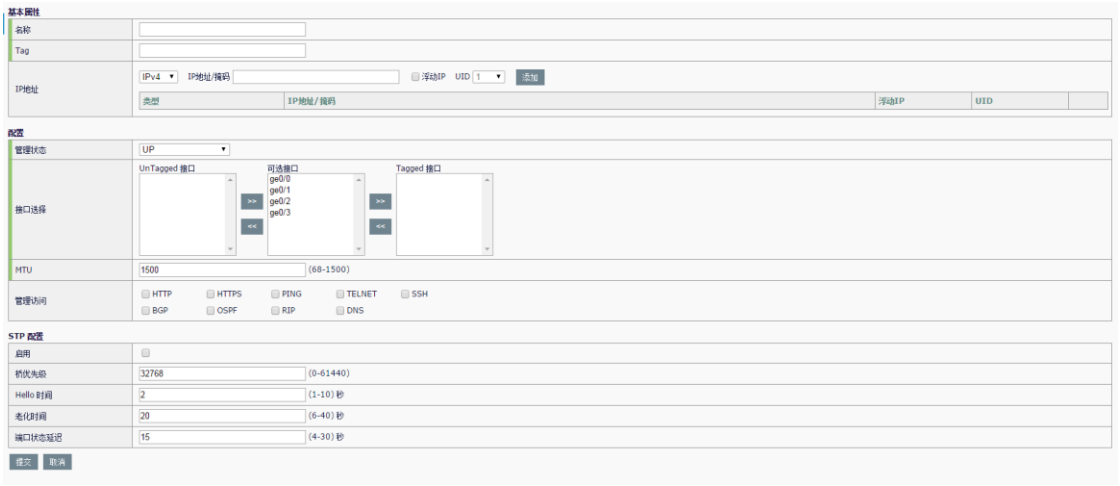
IP 地址：VLAN 的 IP 地址

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：



名称：VLAN 名称

Tag：VLAN 的 ID 号

IP 地址：VLAN 的 IP 地址，可选择 IPv4、IPv6，输入 IP 地址并点击**添加**生效

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。

3、VLAN 的 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

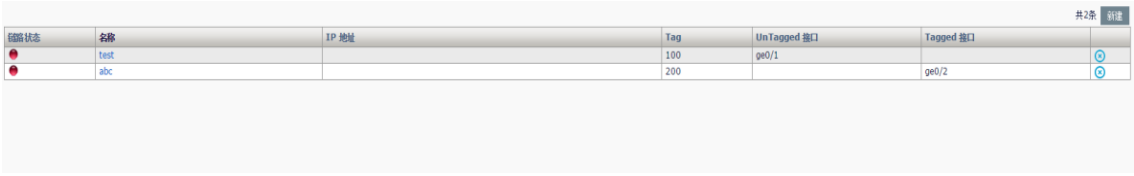
Hello 时间：VLAN 发送 STP bpdu 报文时间，范围 1-10 秒

老化时间：STP 状态隔多长时间没更新，认为拓扑改变，范围 6-40 秒

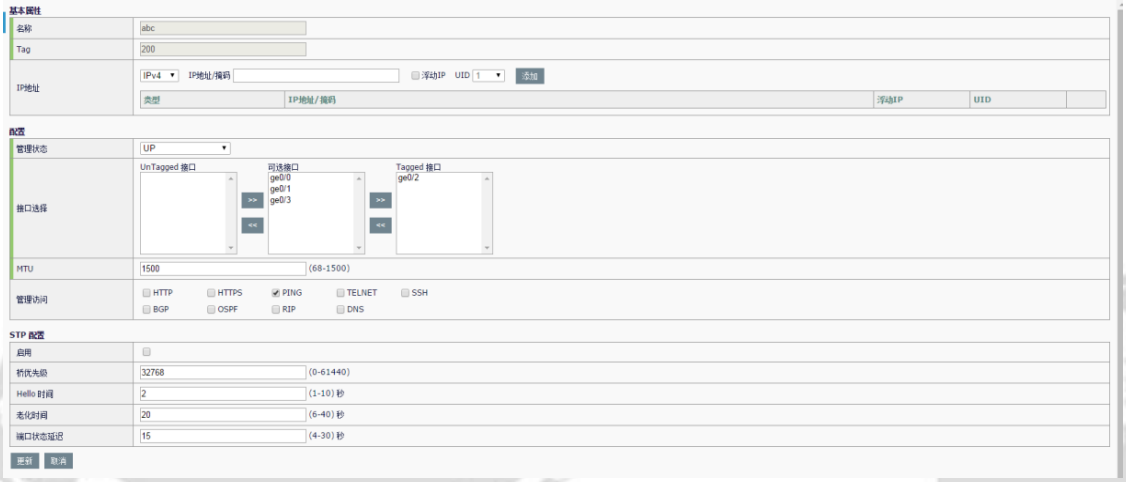
端口状态延迟：端口状态变换的时延，范围 4-30 秒

15.3.2 修改 VLAN

1、进入**网络>接口配置>VLAN**，如下图：



2、点击 vlan **名称**，修改 VLAN，如下图：

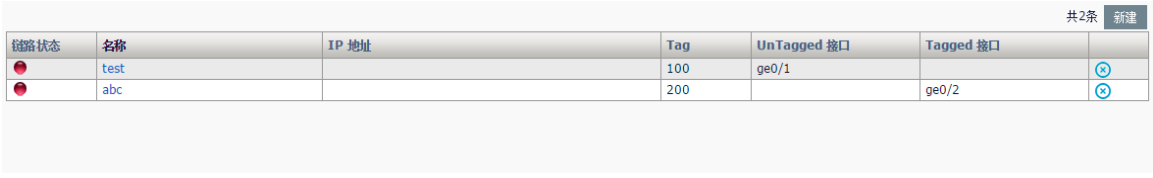


修改 vlan 的 IP 地址、管理状态、UnTagged 接口、Tagged 接口、MTU、STP 配置等信息

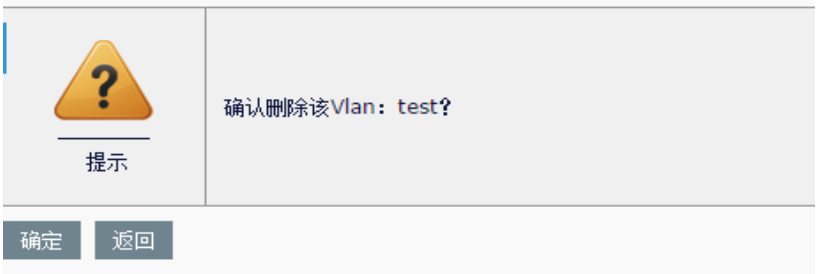
3、点击**更新**完成修改。

15.3.3 删除 VLAN

1、进入**网络>接口配置>VLAN**，如下图：



2、点击删除 VLAN。



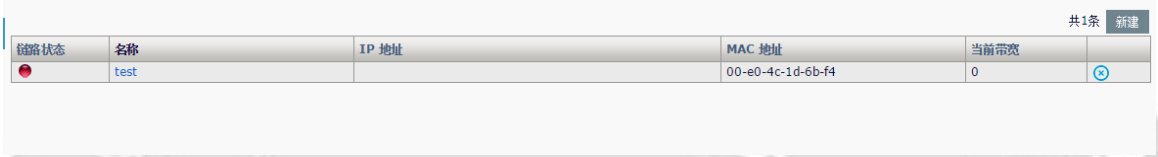
3、点击**确定**删除 VLAN。

15.4 聚合接口

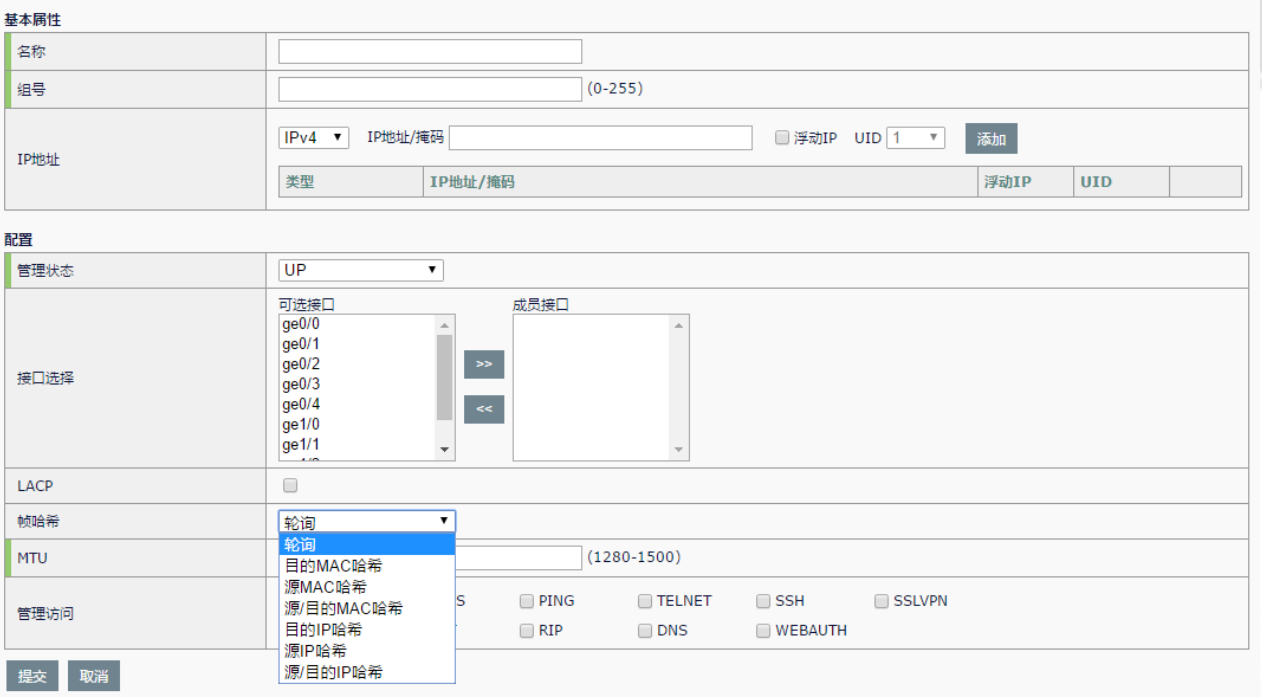
链路聚合是通过将多个链路组合为一个逻辑的网络链路，以提高设备之间通讯通道的容量和可靠性的技术。链路聚合也提供了负载均衡的方式来处理通讯负荷，使得通讯负荷均分在几个链路中，不会有单独一个链路超负载。通过链路聚合，用户可以在许多应用中得到实际的益处：更高的可靠性、更高的带宽，使用现有的设备，节约成本（不需要更新设备来获取更高的带宽）。

15.4.1 添加链路聚合

1、进入**网络>接口配置>聚合接口**，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：



名称：链路聚合名称

组号：链路聚合组号

IP 地址：链路聚合的 IP 地址，可选择 IPv4、IPv6，输入 IP 地址并点击**添加**生效

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，可选轮询/目的 MAC 哈希/源 MAC 哈希/源目的 MAC 哈希/目的 IP 哈希/源 IP 哈希/源目的 IP 哈希/。

MTU：链路聚合 mtu 值，范围为 1280-1500

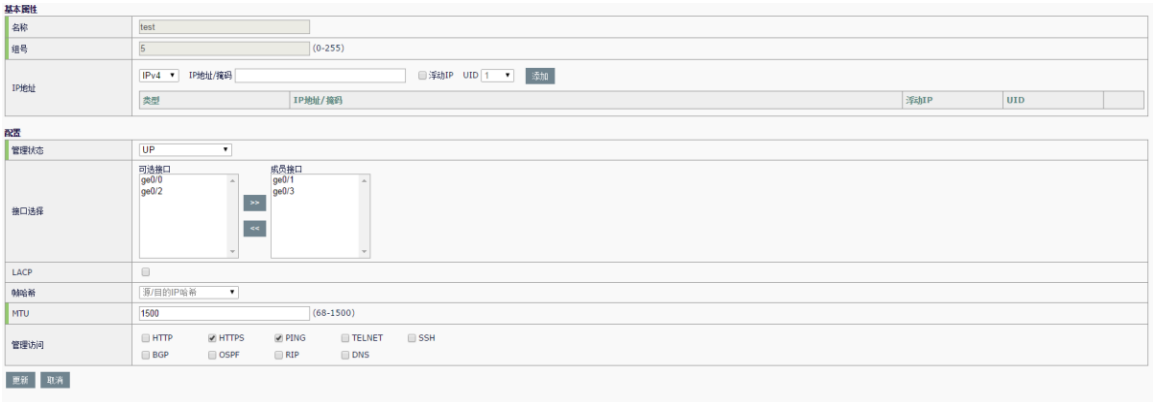
管理访问：配置可通过该链路聚合地址，访问设备提供的服务类别

- **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

15.4.2 修改聚合接口

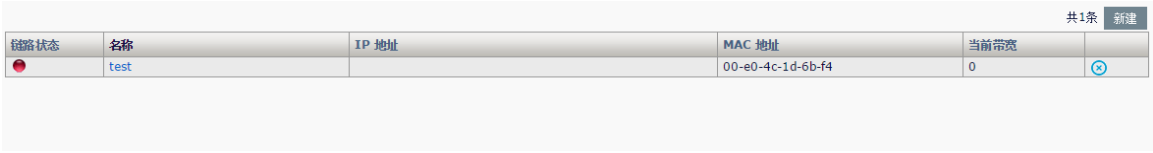
1、进入**网络>接口配置>聚合接口**，如下图：

2、点击链路聚合**名称**修改。



修改链路聚合 IP 地址、管理状态、成员接口、LACP、帧哈希等信息。

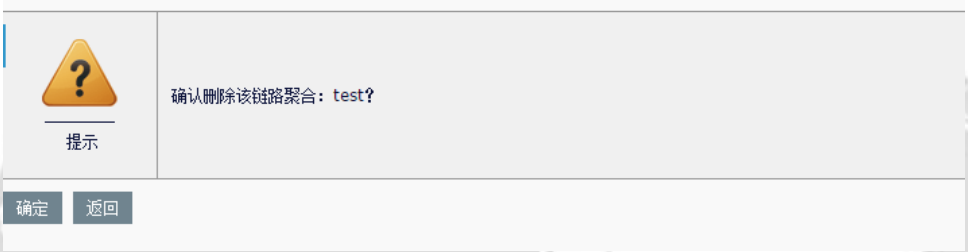
3、点击**更新**完成修改。



15.4.3 删除聚合接口

1、进入**网络>接口配置>聚合接口**，如下图：

2、点击删除链路聚合。

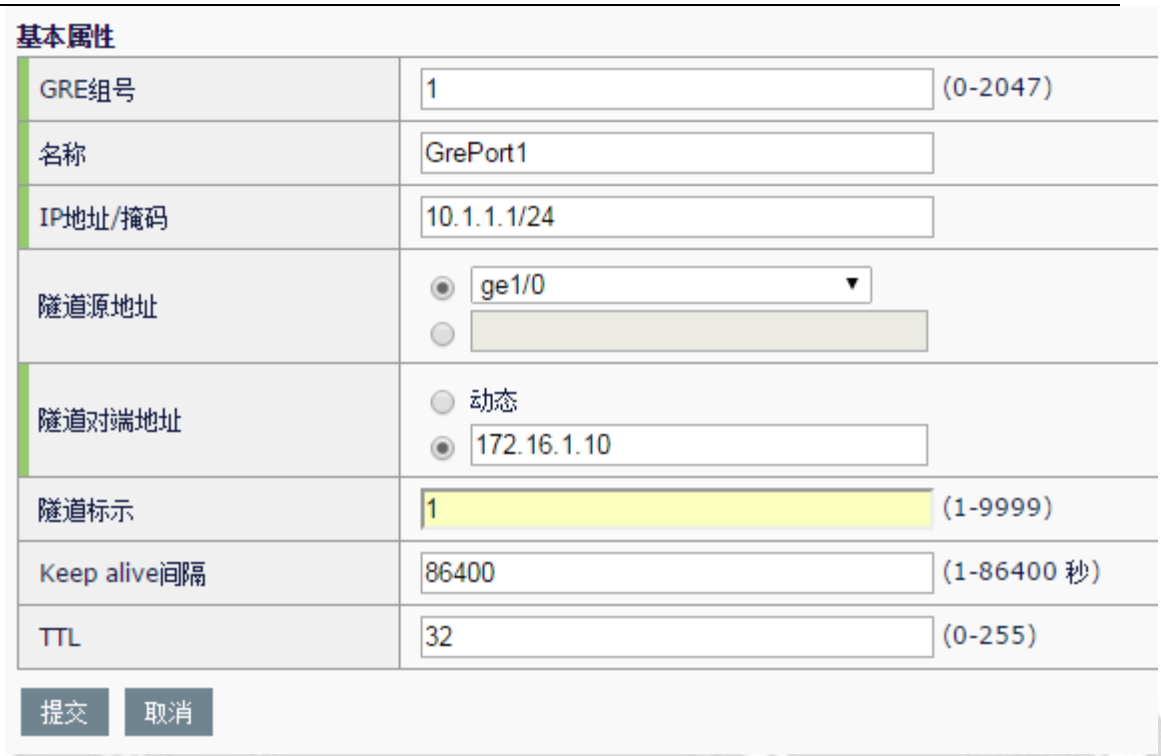


3、点击**确定**删除 VLAN。

15.5 GRE接口

15.5.1 配置 GRE 接口

进入**网络>接口配置>GRE 接口**，点击**新建**。



组号：0-2047

名称：GRE 接口名，不能配置像 vlan，ge，tunl，gre 这样的名字

IP 地址/掩码：GRE 接口的 ip 地址，即封装后的 ip 地址

隧道源地址：封装前的源地址，支持选择接口和手动输入

隧道对端地址：封装前的对端地址

隧道标示：标示隧道，输入范围 1-9999

Keep alive 间隔：开启持续时间 1-86400 秒

TTL：IP 包被路由器丢弃之前允许通过的最大网段数量，0-255

15.6 旁路接口

在此工作模式中，网络的流量不会流经设备，而是由其它网络设备把需要检测的流量镜像一份给系统。在这种部署模式下，IPS 设备不会影响网络的正常运行，也可以通过与防火墙联动等手段来阻断攻击。

15.6.1 配置旁路接口

进入**网络>接口配置>旁路部署**，勾选启动旁路模式的接口就可以完成旁路配置

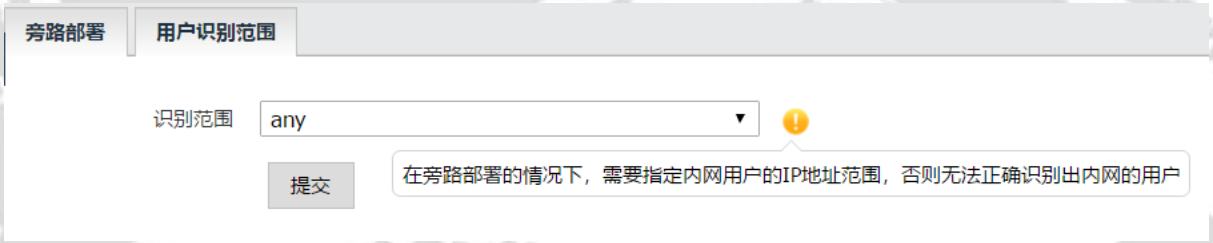
旁路部署 | 旁路用户

	接口名称	状态	启用
1	ge1/0	✓	☑
2	ge1/1	✓	☑
3	ge1/2	✓	☑
4	ge1/3	✓	☑
5	ge1/4	✓	☑
6	ge1/5	✓	☑
7	ge1/6	✓	☑
8	ge1/7	✓	☑
9	xge2/0	−	☐
10	xge2/1	−	☐
11	ge3/0	−	☐
12	ge3/1	−	☐
13	ge3/2	−	☐
14	ge3/3	−	☐
15	ge3/4	−	☐
16	ge3/5	−	☐
17	ge3/6	−	☐
18	ge3/7	−	☐

15.6.2 旁路用户

点击**旁路用户标签**，可以选择识别范围。

在旁路模式下，需要制定内网用户的 IP 地址范围，否则无法正确识别出内网的用户。



15.7 配置案例

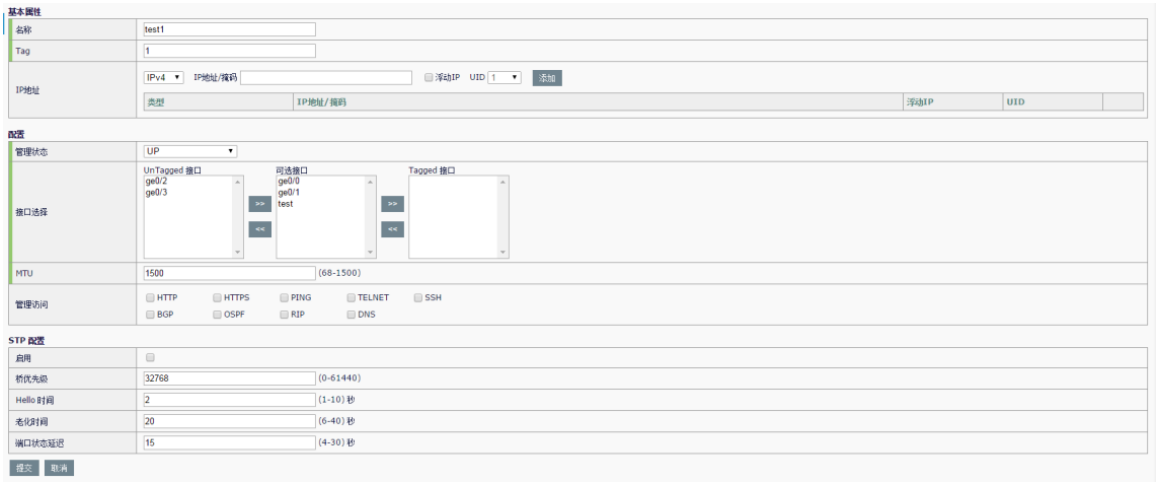
15.7.1 配置案例 1：增加一个 VLAN

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>接口配置>VLAN**，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。

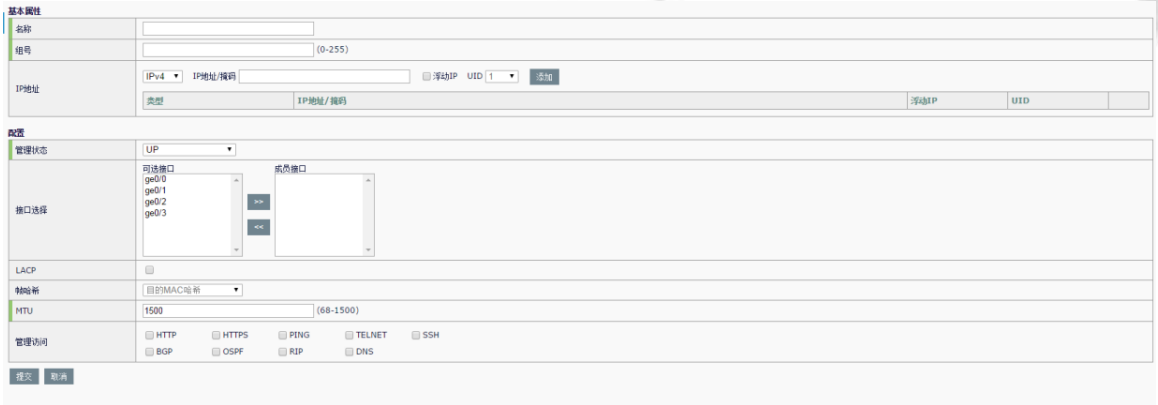
15.7.2 配置案例 2：增加一个聚合接口

案例描述

创建一个聚合接口，并在其中加入物理接口成员。

配置步骤：

1、进入**网络>接口配置>链路聚合**，点击**新建**，如下图：



2、输入参数：名称 tvi1，组号 1，管理状态 UP。

3、**可选接口**中的接口 ge0/1、ge0/2 点击 >> 加入到链路聚合中。

4、**开启 LACP**，**帧哈希**选择源/目的 IP 哈希。

5、点击**提交**完成创建链路聚合。

15.8 常见故障分析

15.8.1 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 合口配置，使两端聚合 LACP 协商成功

15.8.2 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

第16章 DHCP 服务

本模块提供两种 DHCP 服务功能：DHCP 服务器和 DHCP Relay。设备作为 DHCP 客户端时，其配置请参考接口配置。

16.1 DHCP 服务器概述

DHCP 的全称是动态主机配置协议（Dynamic RG-WALL 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。

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络，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。

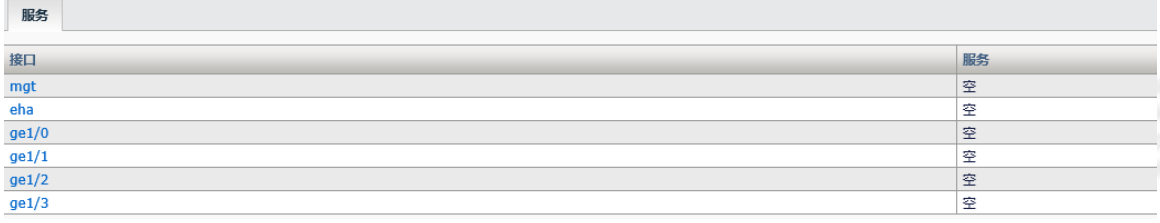
客户端收到确认后开始使用此地址。

16.2 DHCP 中继代理(Relay)

DHCP 中继代理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 中继代理存在的原因是因为 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。

16.2.1 查看服务

1、进入**网络>DHCP>服务**，查看 DHCP 服务概览页面



2、在该页面上，可以“编辑”，设置各个接口下的 DHCP 服务类型。

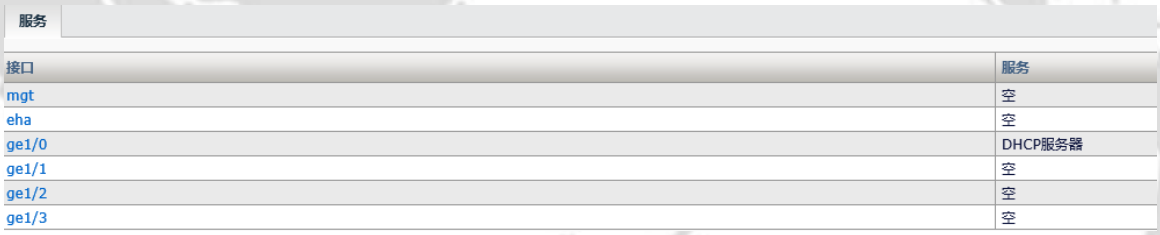
16.2.2 编辑 DHCP 服务

1、进入**网络>DHCP>服务**，点击**接口**名称。

接口：物理口名称

服务：可以启用 DHCP 中继代理，或 DHCP 服务器，或不启用 DHCP 服务

2、点击**提交**，如下图：



3、点击**接口**名称进行更改。

16.2.3 配置服务器

1、进入**网络>DHCP>服务器**，点击**新建**。

接口：新建 DHCP 服务器的名称

子网/掩码：DHCP 服务器的子网网段，及掩码

缺省网关：DHCP 服务器的网关

IP 地址范围：IP 地址池的地址范围

租期：IP 地址的有效期

DNS 服务器 1：DHCP 服务器的主 DNS

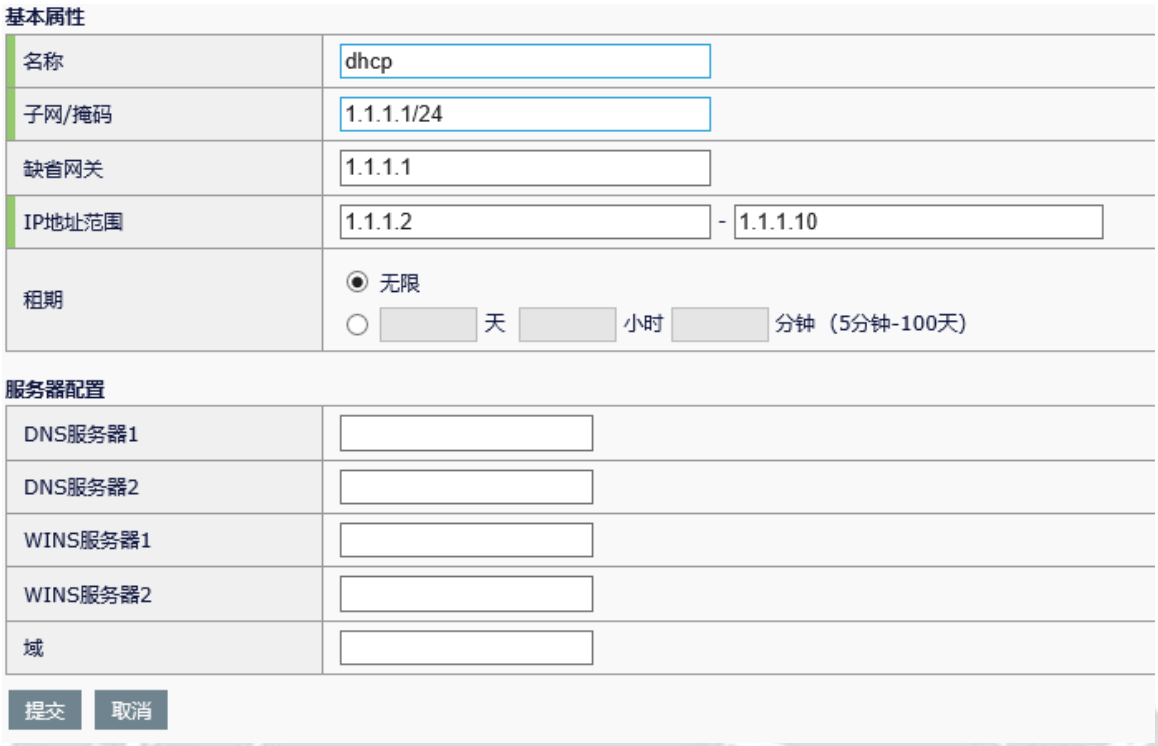
DNS 服务器 2：DHCP 服务器的备 DNS

WINS 服务器 1：DHCP 服务器的主 Wins

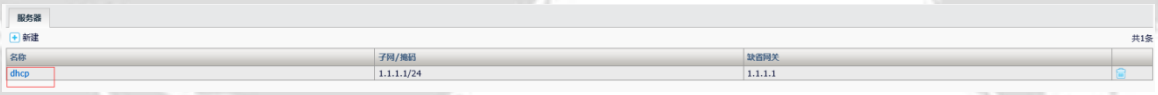
WINS 服务器 2：DHCP 服务器的备 Wins

域：DHCP 服务器的域

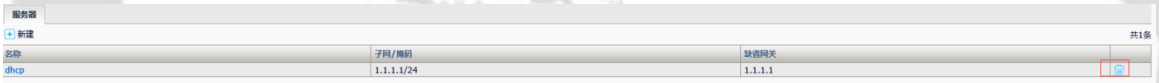
2、配置完成后，点击**提交**。



3、点击 **DHCP** 服务器名称，进行编辑



4、点击**删除**按钮，可以删除 DHCP 服务器



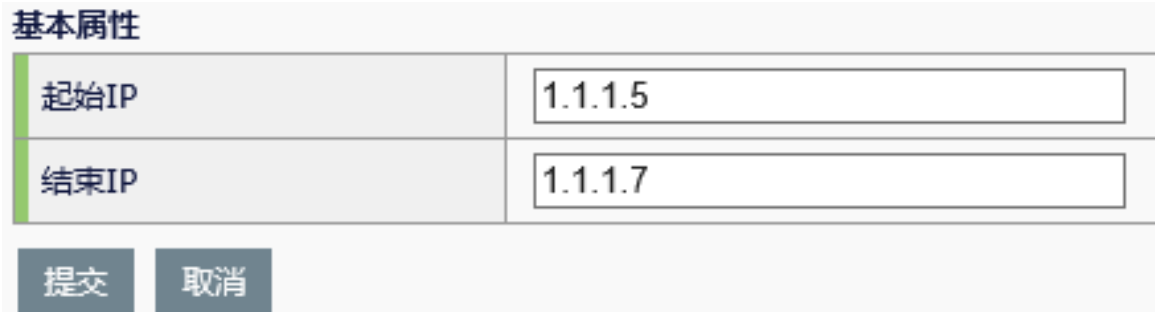
16.2.4 配置排除范围

1、进入**网络>DHCP>排除范围**，点击**新建**。

起始 IP：排除范围的起始 IP 地址

结束 IP：排除范围的结束 IP 地址

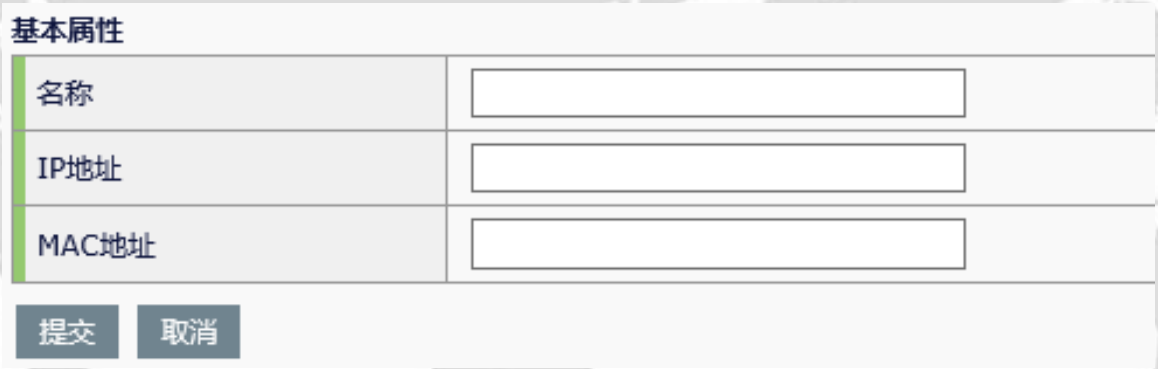
2、配置完成后，点击**提交**。



3、点击**删除**按钮，可以删除排除范围

16.2.5 配置 IP-MAC 绑定

1、进入**网络>DHCP>IP-MAC 绑定**，点击**新建**。

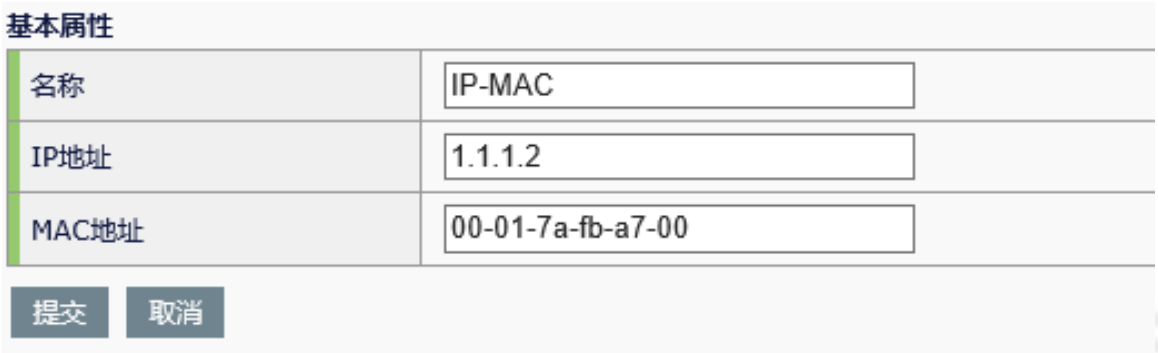


名称：IP-MAC 绑定配置的名称

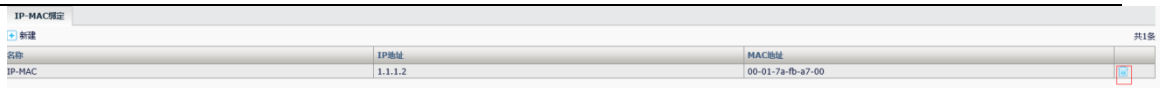
IP 地址：要绑定的 IP 地址

MAC 地址：要绑定的 MAC 地址

2、配置完成后，点击**提交**。

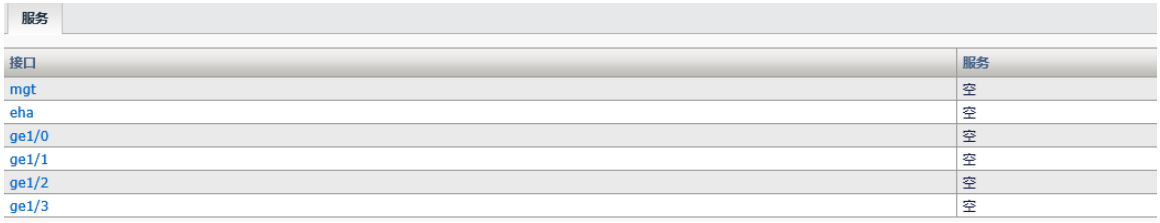


3、点击**删除**按钮，可以删除 IP-MAC 绑定



16.2.6 监视器

1、进入**网络>DHCP>监视器**，在该配置页面，可以“查看”所有已分配出去的 IP 地址，可以“清除”已分配的 IP 地址。



服务

接口	服务
mgt	空
eha	空
ge1/0	空
ge1/1	空
ge1/2	空
ge1/3	空

第17章 安全域

17.1 安全域概述

域就是接口组，可以在一个域中加入多个接口，但是一个接口只能属于一个域。如果一个接口被包含在某个域中，就不能单独对该接口进行配置。

17.2 安全域配置

17.2.1 添加安全域

配置步骤：

1、进入**网络>安全域**：点击**新建**进入安全域配置页面

名称：安全域名称

允许接口间相互访问：是否允许组内成员互访

接口选择：添加组内接口

2、点击**提交**，完成设置。

17.2.2 修改安全域

配置步骤：

1、进入**网络>安全域**，如下图：

2、点击安全域**名称**修改。

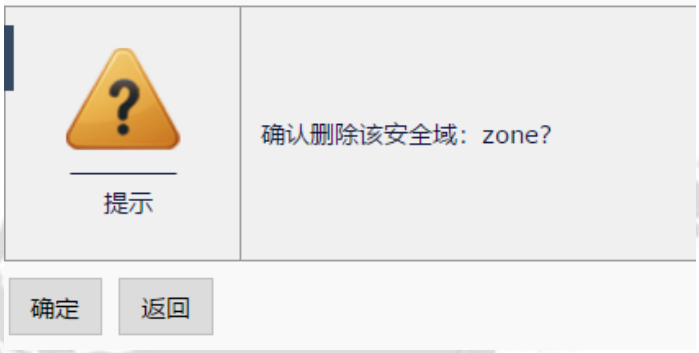
修改安全域的组内成员，选择是否**允许接口间相互访问**。

3、点击**更新**完成修改。

17.2.3 删除安全域

1、进入**网络>安全域**，如下图：

2、点击 删除安全域。



3、点击**确定**删除安全域。

第18章 静态路由

18.1 静态路由概述

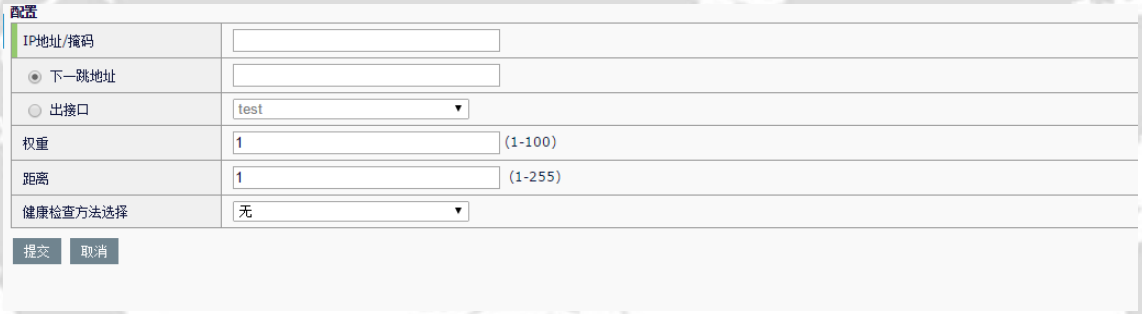
静态路由是在路由器中人工配置的固定路由条目。除非网络管理员干预，否则静态路由不会发生变化。由于静态路由不能对网络的改变作出反映，一般用于网络规模不大、拓扑结构固定的网络中。静态路由的优点是简单、高效、可靠。在所有的路由中，静态路由优先级最高。当动态路由与静态路由发生冲突时，以静态路由为准。

18.2 配置静态路由

18.2.1 配置 IPv4 静态路由

配置步骤：

1、进入**网络>IPv4 路由>静态路由**：点击**新建**进入静态路由配置页面



IP 地址/掩码：目的 IP 地址及掩码。

下一跳地址：路由网关地址。

出接口：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>。

健康检查方法选择：选择健康检查对象

2、点击**提交**，完成设置。

18.2.2 查看 IPv4 路由表

配置步骤：

1、进入**网络>IPv4 路由>路由表**：路由表查看

路由表

所有 ▼ 目的地址 下一跳 搜索 共14条

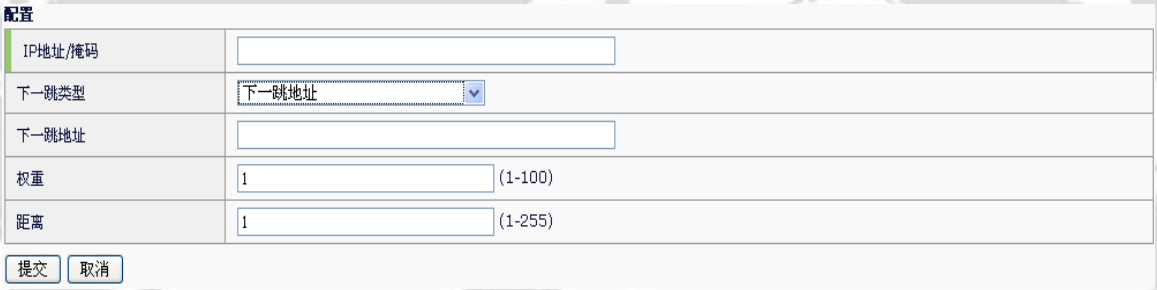
类型	目的地址	下一跳	出接口	距离	权重	持续时间	系统状态
静态	0.0.0.0/0	172.17.0.1	ge1/7	1	1	00:14:16	有效
直连	9.9.9.0/24		tunl1	0	0	00:14:19	有效
主机	9.9.9.1/32		tunl1	0	0	00:14:19	有效
直连	127.0.0.0/8		lo	0	0	00:14:47	有效
静态	172.0.0.0/8	172.17.0.1	ge1/7	1	1	00:14:16	有效
直连	172.17.0.0/16		ge1/7	0	0	00:14:16	有效
主机	172.17.90.99/32		ge1/7	0	0	00:14:16	有效
静态	192.168.0.201/32	172.17.0.1	ge1/7	1	1	00:14:16	有效
直连	198.16.20.0/24		ge1/1	0	0	00:05:41	有效
主机	198.16.20.1/32		ge1/1	0	0	00:05:41	有效
直连	198.16.80.0/24		ge1/3	0	0	00:14:14	有效
主机	198.16.80.1/32		ge1/3	0	0	00:14:14	有效
直连	198.16.100.0/24		ge1/8	0	0	00:13:07	有效
主机	198.16.100.1/32		ge1/8	0	0	00:13:07	有效

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。

18.2.3 配置 IPv6 静态路由

配置步骤：

1、进入**网络>IPv6 路由>静态路由**：点击**新建**进入 IPv6 路由页面



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。

权重：路由权重，范围 1-100。

距离：路由优先级，范围<1-255>。

2、点击**提交**，完成设置。

18.2.4 查看 IPv6 路由表

配置步骤：

1、进入**网络>IPv6 路由>路由表**：进入 IPv6 路由表查看页面。

路由表

所有 ▾ 目的地址 下一跳 搜索 共8条

类型	目的地址	下一跳	出接口	距离	权重	持续时间	系统状态
直连	::1/128		lo	0	0	00:19:07	有效
直连	6a8a::/64		ge1/1	0	0	00:10:01	有效
直连	6a8c::/64		ge1/3	0	0	00:18:34	有效
直连	9a9a::/64		lo	0	0	00:18:46	有效
直连	fe80::/64		ge1/8	0	0	00:00:30	有效
直连	fe80::/64		ge1/1	0	0	00:10:01	有效
直连	fe80::/64		ge1/3	0	0	00:18:33	有效
直连	fe80::/64		ge1/7	0	0	00:12:04	有效

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。

第19章 策略路由

19.1 策略路由概述

策略路由，也叫做基于策略的路由，是指在决定一个 IP 包的下一跳转发地址时，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。它转发分组到特定网络需要基于预先配置的策略，这个策略可能指定从一个特定的网络发送的通信应该被转发到一个指定的接口。

19.2 配置策略路由

19.2.1 配置策略路由

配置步骤：

1、进入**网络>IPv4 路由>策略路由**：点击**新建**进入策略路由配置页面

入接口：数据流的流入方向，可以指定某个特定接口

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。

用户：数据流中源 IP 地址所对应用户。any 表示用户为任意。

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。

应用：数据流中匹配的应用，any 表示应用为任意。

时间：数据流中匹配的应用，any 表示应用为任意。

下一跳：路由网关地址。

权重：路由权重，范围 1-100。

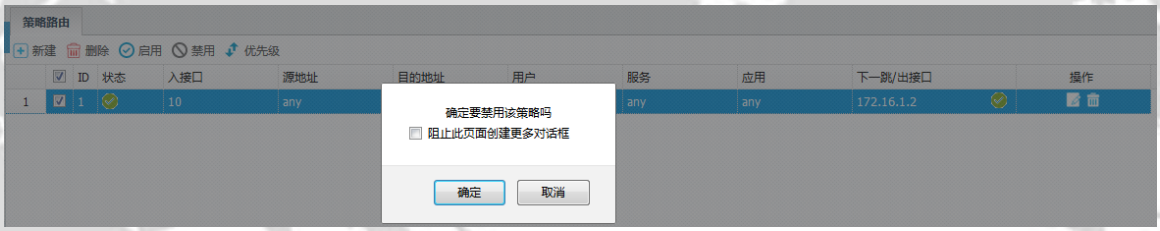
健康检查方法选择：选择健康检查对象。

多路径选择：可选根据源 IP/根据连接。

2、查看策略

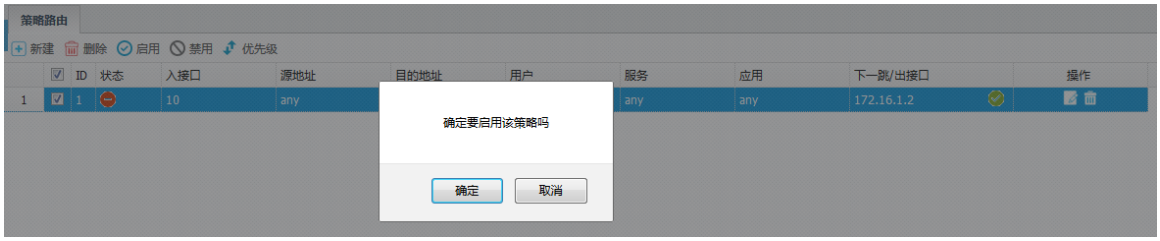
19.2.2 配置策略启用/禁用

1、进入**网络>IPv4 路由>策略路由**，选中策略，点击**禁用**。



2、提交后，查看策略状态为禁用。

3、选中策略，点击**启用**。



4、提交后，查看策略状态为启用。

19.2.3 编辑策略路由

配置步骤：

1、进入**网络>IPv4 路由>策略路由**，对某条存在的策略路由点击  进入编辑界面

2、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**。

19.2.4 删除策略路由

配置步骤：

1、进入**网络>IPv4 路由>策略路由**

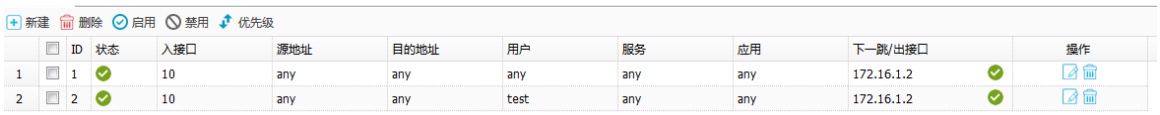
2、点击 删除策略。

19.2.5 调整策略路由的顺序

通过移动策略可以调整安全策略的顺序，从而使位置在前的策略优先匹配。

配置步骤：

1、进入**网络>IPv4 路由>策略路由**，如下图：



2、点击 优先级 移动策略。

被移动策略 ID：需要被移动的策略的 ID 号。

目标策略 ID：参考被移动策略的 ID 号。

策略最前：移动策略到最前。

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。

策略最后：移动策略到最后。

3、点击**提交**。

第20章 配置 RIP

20.1 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，以每 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、毒性逆转机制来防止路由环的形成，并且使用触发更新和路由超时机制确保路由的正确性。

20.2 配置RIP协议

20.2.1 缺省配置信息

下一代防火墙设备关于 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

20.2.2 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>IPv4 路由>动态路由>RIP**：进入 RIP 配置页面

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。

20.2.3 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>IPv4 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

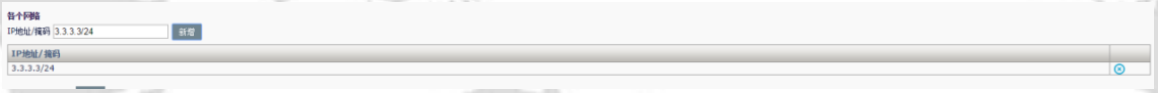
RIP 定时器-超时：设置超时定时器的触发时间
RIP 定时器-失效：设置垃圾收集定时器的触发时间
路由重发布-直连路由：设置是否重发布直连路由
路由重发布-OSPF：设置是否重发布 OSPF 路由
路由重发布-静态路由：设置是否重发布静态路由
跳数：三种重发布类型进行重发布是的度量

2、点击**提交**：完成对 RIP 的设置。

20.2.4 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>IPv4 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

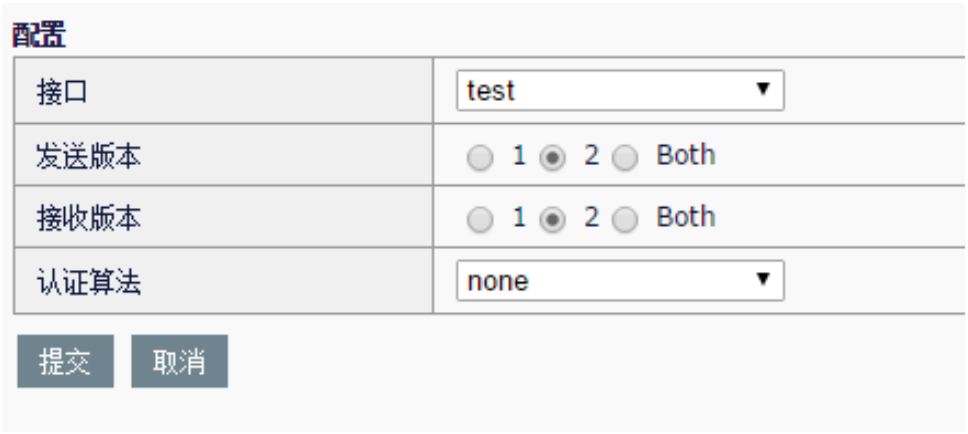


3、点击  ：删除对应配置的网络。

20.2.5 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>IPv4 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**

4、点击**接口名称**：对已有的接口配置进行编辑。

5、点击  ：删除对应接口的配置。

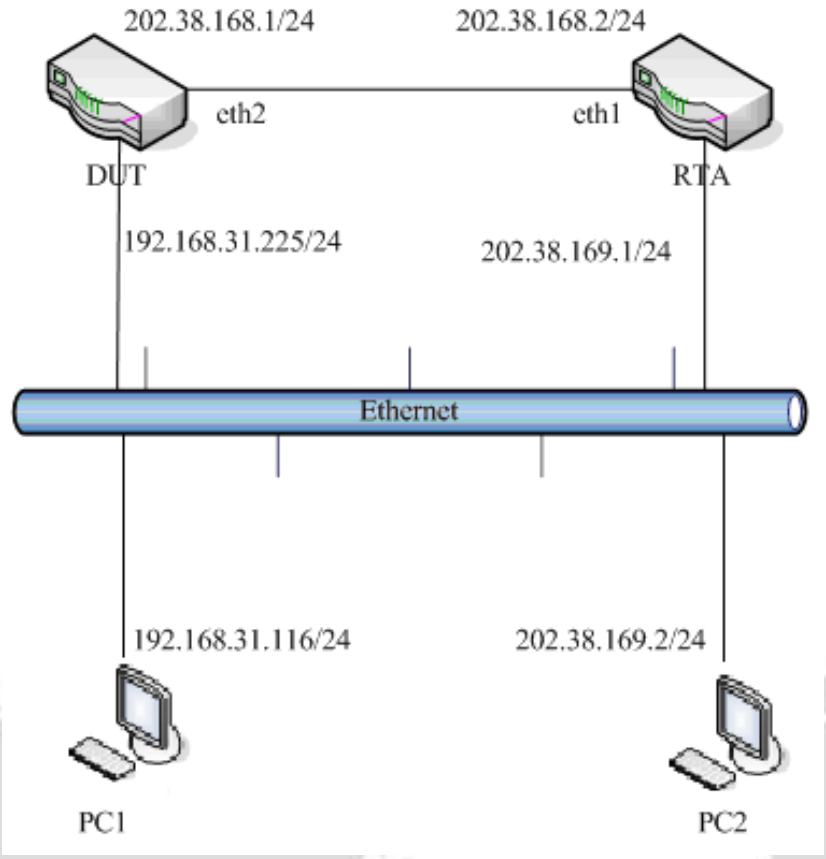
20.3 配置案例

20.3.1 配置案例：配置两台下一代防火墙设备互连

案例描述

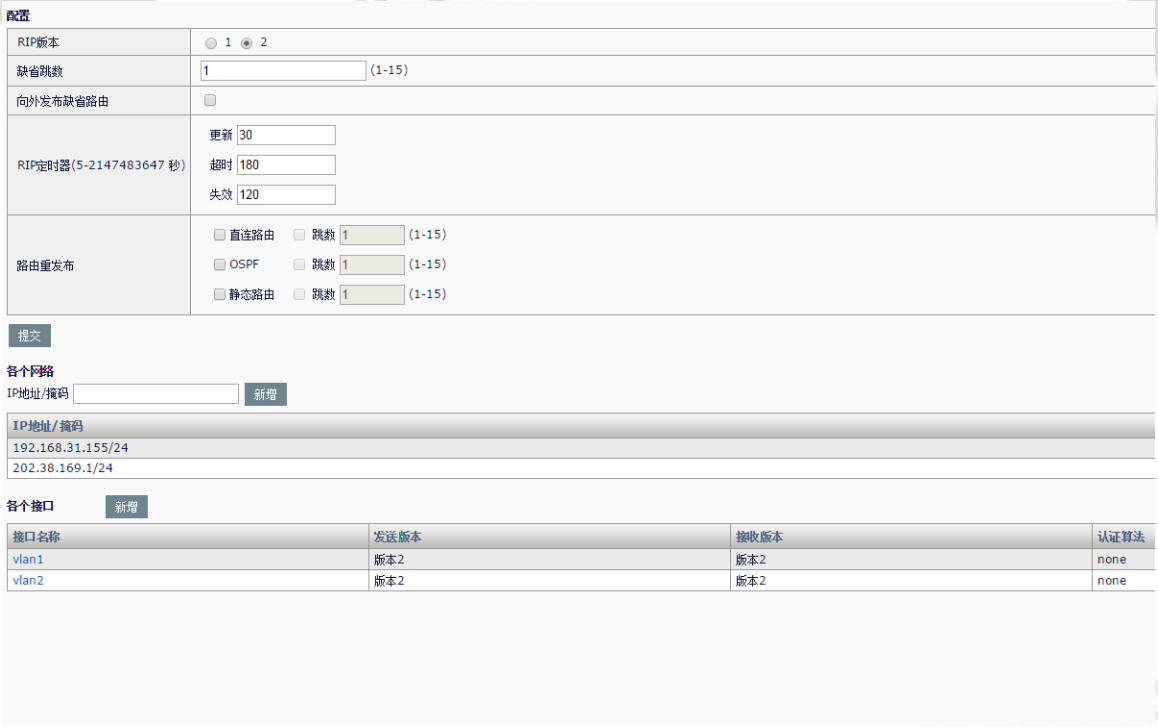
DUT 和 RTA 都为下一代防火墙设备，IP 地址配置如图，DUT 在 vlan0 和 vlan2 接口上启用了 RIP，RTA 在接口 vlan0 和 vlan1 上启用了 RIP，两个设备互连的接口收发报文的版本都设置为 2）。

案例组网图：

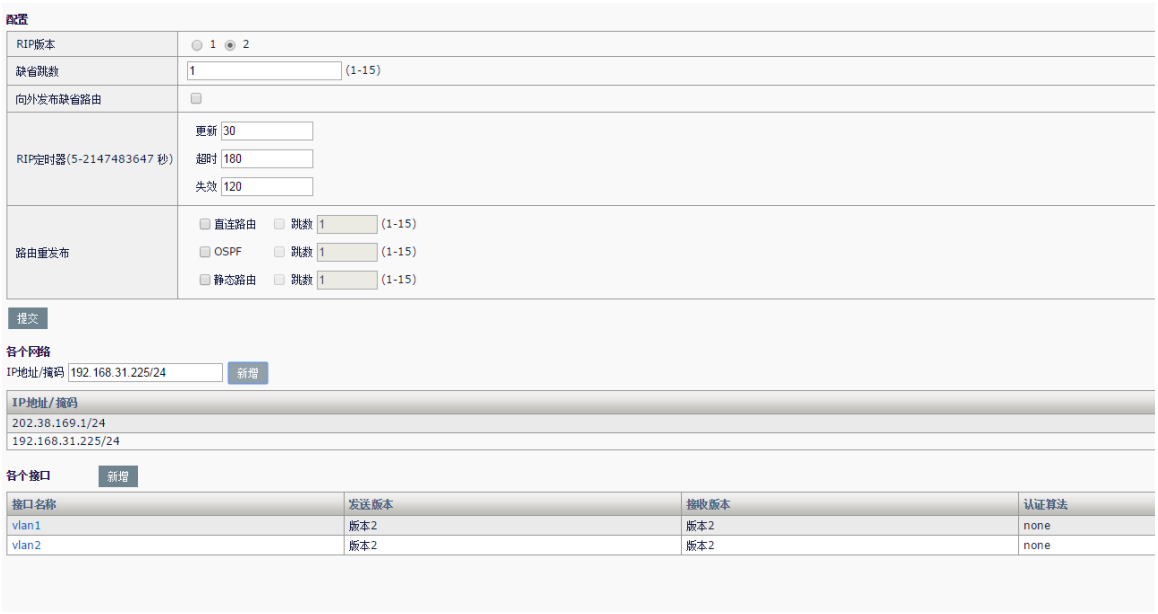


配置步骤：

1、配置 DUT 的基本信息。



2、RTA 的基本配置。

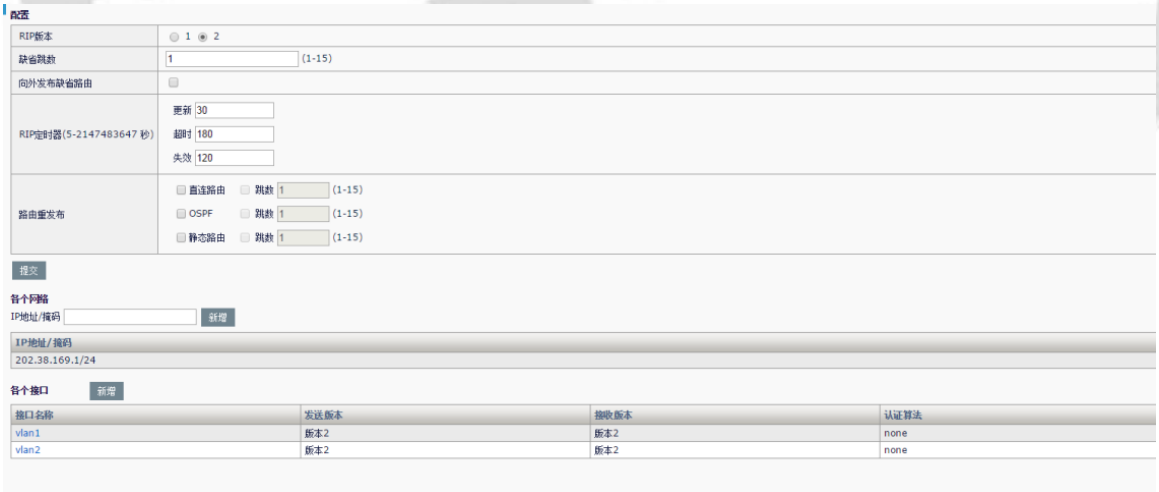


3、配置 PC1 的网关为 192.168.31.225，配置 PC2 的网关为 202.38.169.1。从 PC1PING 向 PC2，可以 PING 通。

20.4 查看RIP配置信息

20.4.1 查看 RIP 配置信息

进入**网络>IPv4 路由>动态路由>RIP**，可以查看 RIP 的配置。



20.5 常见故障分析

20.5.1 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

第21章 配置 OSPF

21.1 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。

21.2 配置OSPF协议

21.2.1 缺省配置信息

下一代防火墙设备关于 OSPF 的缺省设置信息如以下表所示：

OSPF 缺省配置信息

内容	缺省设置	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

21.2.2 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>IPv4 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。

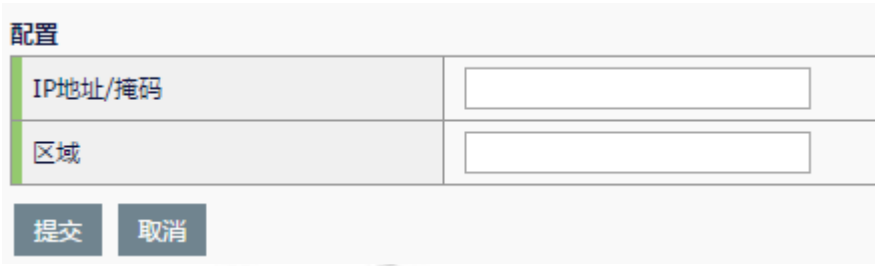
2、点击**提交：**完成对 OSPF 的设置。

21.2.3 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>IPv4 路由>动态路由>OSPF**：进入配置页面

2、点击**新增**：



IP 地址/掩码：网络地址和网络地址掩码

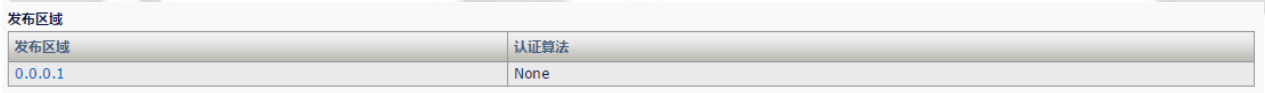
区域：区域 ID

3、点击**提交**。

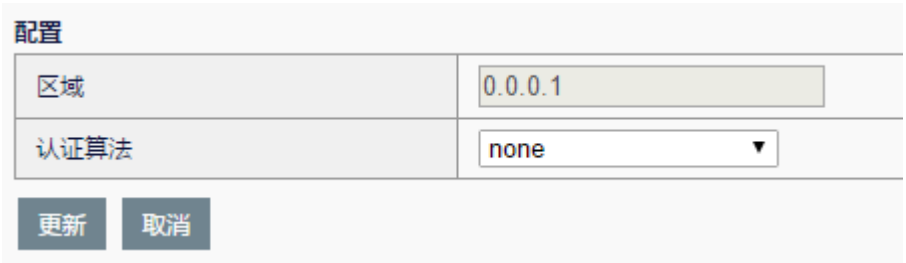
21.2.4 编辑区域属性

编辑区域的认证方式：

1、进入**网络>IPv4 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**提交**。

21.2.5 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>IPv4 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。

ID：Key-ID。

密钥：密文认证时候的密钥。

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。

3、点击**提交**，完成配置

21.3 OSPF监控与维护

21.3.1 查看邻居路由器状态信息

进入**网络>IPv4 路由>动态路由>OSPF 监视器**，可以查看邻居路由状态信息：

21.4 常见故障分析

21.4.1 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	区域 ID 不匹配 认证类型不匹配 密钥不匹配 网段（网络掩码匹配） Hello-interval 不匹配 Dead-interval 不匹配 两台设备间是否需要建立邻接关系？
解决	检查接口上 OSPF 参数的配置 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： 网络类型是点对点的 网络类型是点到多点的 网络类型是虚链路 本地路由器是邻接路由器所在网络的 DR 本地路由器是邻接路由器所在网络的 BDR 邻居路由器是 DR 邻居路由器是 BDR

第22章 配置 BGP

22.1 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。

22.2 配置BGP协议

22.2.1 缺省配置信息

BGP 缺省配置信息

内容	缺省设置	备注
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
缺省路由生成	不生成	可更改设置
EBGP 多跳	关闭/2555	可更改设置
发布缺省路由	不发布	可更改设置
TCP MD5 认证	不认证	不可更改设置
Keepalive Time 值	60 秒	建议采用缺省设置
Holdtime 值	180 秒	可更改设置
ConnectRetry time	120 秒	不可更改设置
AdvIntelval（IBGP）	15 秒	建议采用缺省设置
Advintelval(EBGP)	30 秒	建议采用缺省设置
Bgp scan time	60 秒	可更改设置
MED 值	0	可更改设置
Local_pref 值	100	可更改设置
路由聚合	关闭	可更改设置
路由衰减	关闭	可更改设置
Suppress limit	2000	可更改设置
Half-life-time	15minutes	可更改设置
Reuse limit	750	可更改设置

Max-suppress time	4*half-life-time	可更改设置
管理距离	EBGP 20 IBGP 200 Local 200	
IGP 路由检查	不检查	可更改设置

22.2.2 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>IPv4 路由>动态路由>BGP4**,查看配置页面

参数说明：

本地自治系统：本地自治系统的 ID,用户指定。

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。

2、填写本地自治系统 ID。

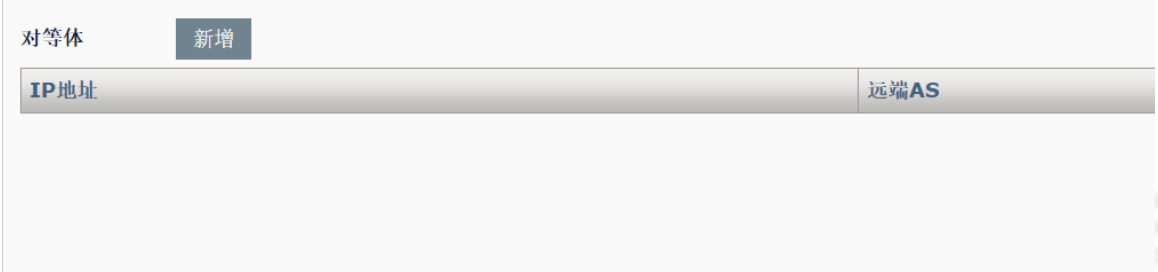
3、点击**提交：**完成对路由器 ID 设置，并且按照高级选项的默认值进行配置。

22.2.3 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>IPv4 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

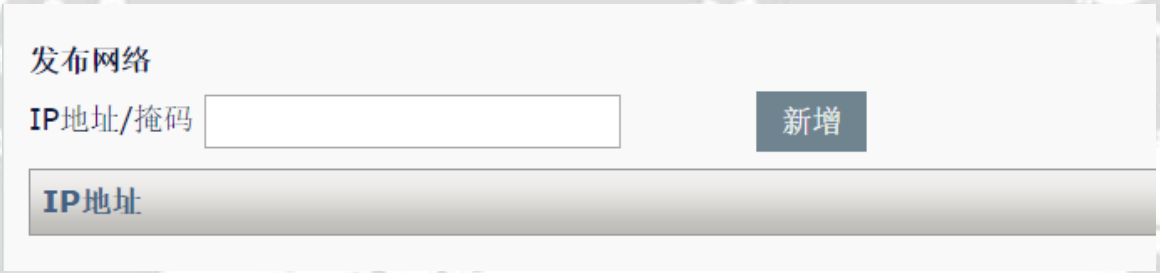
3、点击**提交**：提交对应的配置。点击**取消**：取消本次配置。

22.2.4 配置发布网络

配置发布网络：

配置步骤：

1、进入**网络>IPv4 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。

22.3 常见故障分析

22.3.1 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	两边 peer 地址路由不可达 对等体 IP 地址或者 AS 号配置错误 Open 报文协商不成功 配置 loopback 接口路由不可达 Igp 之间网络不通 Router-id 冲突
解决	检查接口配置

	打开 debug 开关 通过抓包分析

第23章 静态 ARP

23.1 静态ARP概述

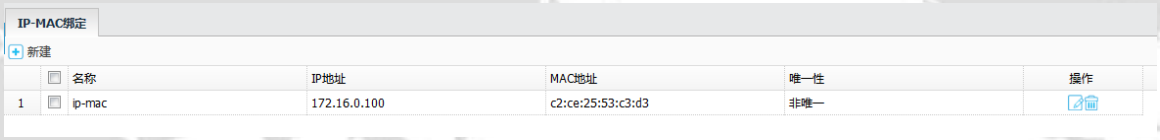
IP 数据包常通过以太网发送。以太网设备并不识别 32 位 IP 地址：它们是以 48 位以太网地址(MAC 地址)传输以太网数据包的。因此，IP 驱动器必须把 IP 地址转换成 MAC 地址。在这两种地址之间存在着某种静态的或算法的映射，常常需要查看一张表。地址解析协议(Address Resolution Protocol，ARP)就是用来确定这些映象的协议。

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。

23.2 静态ARP配置

23.2.1 添加静态 ARP

1、进入**网络>ARP>ARP 绑定**，如下如所示：



名称：arp 绑定名

IP 地址：静态 ARP 被绑定的 IP 地址

MAC 地址：静态 ARP 被绑定的 MAC 地址

唯一性：ip 地址与 mac 地址的绑定是否唯一

2、点击**新建**添加静态 ARP，如下图所示：

名称：arp 绑定名

IP 地址：静态 ARP 被绑定的 IP 地址

MAC 地址：静态 ARP 被绑定的 MAC 地址

唯一性：ip 地址与 mac 地址的绑定是否唯一

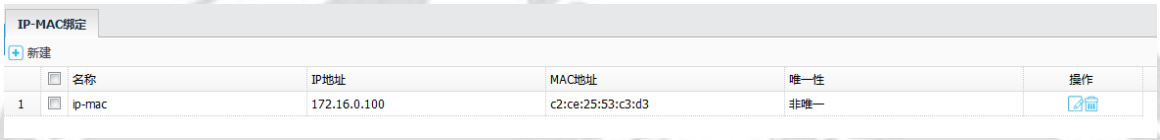
3、点击**提交**完成今天 ARP 的添加。

提示：

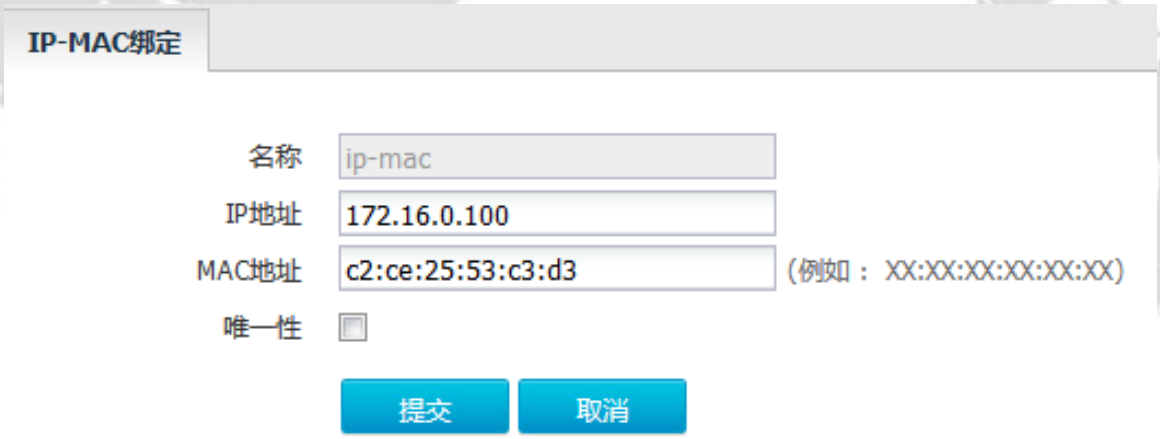
配置静态 ARP 时，MAC 地址可以重复添加，但 IP 地址必须唯一。

23.2.2 修改静态 ARP

1、进入**网络>静态 ARP**，如下如所示：



2、点击静态 ARP 的 修改，如下图所示：

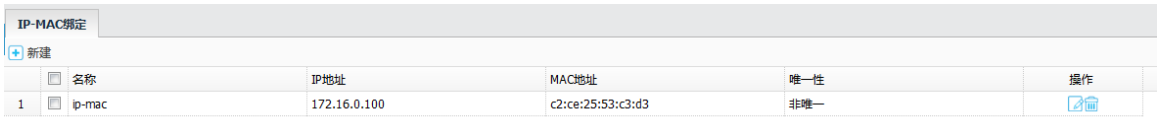


修改静态 ARP 的 ip 地址跟 MAC 地址信息。

3、点击**更新**完成修改。

23.2.3 删除静态 ARP

1、进入**网络> ARP>ARP 绑定**，如下如所示：



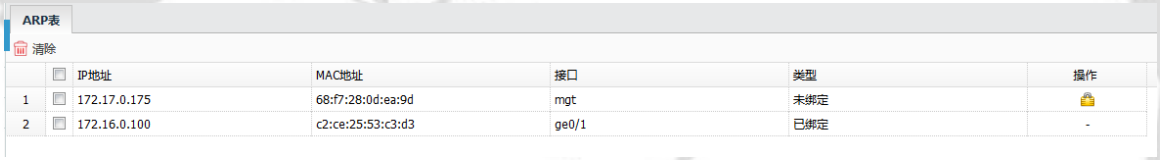
2、点击 删除静态 ARP，如下图所示：

3、点击**确定**删除。

23.3 静态ARP表查看

23.3.1 查看 arp 表

进入**网络>ARP>ARP**



IP 地址：ip 地址

MAC 地址：mac 地址

接口：对应的接口

类型：是否已绑定 arp

操作：对于未绑定的记录可进行 ip-mac 绑定

23.3.2 ip-mac 绑定

点击 可以将未绑定的 ip 地址、mac 地址绑定

23.3.3 清除 arp 表

点击  可以删除某条 arp 记录

点击确定，即可删除

23.4 常见故障分析

23.4.1 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 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

第24章 跨协议转换

24.1 跨协议转换概述

跨协议转换，即 IPv4 与 IPv6 协议地址的互转功能，主要是为了满足用户实现不同网络协议栈之间的互访的需求，实现两种协议栈的无缝衔接，从而可达到从 IPv4 网络环境逐步向 IPv6 网络环境过渡的效果。

目前下一代防火墙设备实现了 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。

24.2 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。

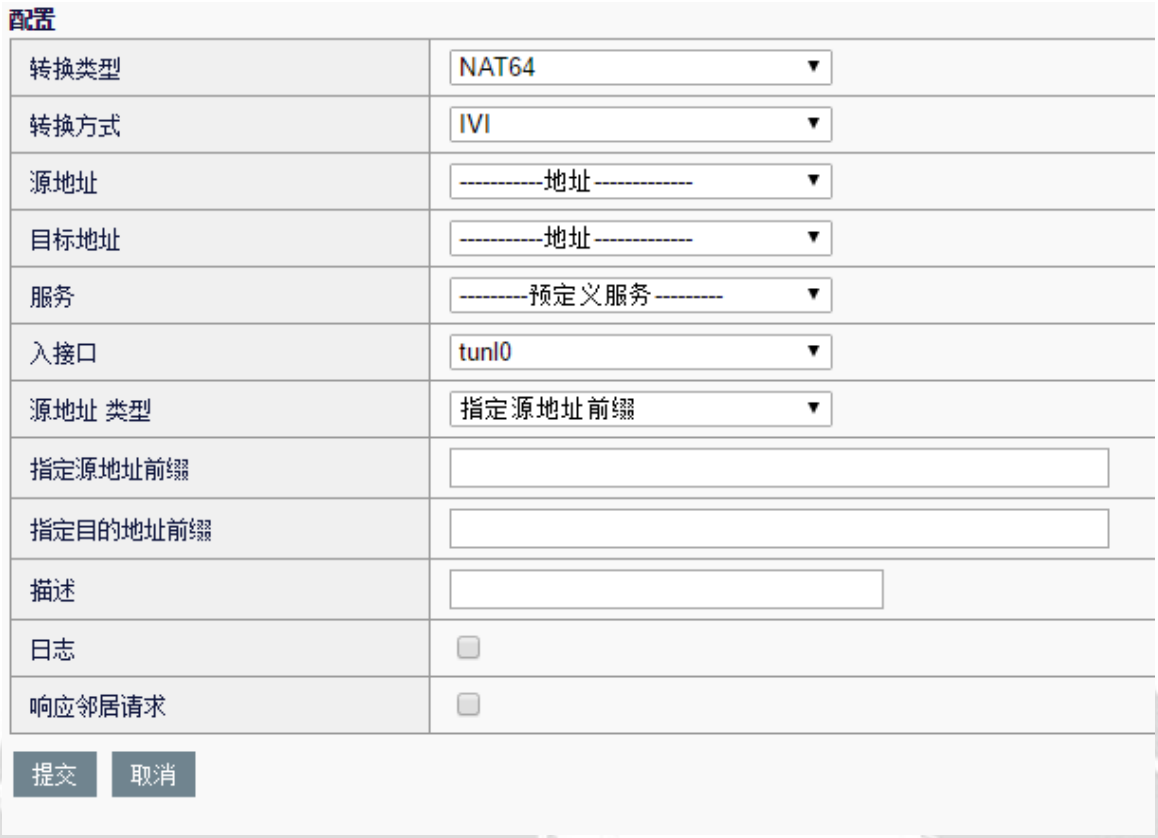
24.2.1 配置 IVI 转换方式

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**策略>NAT 策略>跨协议转换**，点击**新建**。



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。

描述：添加对该规则的描述，最多可为 128 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。

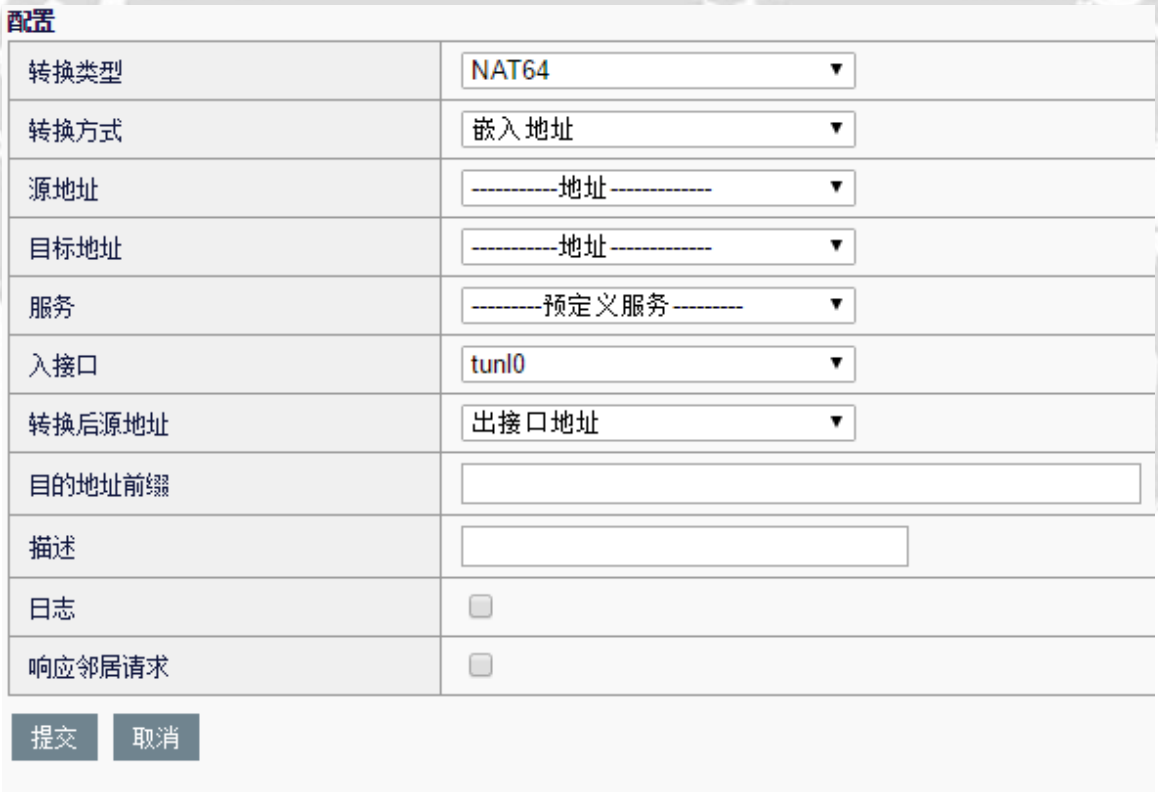
2、点击**提交**。

24.2.2 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。源地址转换可指定 NAT 地址池，或者直接转换为出接口地址。

配置步骤：

1、进入**策略>NAT 策略>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”。



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）。

描述：添加对该规则的描述，最多可为 128 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)。

提示：

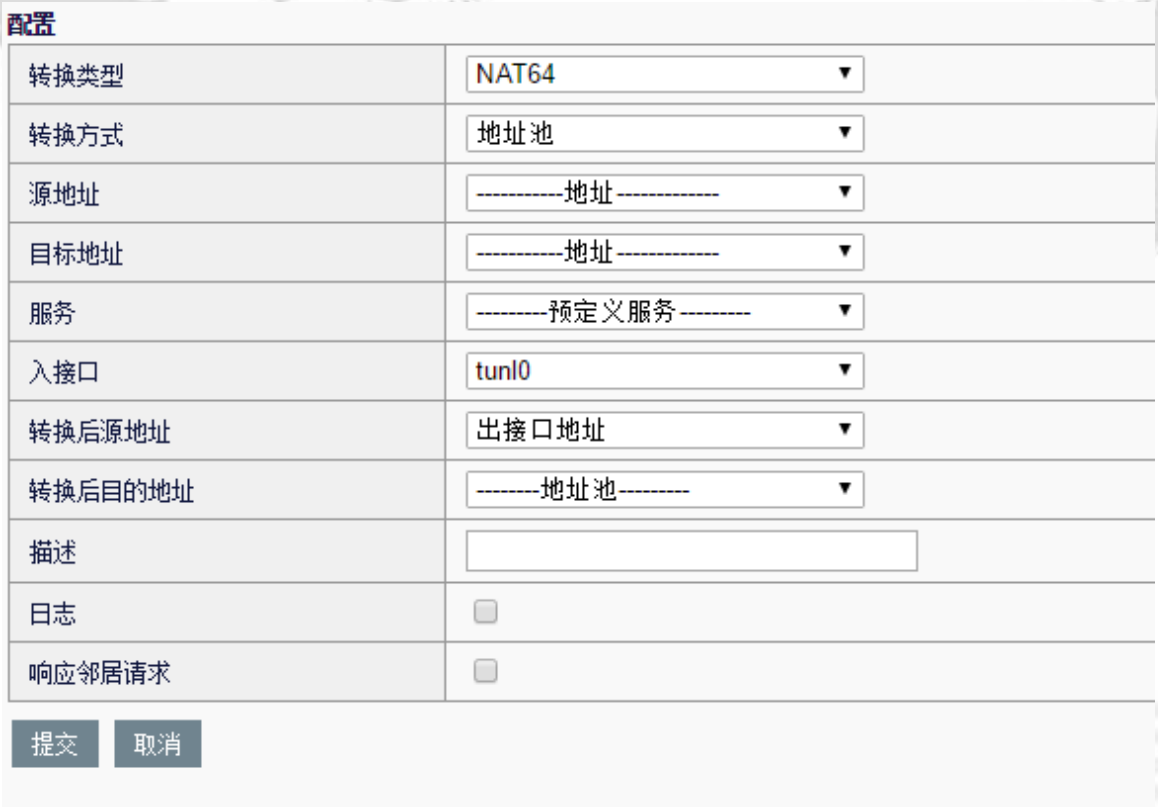
进行嵌入地址转换时，如果配置的目的地址前缀与匹配到该规则的报文的目的地址不符，那么报文不会进行任何更改。

24.2.3 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：

1、进入**策略>NAT 策略>跨协议转换**，点击**新建**，转换方式选择“地址池”。



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。

描述：添加对该规则的描述，最多可为 128 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，)。

提示：

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。

24.2.4 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**策略>NAT 策略>跨协议转换**。

#	所有	入接口	转换后源地址	转换后目的地址	转换方式	日志	描述	
1	NAT64	tunl0	出接口地址		IVI	禁用		

2、点击规则编号。

3、对原有的规则进行编辑。

4、点击**更新**。

24.2.5 删除跨协议转换规则

删除步骤：

1、进入**策略>NAT 策略>跨协议转换**。

#	所有	入接口	转换后源地址	转换后目的地址	转换方式	日志	描述	
1	NAT64	tunl0	出接口地址		IVI	禁用		

2、点击规则编号后对应的，删除该条跨协议转换规则。

24.2.6 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**策略>NAT 策略>跨协议转换**。

#	所有	入接口	转换后源地址	转换后目的地址	转换方式	日志	描述	
1	NAT64	tunl0	出接口地址		IVI	禁用		
2	NAT64	ge4/0	出接口地址		IVI	禁用		

2、点击要移动的规则编号后对应的，可移动该规则。

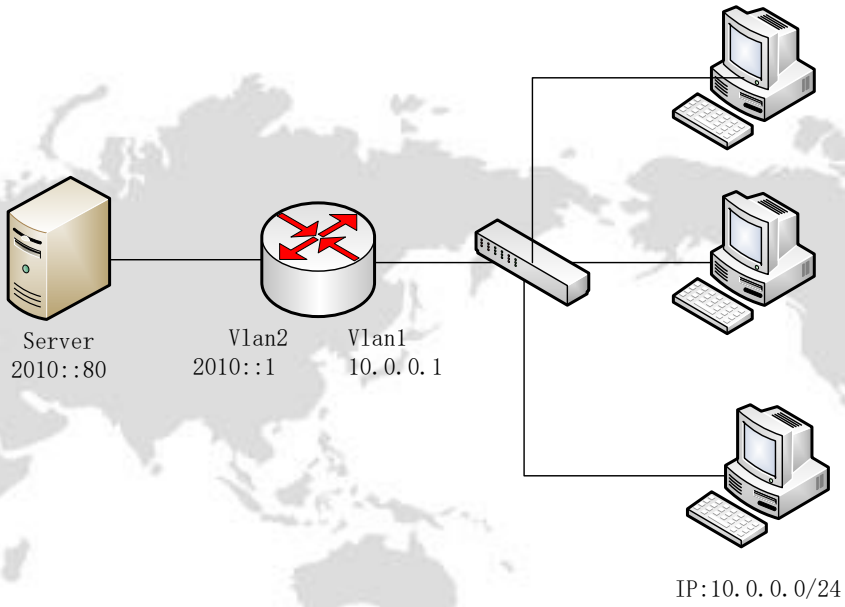
24.3 配置案例

24.3.1 配置 NAT46 转换

案例描述：

公司内部局域网为 IPv4 网络，需要通过应用设备访问另外一个 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。下一代防火墙作为核心路由，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>地址对象**，创建 IPv4 类型的地址对象“inside-net”。

2、进入**对象>地址对象>地址对象**，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	引用	描述	
any	0.0.0.0/0,::/0	8		
inside-nat	10.0.0.0/24	0		
inside-ftp	10.0.0.100	0		

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

名称	起始地址	结束地址	选择算法	描述	
⊟ ftp-server			默认		
	2010::80	2010::80			

4、进入**策略>NAT 策略>跨协议转换**，创建 NAT46 规则。

配置

转换类型	NAT46
转换方式	地址池
源地址	inside-nat
目标地址	inside-ftp
服务	ftp
入接口	ge4/0
转换后源地址	出接口地址
转换后目的地址	ftp-server
描述	
日志	
响应ARP	

提交 取消

提示：

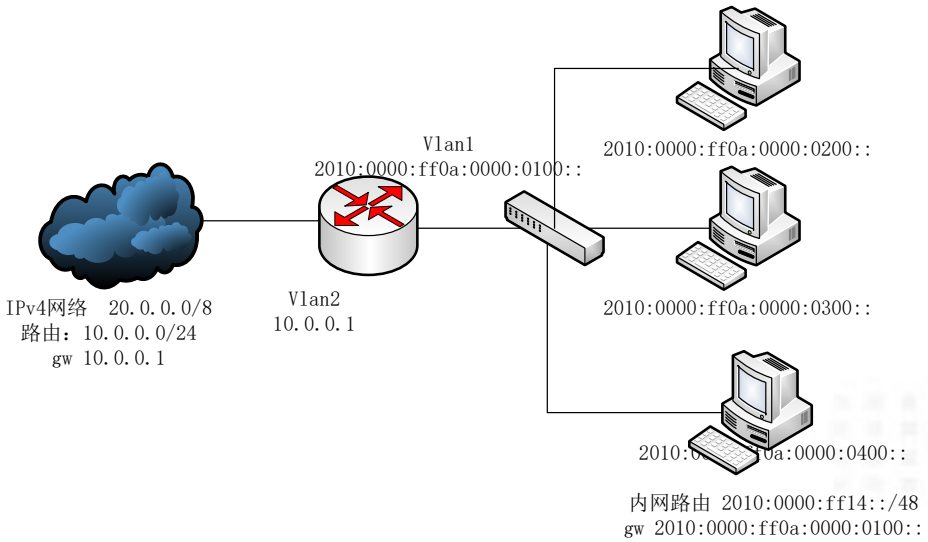
这种环境下，设备会代理 IPv6 服务器的业务，所以配置时要勾选响应 ARP，以保证 IPv4 内网向代理服务器地址 10.0.0.100 发出的请求能被发送至设备上。

24.3.2 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。下一代防火墙设备作为核心路由，串行接入设备。

配置案例组网图：

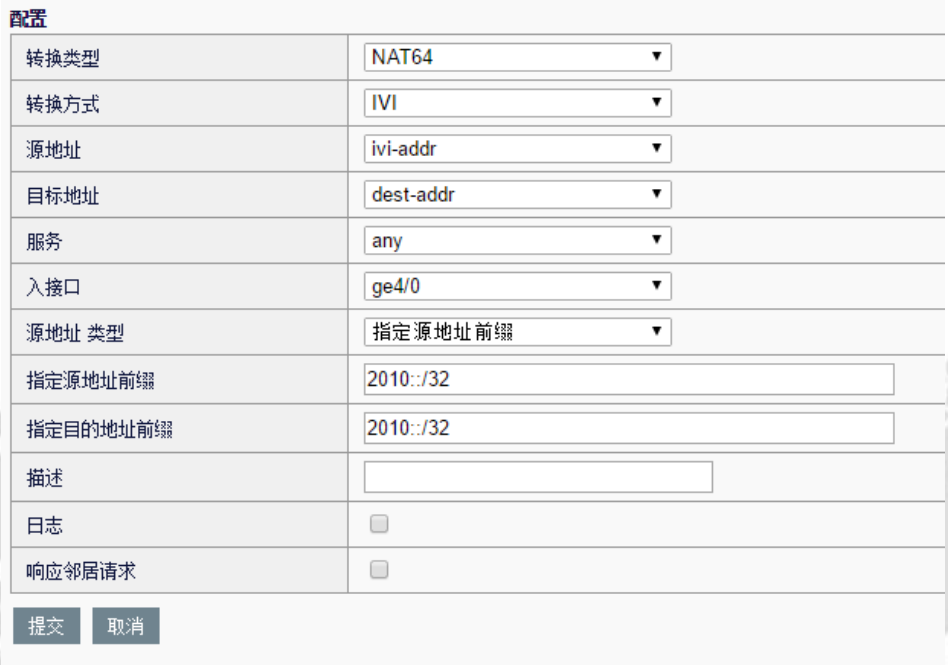


配置步骤：

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

名称	成员	引用	描述	
any	0.0.0.0/0,::/0	8		
ivi-addr	2010:0:ff00::/40	0		
dest-addr	2010:0:ff14::/48	0		

2、进入**策略>NAT 策略>跨协议转换**，配置 NAT64 转换规则。



提示：

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”。

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。

24.4 常见故障分析

24.4.1 用户发现网络中一直有地址冲突的情形

现象	用户发现 PC 一直有地址冲突的情形。
分析	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。
解决	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。

24.4.2 用户发送的请求报文无法到达设备

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	如果没有开启响应邻居/ARP 请求可能导致请求报文无法学到对应目的地址的 MAC。
解决	可查看 NAT64/NAT46 规则是否开启响应邻居/ARP 请求。

24.4.3 地址转换失败

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	如果是 NAT64 转换，可查看配置： 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。
解决	检查配置： 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

第25章 IPsec VPN

25.1 IPsec VPN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

25.2 配置IPsec VPN

25.2.1 配置 IPsec 提案

1、进入网络>IPsec-VPN>IPsec 提案，点击新建 IKE

网关名称：IKE 名称

对端网关：指定对端网关。可以有静态 IP、域名、动态三种选择。如果采用域名方式，需启用 DNS 功能并配置正确的 DNS 地址

模式：一阶段协商过程中使用的模式，分主模式和野蛮模式

认证方式：指定一阶段认证所采用的方式，有预共享秘钥和数字证书两种选择。数字证书的签发与导入请参考证书管理章节

IKE 协商交互提案：添加一阶段协商所需要的加密提案，最多可以添加 3 个

DH 组：指定 DH 交换组

NAT 穿越连接频率：即在穿越 NAT 时，NAT 会话保活报文的发送间隔

本端 ID：以 IP 地址的方式指定本端 ID，如果不填，则默认为出接口 IP

对等体状态探测：即 dpd 监测，可以开启该功能，用以探测对端的存活状况

扩展认证：开启该功能后，需要在用户管理页面添加用户，具体步骤可参考用户管理模块

模式配置：给远程接入的用户分配地址及下发 DNS、WINS 服务器。地址池以地址对象的形式设置，需提前添加地址对象

模式：野蛮模式

本地 ID 类型：分为 IP、FQDN、USER-FQDN

本地 ID：以 IP 地址的方式指定本端 ID，或字符的方式

对端 ID 类型：分为 FQDN、USER-FQDN

对端 ID：以字符的方式指定对端 ID

2、提交成功后，点击**编辑**，可以对 IKE 进行编辑

3、点击**删除**，可以删除 IKE

4、选中步骤 1 配置成功的 IKE，点击**新建 IPsec**

5、配置 IPsec 协商

通道名称：输入 IPSEC 的名称

IKE：指定一个已经存在的 IKE

IPSEC 协商交互方案：添加二阶段协商所需要的加密提案，最多可以添加 3 个

注意！如果发起端同时配置了 AH：md5-hmac 和 AH：null，此时对端不应只配置 AH：null。因为当加密方式存在时，将采取加密方式来进行协商。

完美向前保密（PFS）：指定完美向前保密组

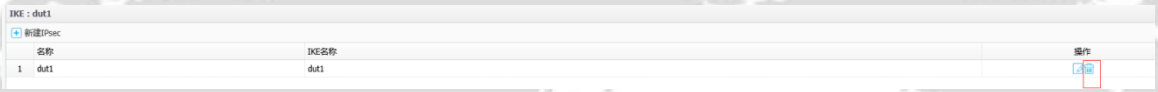
模式：IPSEC 加密的封装模式，目前只支持隧道（tunnel）模式

密钥周期：指定 IPSEC SA 最大有效时间，有时间、流量、时间+流量三种选择

自动连接：是否开启自动连接功能，如果开启此选择需同时设定一个自动重连时间间隔

6、提交成功后，点击编辑，可以对 IPsec 进行编辑

7、点击**删除**，可以删除 IPsec



25.2.2 配置 IPsec 隧道接口

1、进入**网络>IPsec-VPN>IPsec 隧道接口**，点击**新建**

IPsec 接口：IPsec 隧道接口名称

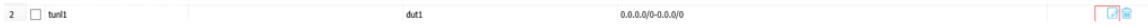
IPv4 地址：为 tunnel 接口指定一个 IPv4 地址

IPsec：指定一个已经存在的 IPSEC 协商策略

自动添加路由：是否自动生成 ipsec 的路由

地址项目：设置感兴趣流，以地址对象的形式进行配置，分源和目的。如果不配，默认为 any-any。

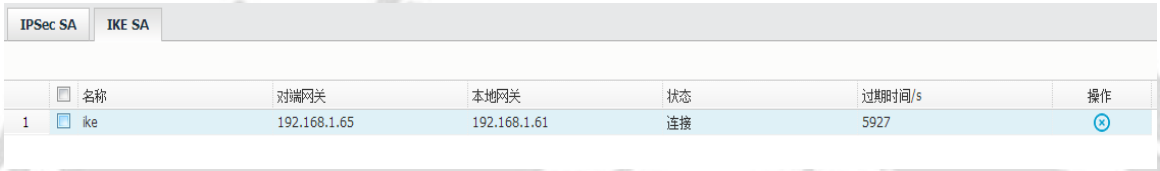
2、提交成功后，点击**编辑**



3、点击**删除**，删除 tunnel 口

25.2.3 IPsec 监控

1、进入**网络>IPsec-VPN>IPsec 监控>IKE SA**，查看 IKE SA 的建立情况



2、进入**网络>IPsec-VPN>IPsec 监控>IPsec SA**，查看 IPsec SA 的建立情况

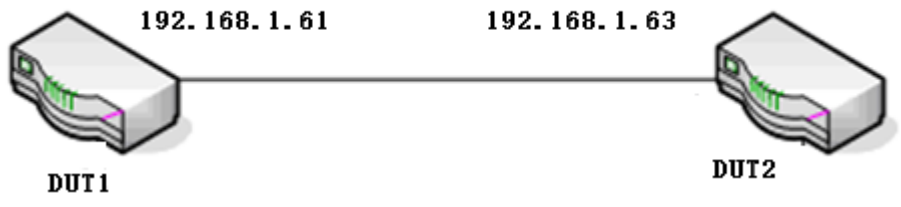
25.3 配置案例

25.3.1、案例一 配置 IPsecVPN

案例描述：

DUT1 与 DUT2 为两台具有 IPsec VPN 功能的网关。

拓扑如下：



DUT1 之后有局域网 2.2.2.0/24，DUT1 之后有局域网 1.1.1.0/24，现要通过 IPsec VPN 连通 DUT1 和 DUT2 各自的局域网。

配置步骤：

1、配置 IKE 协商策略

DUT1 设备配置信息：

DUT2 设备配置信息：

2、配置 IPsec 协商策略

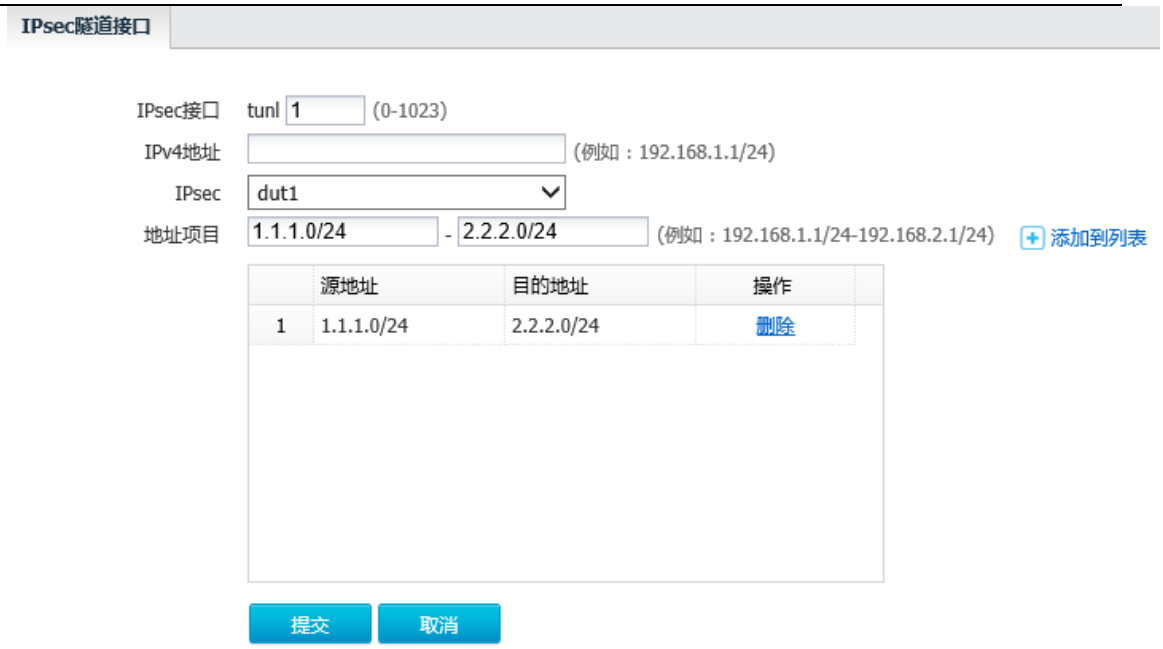
DUT1 设备配置信息：


IPSEC协商
基本设置
通道名称
dut1
(1-31 字符)
IKE
dut1
高级选项
IPSEC协商交互方案
ESP
NULL_NULL
AH
NULL
添加到列表
ESP
AH
操作
1
3DES_MD5
NULL
删除
完美向前保密(PFS)
无
1
2
5
模式
隧道模式
密钥周期
秒
千字节
两者都有
秒
86400
(120-86400 秒)
自动连接
时间
2
(2-3600 秒)
提交
取消

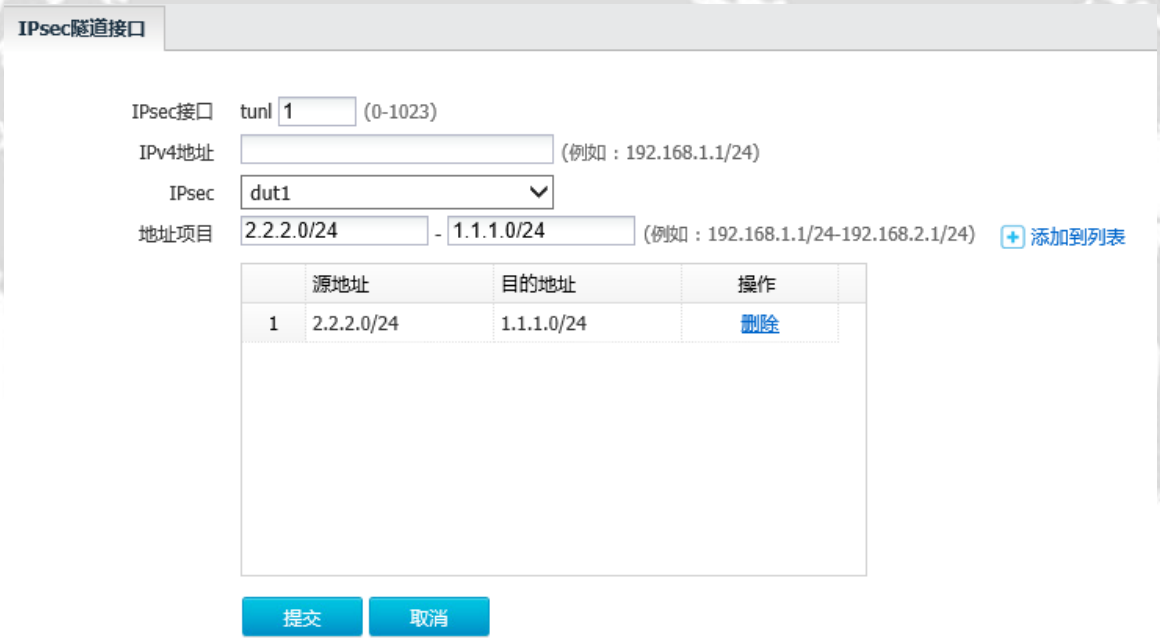
DUT2 设备配置信息：

3、配置 IPsec 隧道接口

DUT1 设备配置信息：

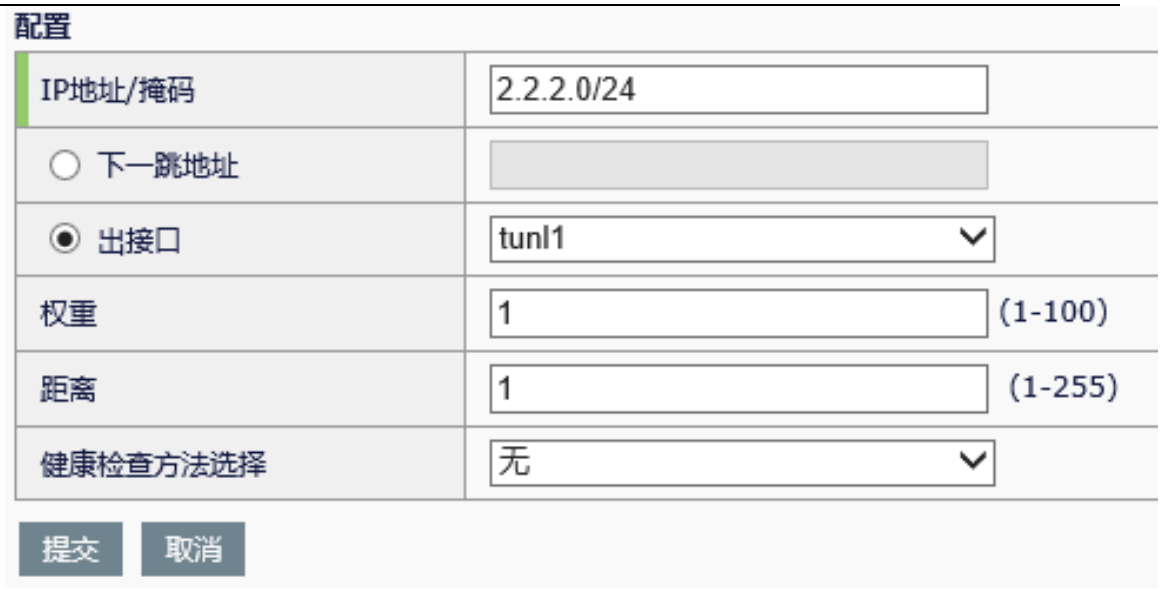


DUT2 设备配置信息：

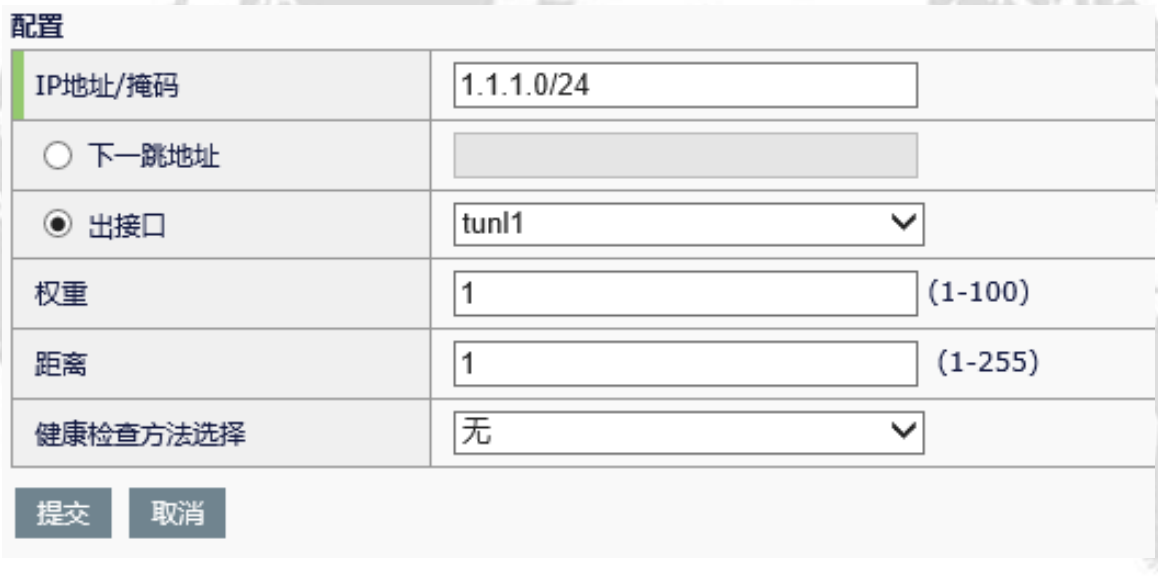


4、配置静态路由，需要将感兴趣流的路由指向 tunnel 口

DUT1 设备配置信息：



DUT2 设备配置信息：

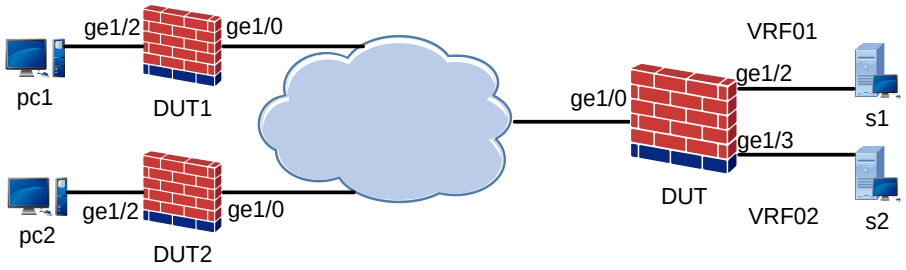


25.3.2、案例二 IPsec 多实例主模式

案例描述：

采用主模式实现 IPsec 多实例。

拓扑如下：



DUT1、DUT2 属于公网端两个分支机构，pc1,pc2 分别是两个分支机构下的 pc 客户端

DUT1:ge1/2 地址 15.0.0.1/24　ge1/0 地址 12.0.0.201/24 pc1 地址 15.0.0.10/24 gw 15.0.0.1

DUT2:ge1/2 地址 15.0.0.1/24　ge1/0 地址 12.0.0.17/24 pc2 地址 15.0.0.10/24 gw 15.0.0.1

DUT 为总部机构、公网口 ge1/0 提供 ipsec 服务。VRF01 ge1/2 端服务器 s1 给 pc1 提供服务、VRF02 ge1/3 服务器 s2 给 pc2 提供服务

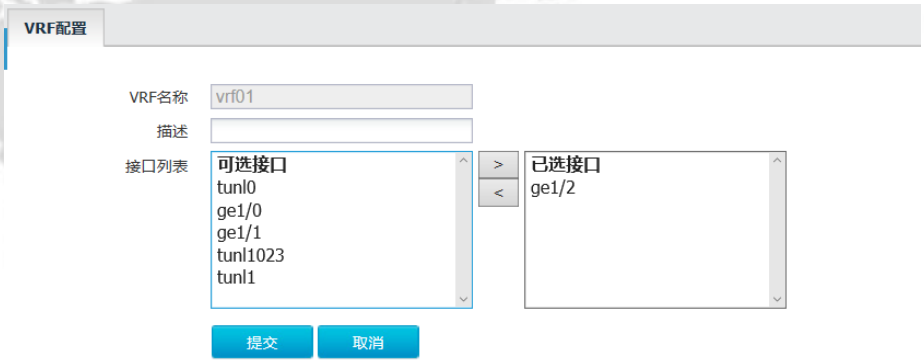
DUT: ge1/0 配置地址 41.0.0.2/24 （VRF01 ipsec 本端公网地址)、41.0.0.3/24（VRF02 ipsec 本端公网地址)，ge1/2 地址 31.0.0.1/24,ge1/3 地址 31.0.0.1/24，分别属于 VRF01 和 VRF02

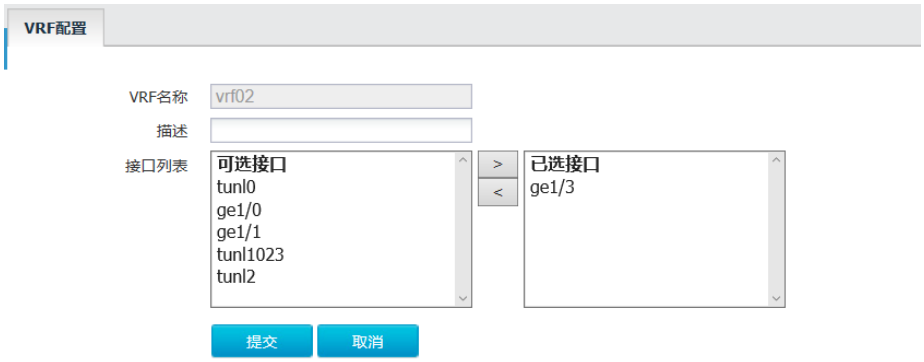
s1 地址 31.0.0.10/24 gw 31.0.0.1

s2 地址 31.0.0.10/24 gw 31.0.0.1

配置步骤：

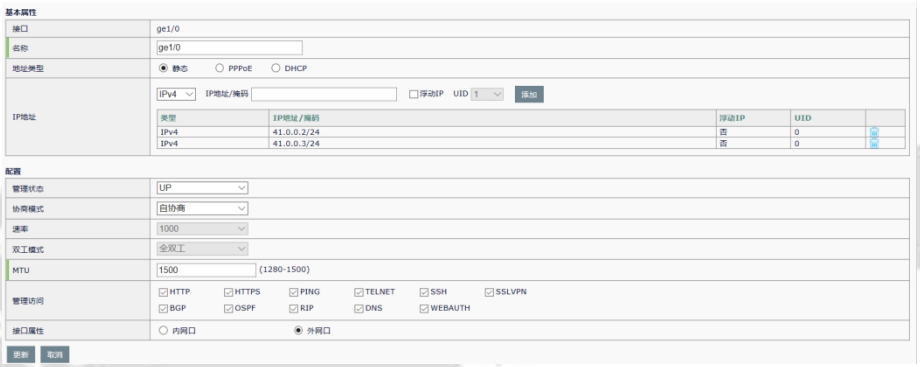
1、DUT：进入**网络>系统>VRF> VRF 配置**，将 ge1/2 加入到 VRF01，ge1/3 加入到 VRF02，分别提交下发配置

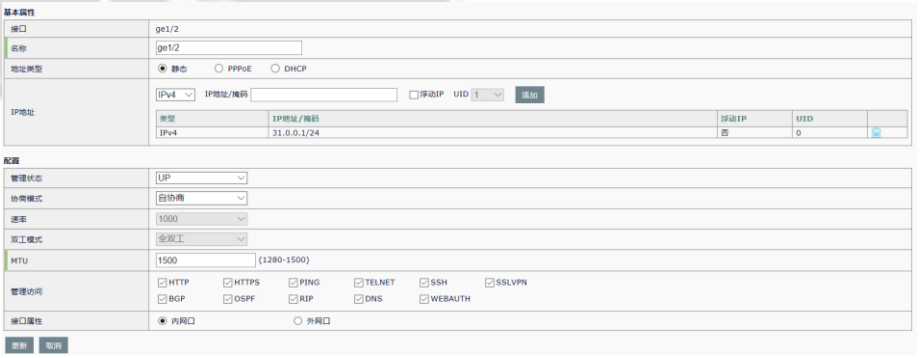


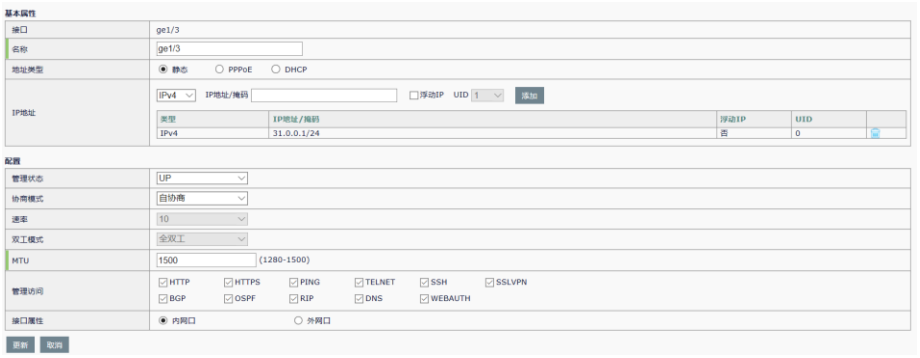


2、进入**策略>防火墙策略>访问控制**，点击**新建**配置 VRF0，VRF01.VRF02 防火墙全通策略

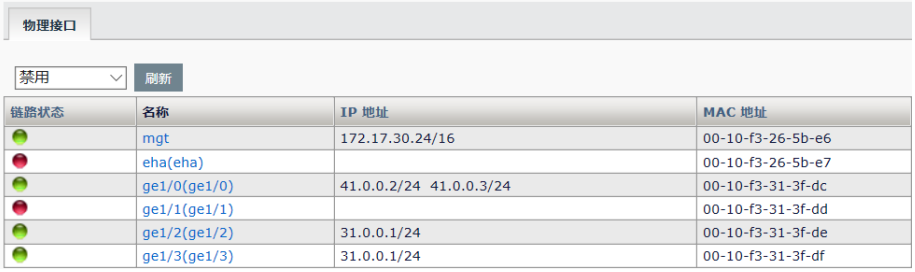
3、进入**网络>接口>物理接口**，点击**接口。**配置 VRF0、VRF01、VRF02 接口地址







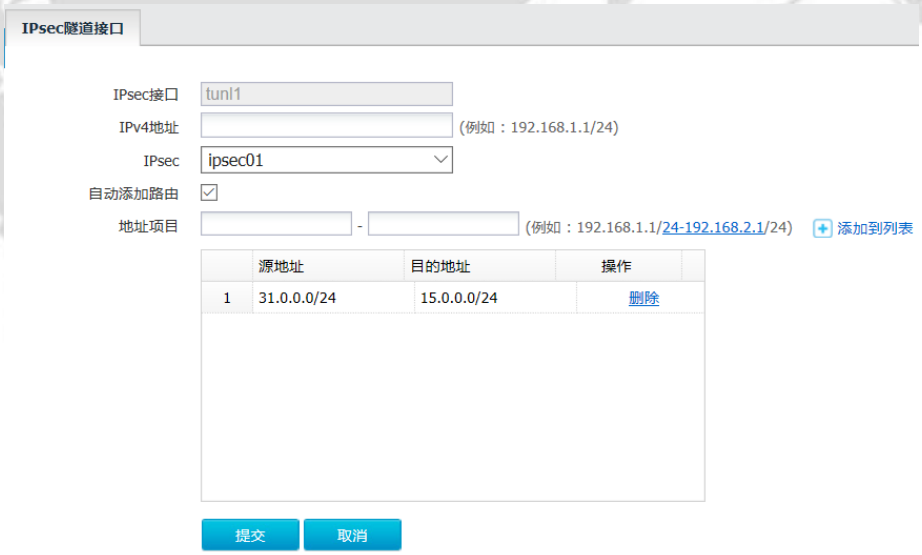
下发配置



4、进入**网络>ipsec-vpn> ipsec 提案**,点击**新建 ike 策略配置 ike 策略关联 VRF01** 和 ipsec 本端公网地址 41.0.0.2

点击**新建 ipsec 策略配置 ipsec 策略**

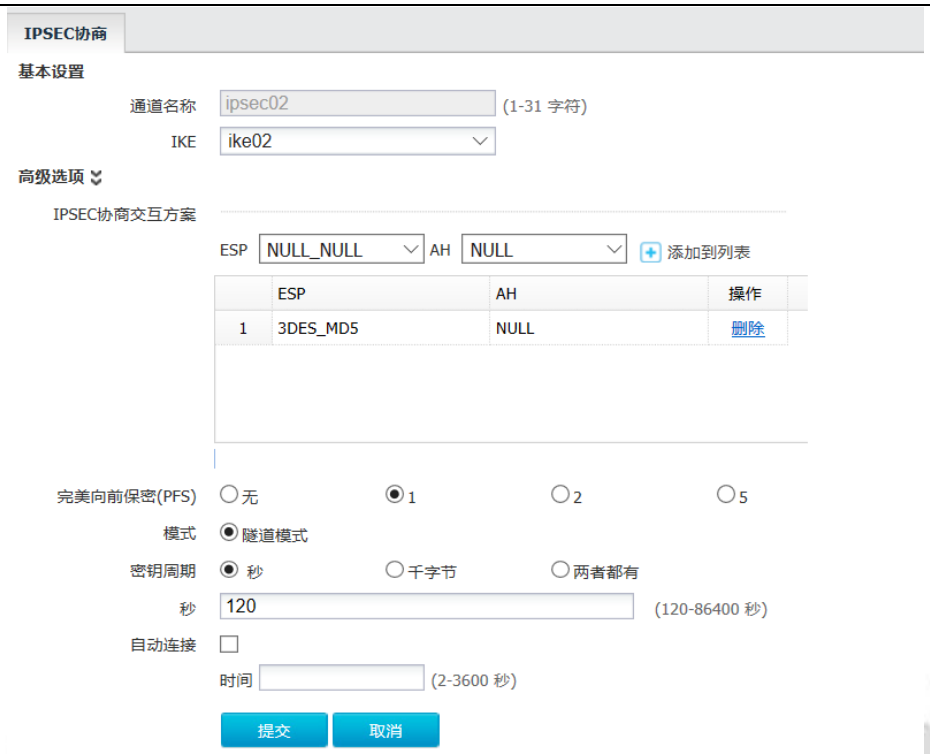
点击**新建 ipsec 隧道接口配置 ipsec 隧道接口**



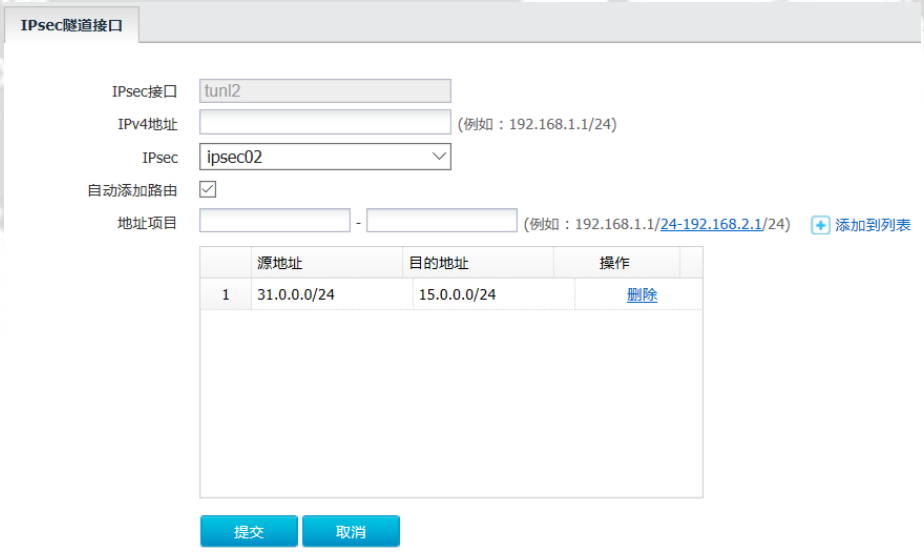
5、进入**网络>ipsec-vpn> ipsec 提案**，点击**新建 ike 策略配置 ike 策略关联 VRF02** 和 ipsec

本端公网地址 41.0.0.3

点击**新建 ipsec 策略配置 ipsec 策略**



点击**新建 ipsec 隧道接口配置 ipsec 隧道接口**

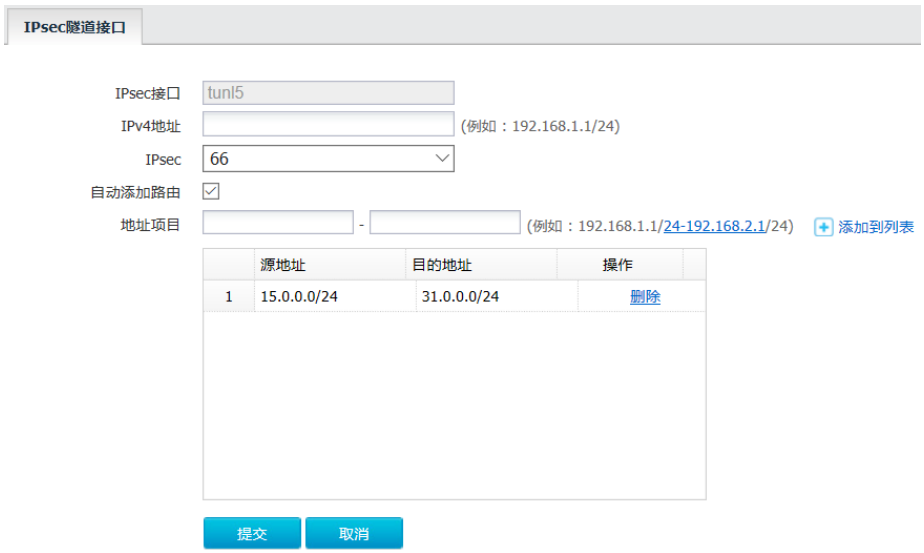


查看 VRF 配置

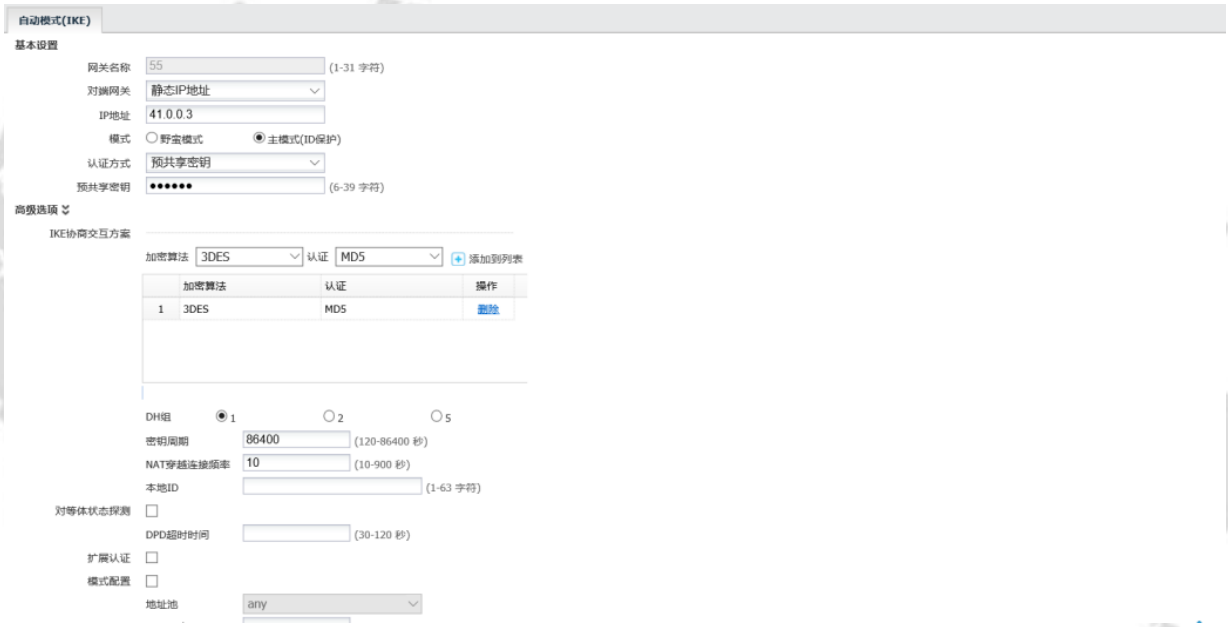
6、确保分支机构 DUT1、DUT2 和 DUT 路由可达。并配置分支机构 ipsec 配置

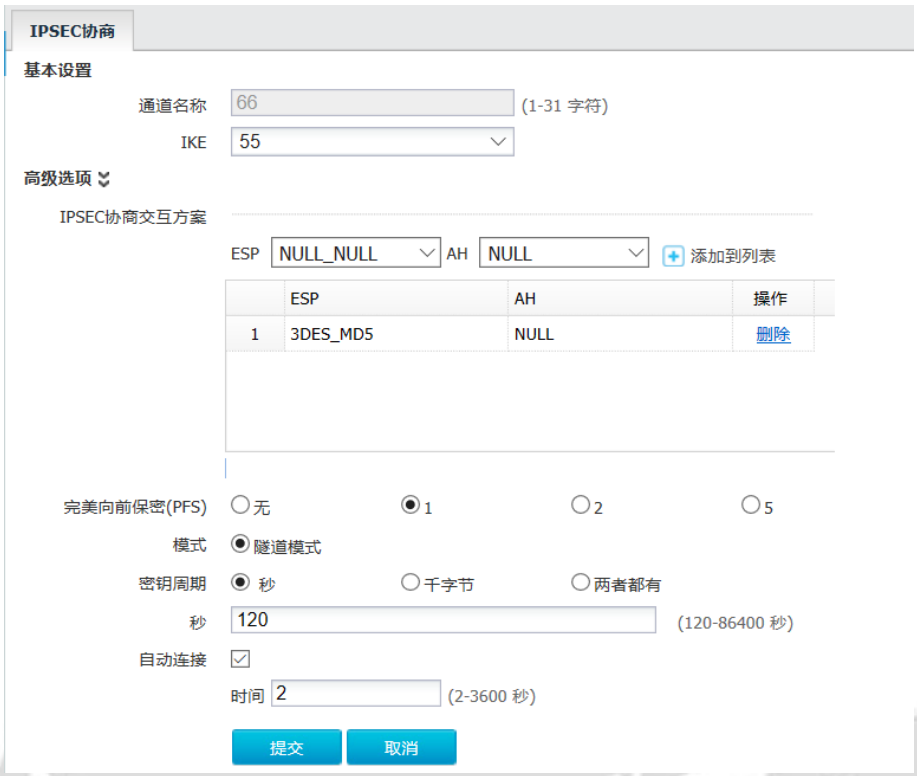
DUT1 Ipsec 配置

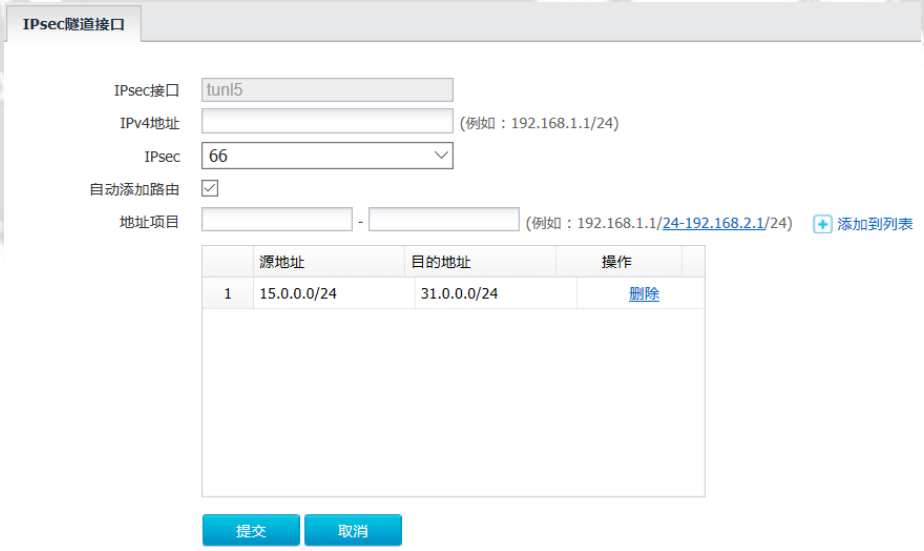

自动模式(IKE)
基本设置
网关名称
55
(1-31 字符)
对端网关
静态IP地址
IP地址
41.0.0.2
模式
野蛮模式
主模式(ID保护)
认证方式
预共享密钥
预共享密钥
(6-39 字符)
高级选项
IKE协商交互方案
加密算法
3DES
认证
MD5
添加到列表
加密算法
认证
操作
1
3DES
MD5
删除
DH组
1
2
5
密钥周期
86400
(120-86400 秒)
NAT穿越连接频率
10
(10-900 秒)
本地ID
(1-63 字符)
对等体状态探测
DPD超时时间
(30-120 秒)
扩展认证
模式配置
地址池
any
拨号用户DNS
IPSEC协商
基本设置
通道名称
66
(1-31 字符)
IKE
55
高级选项
IPSEC协商交互方案
ESP
NULL_NULL
AH
NULL
添加到列表
ESP
AH
操作
1
3DES_MD5
NULL
删除
完美向前保密(PFS)
无
1
2
5
模式
隧道模式
密钥周期
秒
千字节
两者都有
秒
120
(120-86400 秒)
自动连接
时间
2
(2-3600 秒)
提交
取消



DUT2 Ipsec 配置

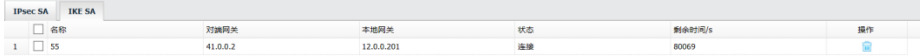




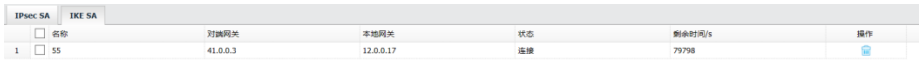


7、DUT：查看 ipsec 监控协商结果

8、DUT1：查看 ipsec 监控协商结果

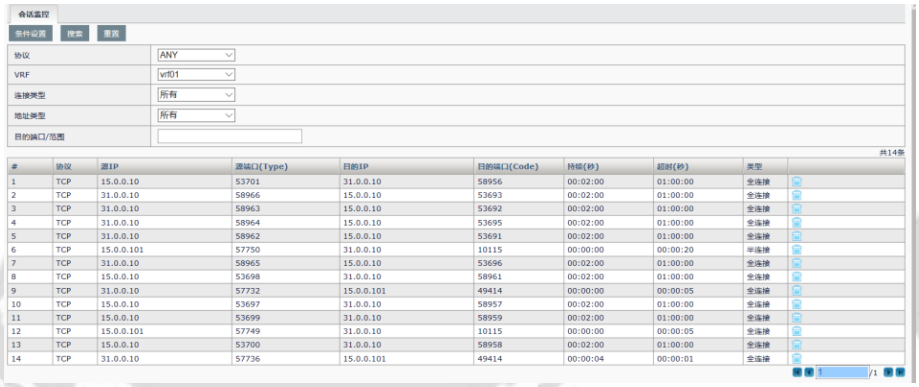


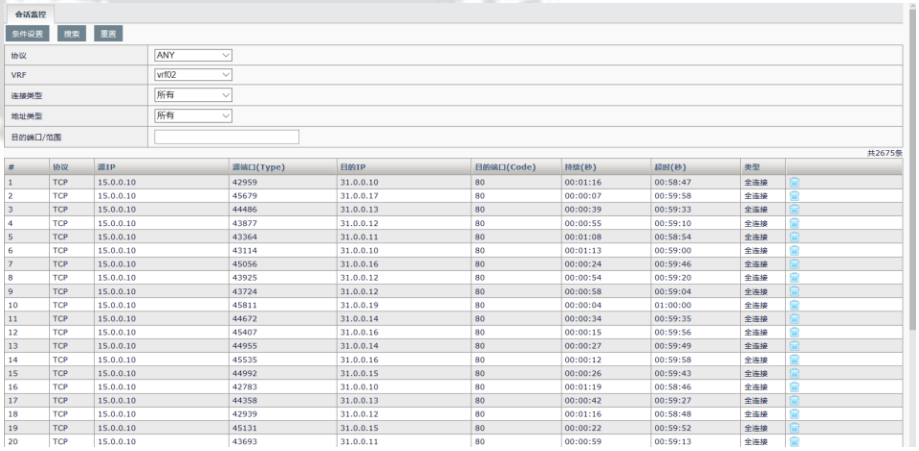
9、DUT2：查看 ipsec 监控协商结果



10、DUT:分支客户端 pc1 向 s1 发起 tcp 请求、分支 pc2 向 s2 发起 http 请求

查看 VRF01 和 VRF02 会话



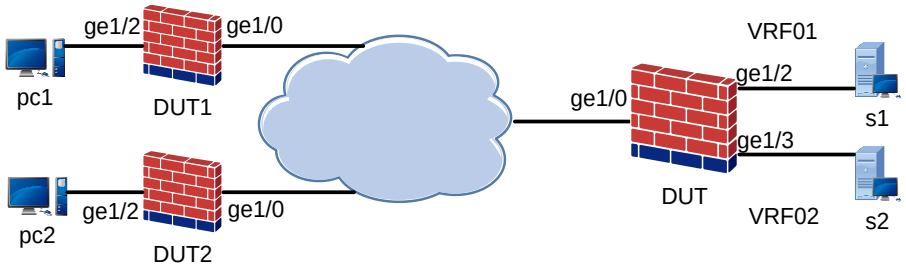


25.3.3、案例三 IPsec 多实例野蛮模式

案例描述：

采用 FQDN 模式实现 IPsec 多实例。

拓扑如下：



DUT1、DUT2 属于公网端两个分支机构，pc1,pc2 分别是两个分支机构下的 pc 客户端

DUT1:ge1/2 地址 15.0.0.1/24　ge1/0 地址 12.0.0.201/24 pc1 地址 15.0.0.10/24 gw 15.0.0.1 USER-FQDN 本端 ID 配置 01@01test.com 对端 ID 配置 test@01test.com

DUT2:ge1/2 地址 15.0.0.1/24　ge1/0 地址 12.0.0.17/24 pc2 地址 15.0.0.10/24 gw 15.0.0.1 USER-FQDN 本端 ID 配置 02@02test.com 对端 ID 配置 test@02test.com

DUT 为总部机构、公网口 ge1/0 提供 ipsec 服务。

VRF01 ge1/2 端服务器 s1 给 pc1 提供服务、策略 ike01：USER-FQDN ID 本端配置 test@01test.com 对端配置@01test.com 勾选通配符；

VRF02 ge1/3 服务器 s2 给 pc2 提供服务、策略 ike02 USER-FQDN ID 本端配置 test@02test.com、对端配置@02test.com 勾选通配符

DUT: ge1/0 配置地址 41.0.0.2/24，ge1/2 地址 31.0.0.1/24,ge1/3 地址 31.0.0.1/24，分别属于 VRF01 和 VRF02

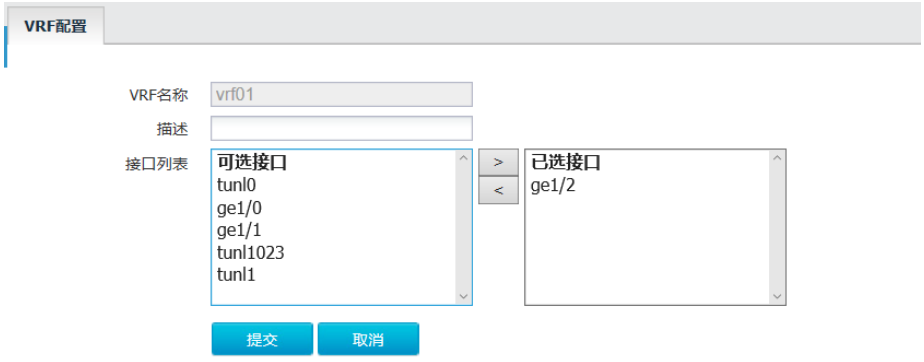
s1 地址 31.0.0.10/24 gw 31.0.0.1

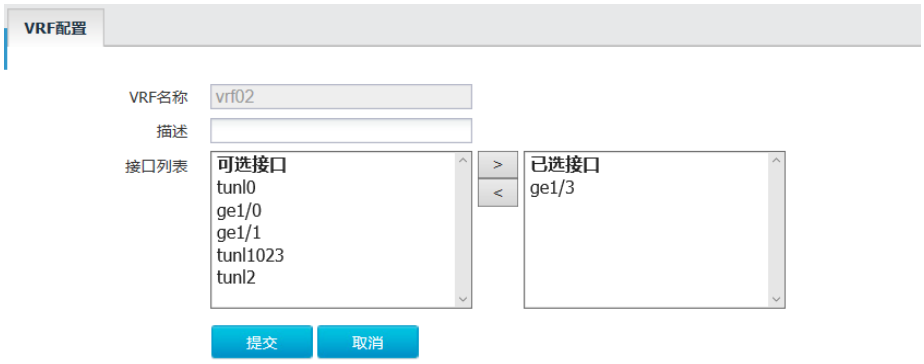
s2 地址 31.0.0.10/24 gw 31.0.0.1

配置步骤：

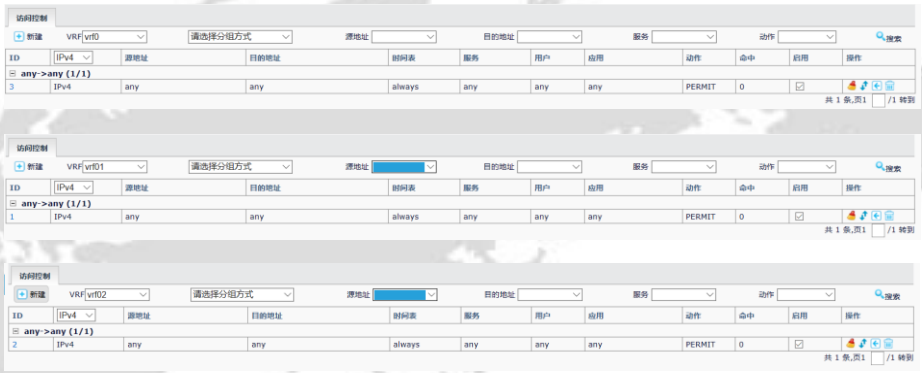
1、DUT:进入**网络>系统>VRF> VRF 配置**,将 ge1/2 加入到 VRF01,ge1/3 加入到 VRF02,

分别提交下发配置

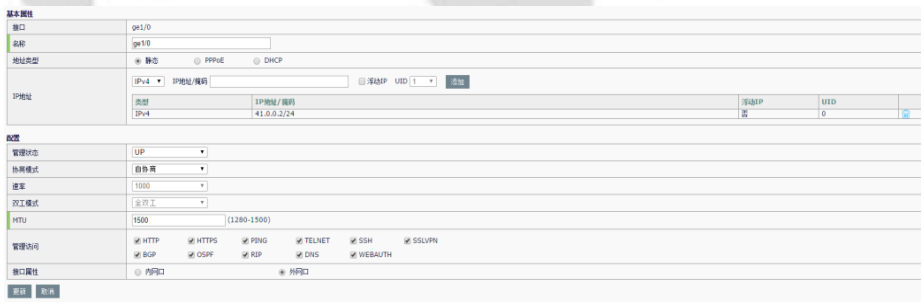


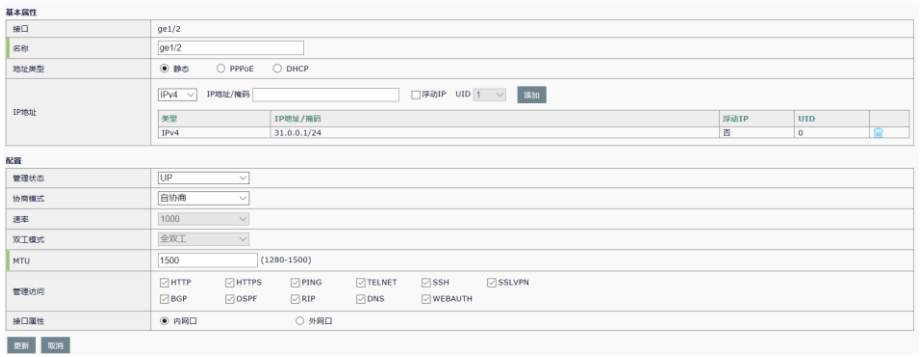


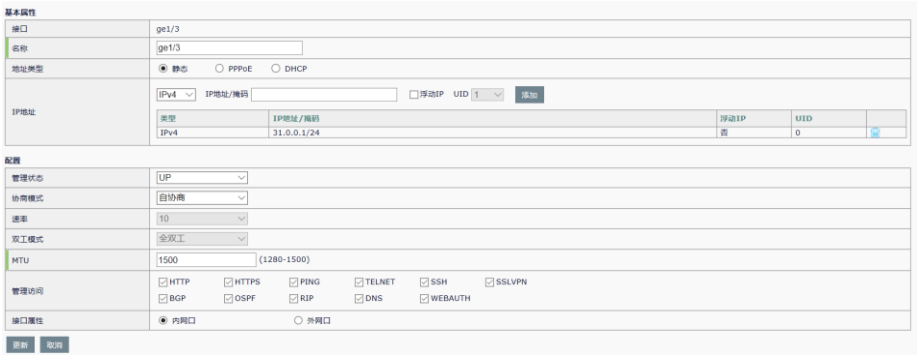
2、进入**策略>防火墙策略>访问控制**，点击**新建**配置 VRF0，VRF01.VRF02 防火墙全通策略



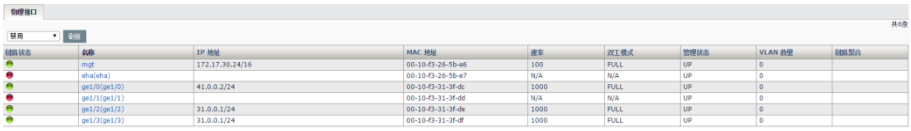
3、进入**网络>接口>物理接口**，点击**接口。**配置 VRF0、VRF01、VRF02 接口地址





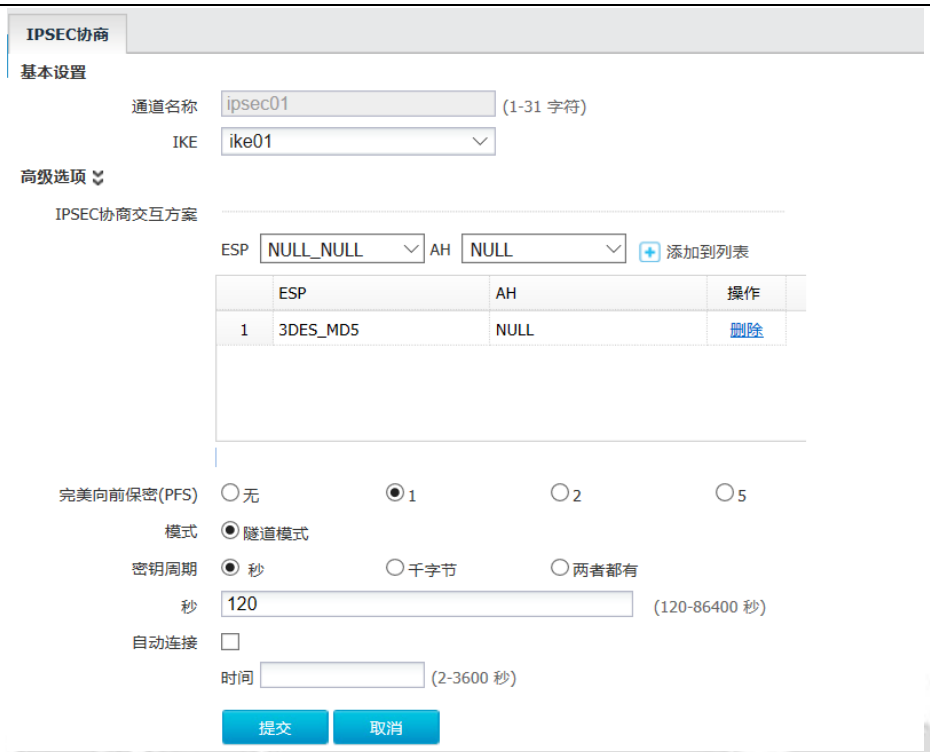


下发配置

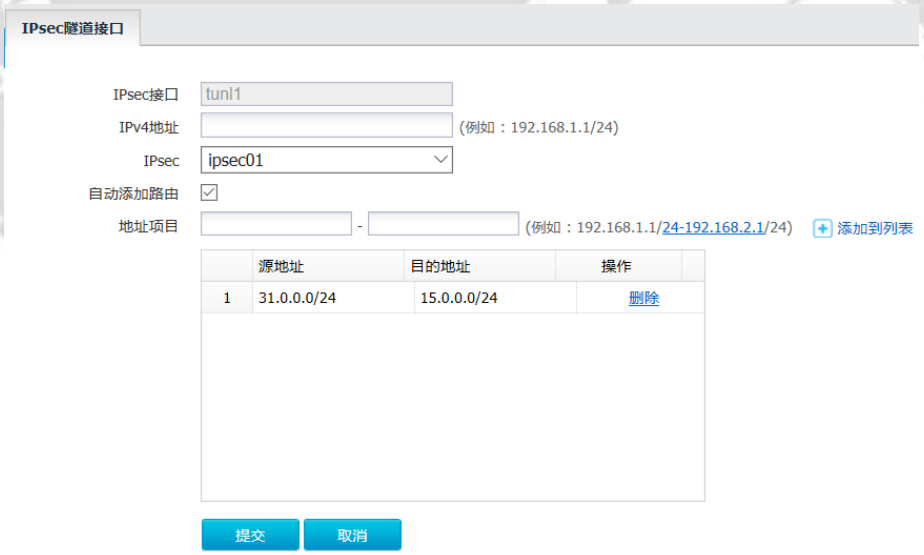


4、进入**网络>ipsec-vpn> ipsec 提案**，点击**新建 ike 策略配置 ike 策略关联 VRF01**

点击**新建 ipsec 策略配置 ipsec 策略**

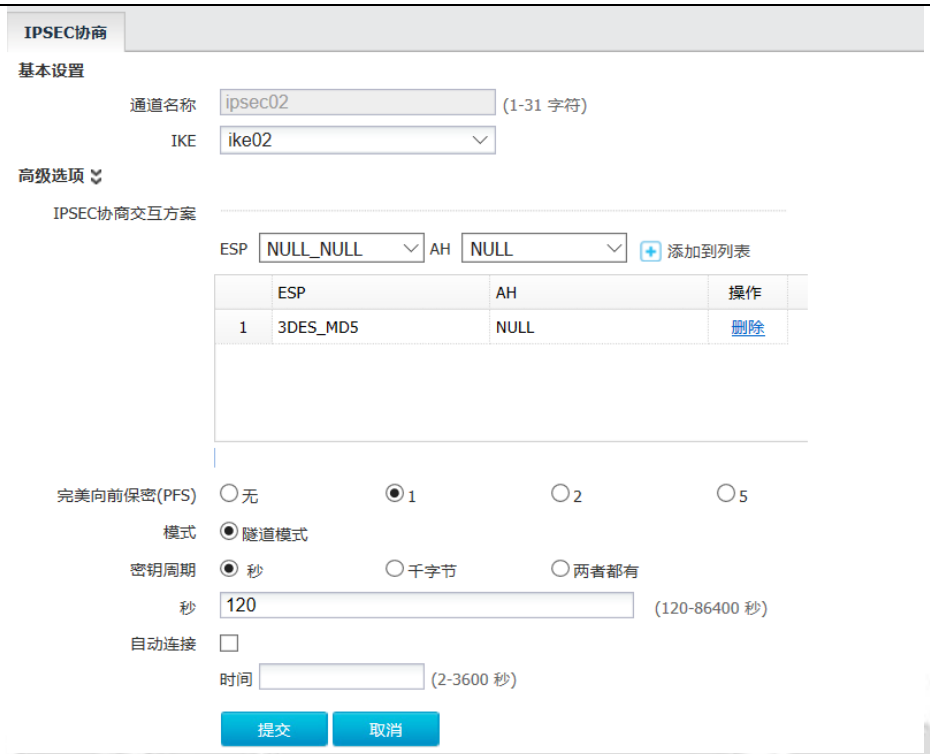


点击**新建 ipsec 隧道接口配置 ipsec 隧道接口**

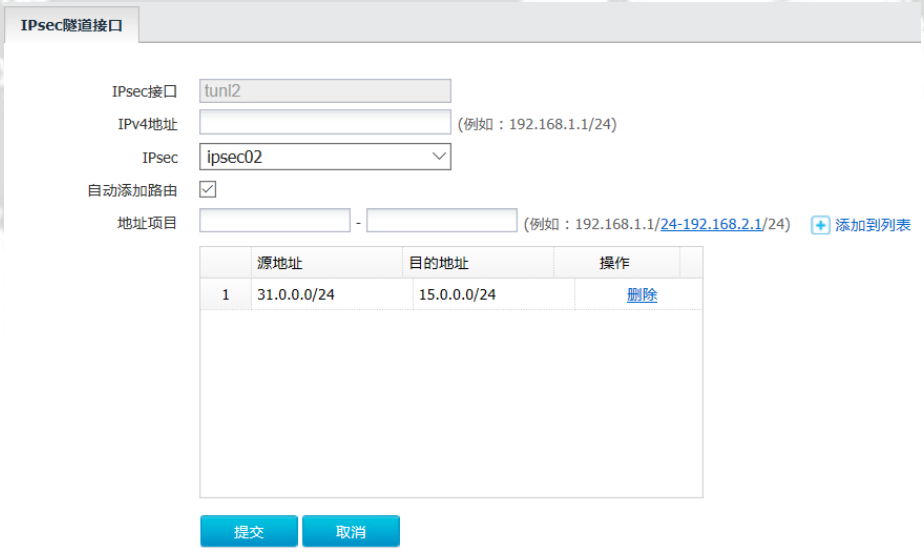


5、进入**网络>ipsec-vpn> ipsec 提案**，点击**新建 ike 策略配置 ike 策略关联 VRF02，**，

点击**新建 ipsec 策略配置 ipsec 策略**



点击**新建 ipsec 隧道接口配置 ipsec 隧道接口**

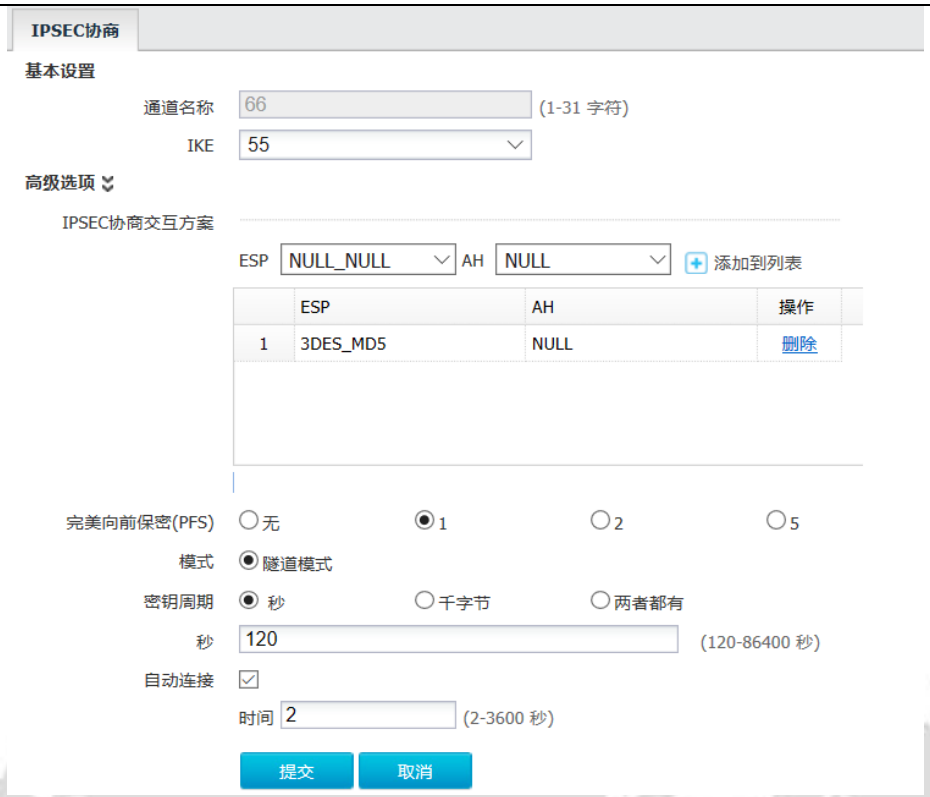


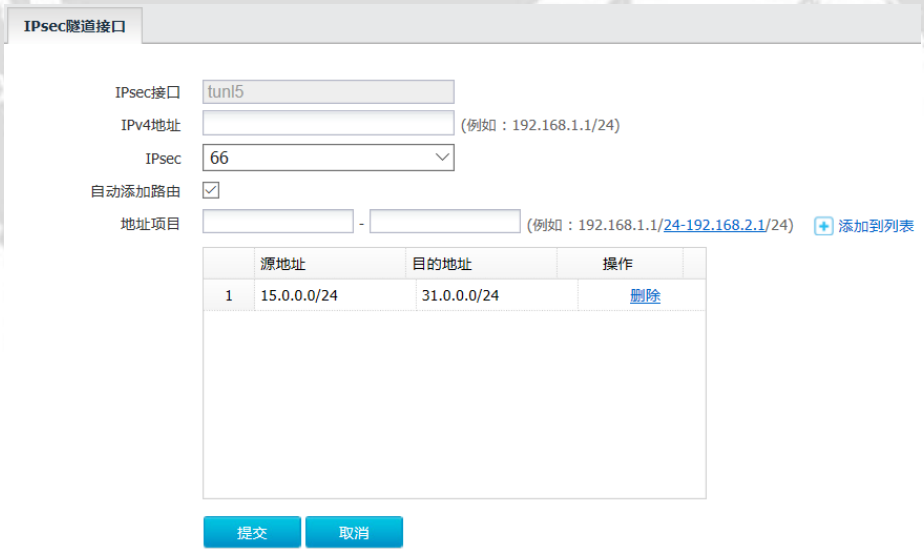
查看 VRF 配置

6、确保分支机构 DUT1、DUT2 和 DUT 路由可达。并配置分支机构 ipsec 配置

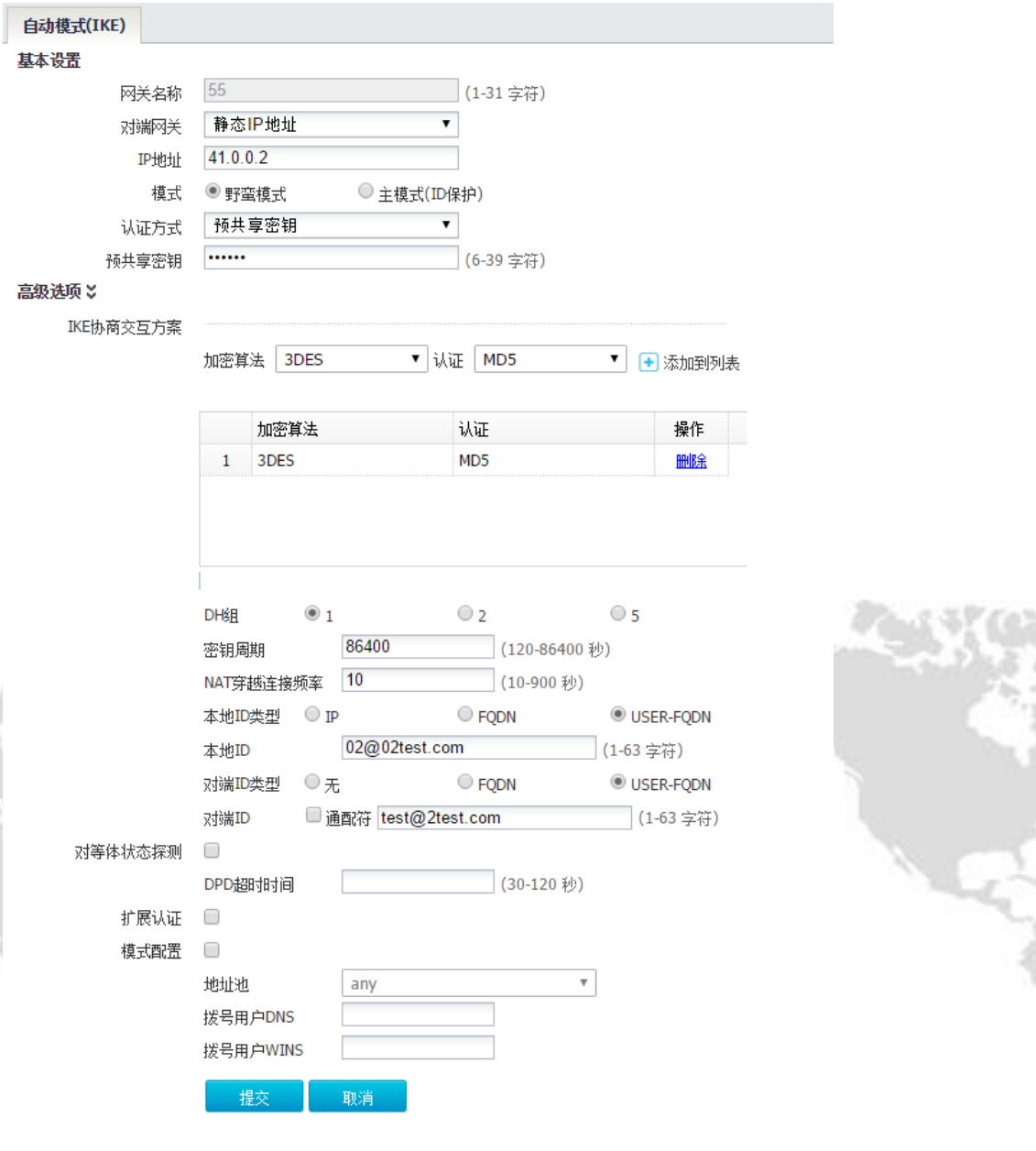
DUT1 Ipsec 配置

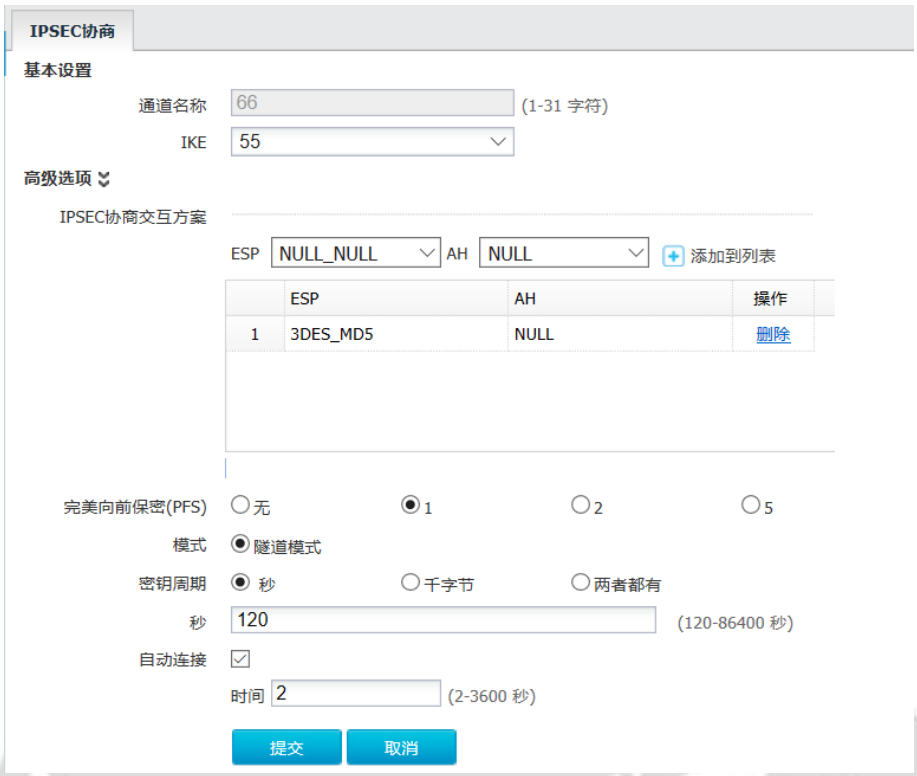

自动模式(IKE)
基本设置
网关名称
55
(1-31 字符)
对端网关
静态IP地址
IP地址
41.0.0.2
模式
野蛮模式
主模式(ID保护)
认证方式
预共享密钥
预共享密钥
(6-39 字符)
高级选项
IKE协商交互方案
加密算法
3DES
认证
MD5
添加到列表
加密算法
认证
操作
1
3DES
MD5
删除
DH组
1
2
5
密钥周期
86400
(120-86400 秒)
NAT穿越连接频率
10
(10-900 秒)
本地ID类型
IP
FQDN
USER-FQDN
本地ID
01@01test.com
(1-63 字符)
对端ID类型
无
FQDN
USER-FQDN
对端ID
通配符
test@1test.com
(1-63 字符)
对等体状态探测
DPD超时时间
(30-120 秒)
扩展认证
模式配置
地址池
any
拨号用户DNS
拨号用户WINS
提交
取消

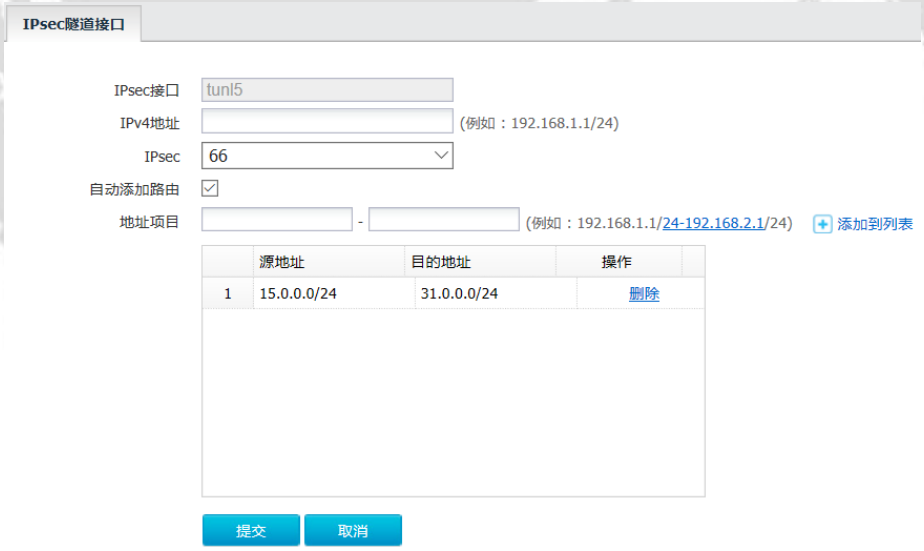




DUT2 Ipsec 配置


自动模式(IKE)
基本设置
网关名称
55
(1-31 字符)
对端网关
静态IP地址
IP地址
41.0.0.2
模式
野蛮模式
主模式(ID保护)
认证方式
预共享密钥
预共享密钥
(6-39 字符)
高级选项
IKE协商交互方案
加密算法
3DES
认证
MD5
添加到列表
加密算法
认证
操作
1
3DES
MD5
删除
DH组
1
2
5
密钥周期
86400
(120-86400 秒)
NAT穿越连接频率
10
(10-900 秒)
本地ID类型
IP
FQDN
USER-FQDN
本地ID
02@02test.com
(1-63 字符)
对端ID类型
无
FQDN
USER-FQDN
对端ID
通配符
test@2test.com
(1-63 字符)
对等体状态探测
DPD超时时间
(30-120 秒)
扩展认证
模式配置
地址池
any
拨号用户DNS
拨号用户WINS
提交
取消





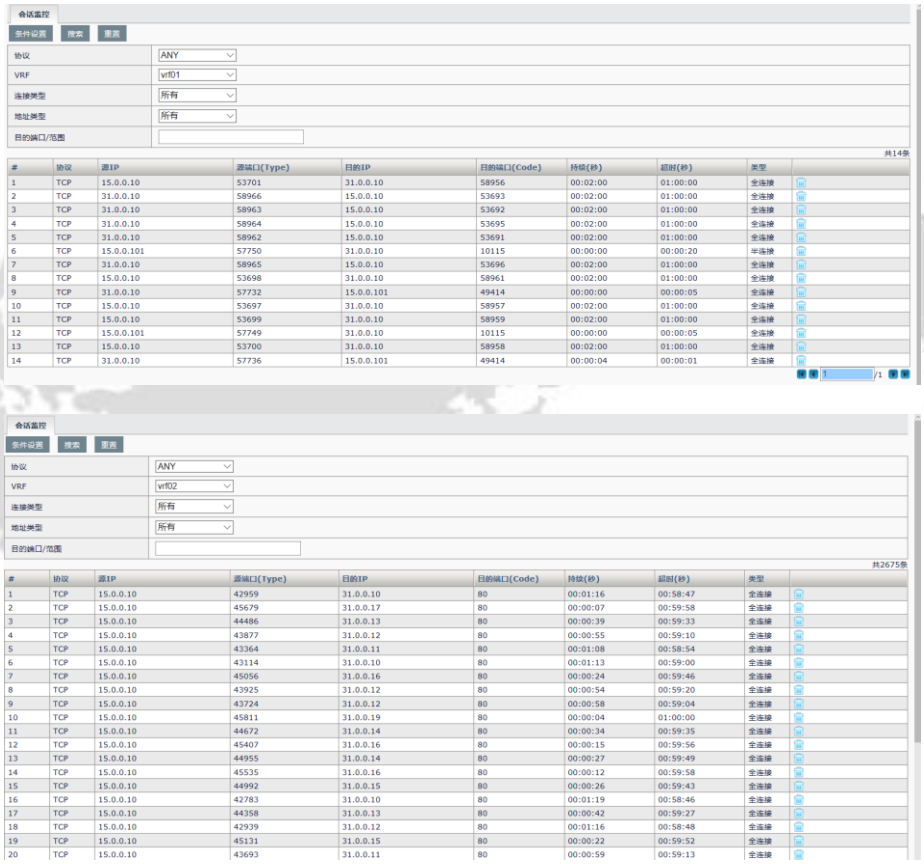
7、DUT：查看 ipsec 监控协商结果

8、DUT1：查看 ipsec 监控协商结果

9、DUT2：查看 ipsec 监控协商结果

10、DUT:分支客户端 pc1 向 s1 发起 tcp 请求、分支 pc2 向 s2 发起 http 请求

查看 VRF01 和 VRF02 会话



第26章 端口管理

26.1 端口管理概述

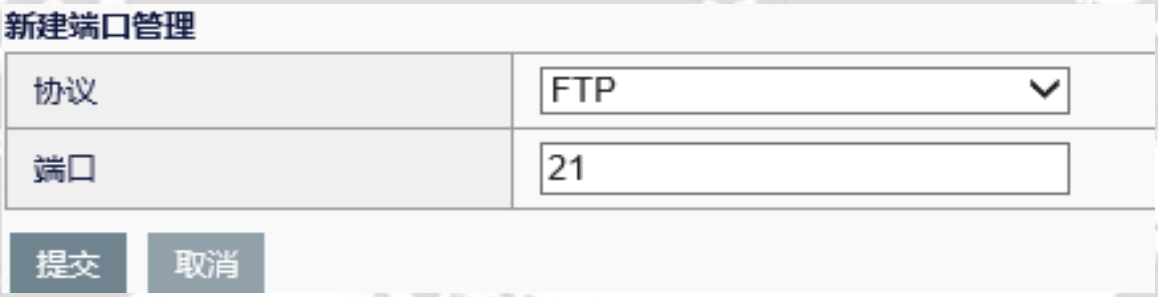
针对服务器有时会改变或者添加所提供服务对应的监听端口号的情况，下一代防火墙设备需要改变或添加预置的 ALG 端口号，使设备能正确识别报文中端口号所对应的服务类型。

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。

26.2 端口配置

26.2.1 设置 ALG 端口号

1、进入**策略>NAT 策略>端口管理**，点击“**新建**”按钮。如下图：



协议：ALG 协议类型，目前仅支持 FTP 和 TFTP。

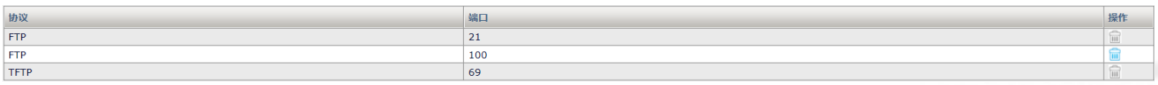
端口：要添加的 ALG 协议的监听端口号。

提示：

每个协议，除了默认端口，最多可以添加 7 个端口号。

26.2.2 删除 ALG 端口号

1、进入**网络配置>NAT>端口管理**。



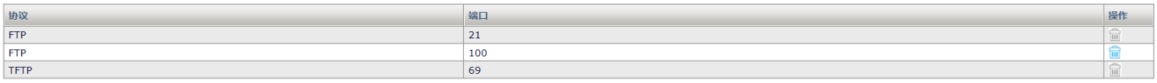
点击最后一列的图标，即可删除配置的端口号。

提示：

协议对应的默认端口号无法改变或删除。

26.2.3 查看 ALG 端口号

1、进入**策略>NAT 策略>端口管理，**可查看到配置的所有端口号。



26.3 配置案例

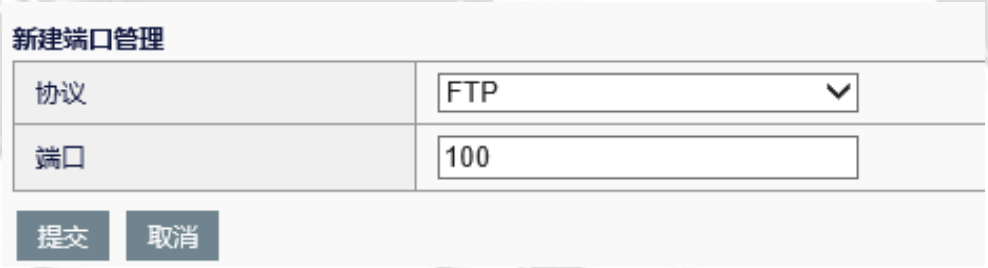
配置案例 1

案例描述：

添加一个 FTP 协议的监听端口号 100。

配置步骤：

1、 进入**网络配置>NAT>端口管理**，点击“**新建**”按钮。如下图：



2、点击“**提交**”提交配置。

提示：

不同的协议添加的 ALG 端口可以相同。

第27章 安全策略

27.1 安全策略概述

为了对数据流进行统一控制，方便用户配置和管理，下一代防火墙设备引入了安全策略的概念。

通过配置安全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，把该报文的方向、源地址、目的地址、协议、端口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。

同时，在安全策略中还可以根据匹配结果，对符合规则的报文实行策略引用的安全防护表中设置的安全检查。在没有配置任何安全策略的情况下，对于经过设备的所有数据包，其缺省为不开启策略匹配，且状态为 PERMIT。

安全策略按在 IPv4 或 IPv6 的相同入、出接口时从上往下的原则，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。

27.2 配置安全策略

27.2.1 配置策略的基本要素

安全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>访问控制**，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。

出接口：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。

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：数据流中源 IP 地址所对应用户。any 表示用户为任意。

应用：数据流中匹配的应用，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。

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。

源主机连接控制：对匹配该条策略的流，根据源地址连接数进行限制。

源主机连接速率限制：对匹配该策略的流，根据源地址连接速率进行限制。

流量统计：统计匹配该策略的流量，可在系统信息>会话监控>流量统计>基于策略中进行查看。

流量镜像：将匹配到该策略的流量镜像到相应接口。

描述：安全策略的描述，长度限制为 127 个字符。

2、配置完毕后，点击**提交**。

注意：

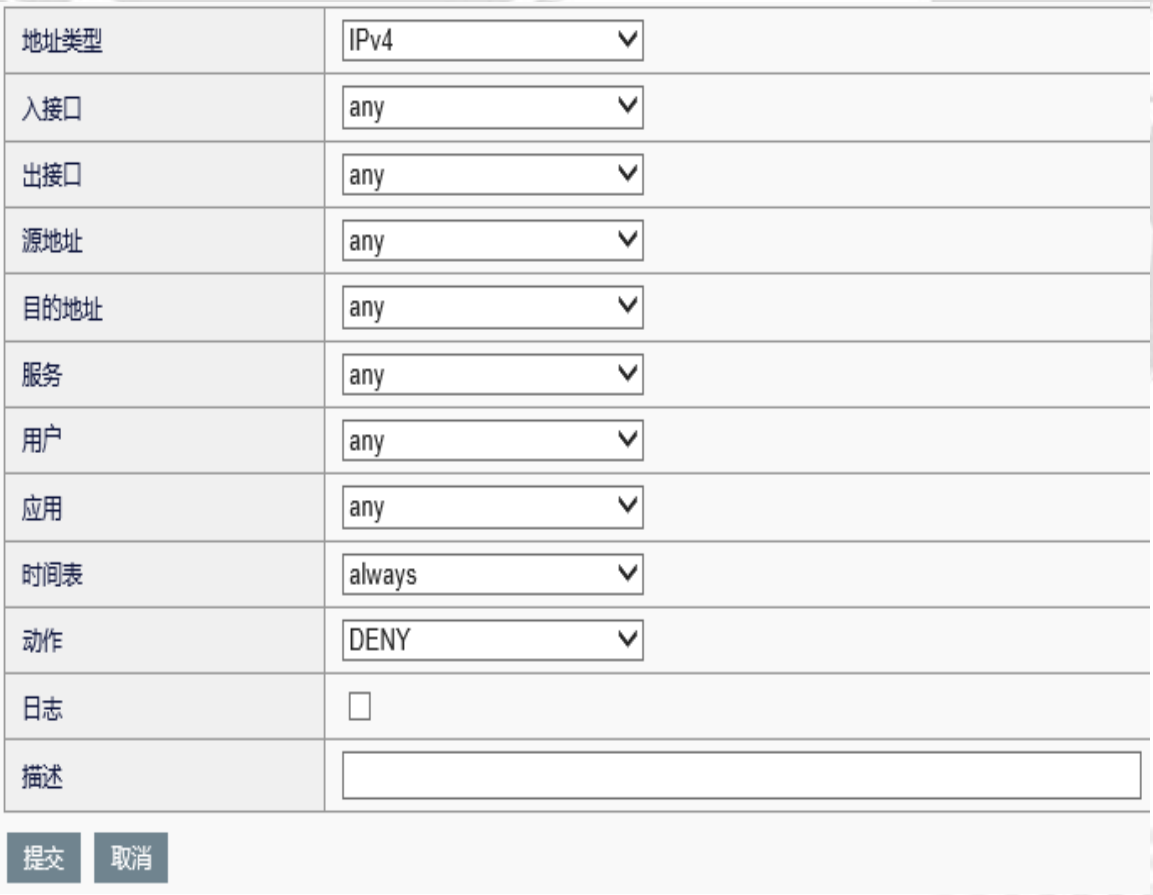
创建一条新的安全策略时，必须引用相同协议类型的地址对象；系统会自动生成该策略的 ID 号，策略 ID 是安全策略的唯一标识。不同协议类型的安全策略的 ID 是相互独立的。

27.2.2 配置 DENY 策略

动作为 DENY 的安全策略中，可以启用 syslog 功能。

配置步骤：

1、进入**策略>防火墙策略>访问控制**，点击**新建**，在动作下拉框中选择 DENY。



syslog 日志：选中此复选框启用 syslog 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，日志的优先级为信息级别。

2、点击**提交**。

27.2.3 配置 PERMIT 策略

动作为 PERMIT 的安全策略中。

配置步骤：

1、进入**策略>防火墙策略>访问控制**，点击**新建**，在动作下拉框中选择 PERMIT。

源主机连接控制：对匹配该条策略的流，根据源地址连接数进行限制，当某个源地址的连接数达到配置阈值时，同主机发起的数据该流会被阻断。配置范围为 0 至 10000000，为 0 时表示无限制。

源主机连接速率限制：对匹配该策略的流，根据源地址连接速率进行限制，当某个源地址连接速率达到阈值时，使用该源地址的数据流会被阻断。配置范围为 0-10000000，为 0 时表示无限制。

流量统计：统计匹配该策略的流量，可在**统计>会话信息监控>会话监控**中进行查看。

注意：

策略缺省为启用。

27.2.4 禁用安全策略

配置步骤：

1、进入**策略>防火墙策略>访问控制**，如下图：

2、取消勾选**启用**可以禁用一条策略。

27.2.5 编辑安全策略

配置步骤：

1、进入**策略>防火墙策略>访问控制**，对某条存在的安全策略点击策略 ID 号进入编辑界面

2、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**。

地址类型	IPv4
入接口	any
出接口	any
源地址	any
目的地址	any
服务	any
用户	所有用户
应用	any
时间表	always
动作	PERMIT
日志	
源主机连接限制	0 (0-10000000)
源主机连接速率限制	0 (0-10000000)/秒
流量统计	
流量镜像	-
描述	

提交 取消

提示：

编辑策略时，地址类型和入接口及出接口都不能改变。

27.2.6 删除安全策略

配置步骤：

1、进入**策略>防火墙策略>访问控制**，如下图：

2、点击 删除策略。

27.2.7 调整安全策略的顺序

通过移动策略可以调整安全策略的顺序，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>访问控制**，如下图：

ID	IPv4	源地址	目的地址	时间表	服务	用户	应用	动作	命中	启用	操作
any->any (2/2)											
1	IPv4	any	any	always	any	any	any	PERMIT	0	☑	
3	IPv4	any	any	always	any	any	any	DENY	0	☑	

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**。

提示：

只有定义在相同入接口与出接口下且相同协议类型的策略，才能调整顺序。

27.2.8 插入一条安全策略

配置步骤：

1、进入**策略>防火墙策略>访问控制**，如下图：

ID	IPv4	源地址	目的地址	时间表	服务	用户	应用	动作	命中	启用	操作
any->any (2/2)											
1	IPv4	any	any	always	any	any	any	PERMIT	0	☑	
3	IPv4	any	any	always	any	any	any	DENY	0	☑	

2、点击 插入一条新的策略到参考策略之前。

地址类型	IPv4
入接口	any
出接口	any
源地址	any
目的地址	any
服务	any
用户	所有用户
应用	any
时间表	always
动作	PERMIT
日志	
源主机连接限制	0 (0-10000000)
源主机连接速率限制	0 (0-10000000)/秒
流量统计	
流量镜像	-
描述	

更新 取消

3、点击**更新**。

注意：

插入策略中的入接口、出接口、地址类型都必须与参考策略中的相同。

27.2.9 查询安全策略

查询步骤：

1、进入**策略>防火墙策略>访问控制**，如下图：

ID	IPv4	源地址	目的地址	时间表	服务	用户	应用	动作	命中	启用	操作
any->any (2/2)											
1	IPv4	any	any	always	any	any	any	PERMIT	0	☑	
3	IPv4	any	any	always	any	any	any	DENY	0	☑	

2、在下拉框中分别选择**源地址**、**目的地址**、**服务**和**动作**，点击**搜索**查询配置中与关键字相符的所有安全策略。

27.3 配置案例

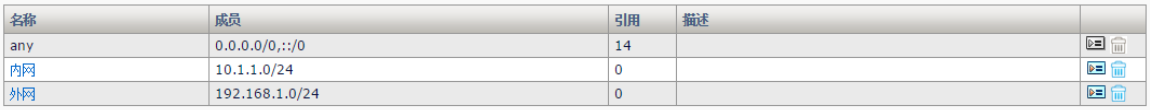
27.3.1 案例 1：创建 IPv4 安全策略允许区域互访

案例描述

设备的 vlan1 连接内网，配置策略允许内网在非工作时间访问外网。

配置步骤：

1、进入**对象>地址对象>地址对象**，配置地址对象“内网”和“外网”，如下图：

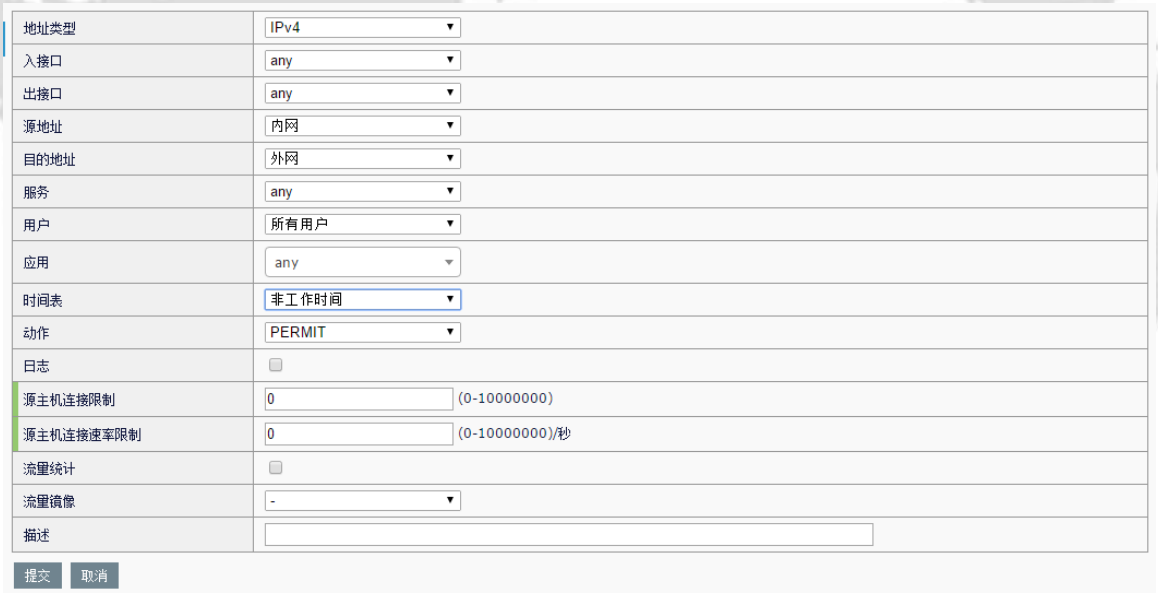


名称	成员	引用	描述	
any	0.0.0.0/0,::/0	14		
内网	10.1.1.0/24	0		
外网	192.168.1.0/24	0		

2、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：

名称	开始日期	结束日期	引用	描述	操作
非工作时间	2000-03-06 11:49	2099-03-06 11:49	0		

3、进入**策略>防火墙策略>访问控制**，点击**新建**，输入参数，如下图：



地址类型	IPv4
入接口	any
出接口	any
源地址	内网
目的地址	外网
服务	any
用户	所有用户
应用	any
时间表	非工作时间
动作	PERMIT
日志	
源主机连接限制	0 (0-10000000)
源主机连接速率限制	0 (0-10000000)/秒
流量统计	
流量镜像	-
描述	

提交 取消

4、点击**提交**。

5、进入**策略>防火墙策略>访问控制**，如下图：

ID	IPv4	源地址	目的地址	时间表	服务	用户	应用	动作	命中	启用	操作
any->any (1/1)											
4	IPv4	内网	外网	非工作时间	any	any	any	PERMIT	0	☑	

6、勾选**启用**完成设置。

27.3.2 案例 2：创建 IPv6 安全策略允许区域互访

案例描述：

设备的 vlan1 连接测试部，配置策略允许测试部在上班时间访问研发部。

配置步骤：

1、进入**对象>地址对象>地址对象**，配置地址对象“测试部”和“研发部”，如下图：

名称	成员	引用	描述	
any	0.0.0.0/0,::/0	10		
测试部	4010::2013:0/112	0		
研发部	4010::2014:0/112	0		

2、进入**对象>时间对象>周期时间**，配置时间对象“上班时间”，如下图：

名称	开始日期	结束日期	引用	描述	操作
上班时间	2000-03-06 14:42	2099-03-06 14:42	0		

3、进入**策略>防火墙策略>访问控制**，点击**新建**，输入参数，如下图：

地址类型	IPv6
入接口	any
出接口	any
源地址	测试部
目的地址	研发部
服务	any
用户	所有用户
应用	any
时间表	上班时间
动作	PERMIT
日志	
源主机连接限制	0 (0-10000000)
源主机连接速率限制	0 (0-10000000)/秒
流量统计	
流量镜像	-
描述	

提交 取消

4、点击**提交**。

5、进入**策略>防火墙策略>访问控制**，如下图：

ID	IPv6	源地址	目的地址	时间表	服务	用户	应用	动作	命中	启用	操作
any->1 (1/1)											
2	IPv6	any	any	always	any	any	any	PERMIT	0	☑	
any->any (1/1)											

6、勾选**启用**完成设置。

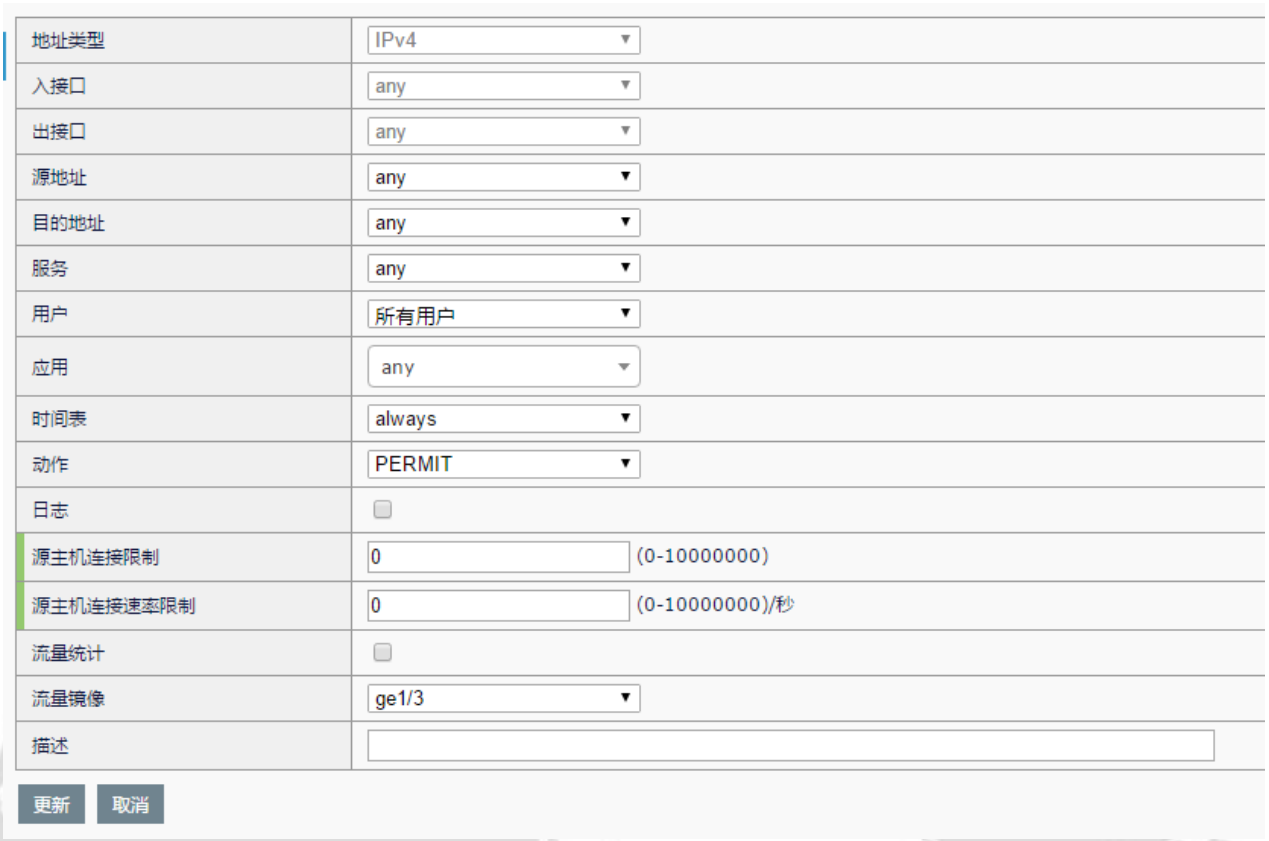
27.3.3 案例 3：将匹配策略的流镜像到物理接口

案例描述：

配置匹配策略的流镜像到物理接口

配置步骤：

1、进入**策略>防火墙策略>访问控制**，点击**新建**，输入参数，如下图：



2、点击**提交**。

3、进入**策略>防火墙策略>访问控制**，如下图：

4、勾选**启用**完成设置。

提示：

将 PC 机与镜像口连接，在 PC 机中开启抓包工具便能够抓取所有的镜像报文。

27.4 安全策略监控与维护

27.4.1 查看安全策略

1、进入**策略>防火墙策略>转发策略**，可以根据协议类型查看已经配置的安全策略

#	IPv6	源地址	目的地址	时间表	服务	用户	应用	动作	命中	启用	操作
vlan1->any (0/1)											
1	IPv6	测试部	研发部	上班时间	any	any	any	PERMIT	0	☑	

27.5 常见故障分析

27.5.1 故障现象：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： 策略匹配模块没有开启，请检查策略配置里的策略匹配是否开启 该策略没有启用，请检查策略状态是否为启用。 由于策略按在 IPv4 或 IPv6 的相同入、出接口时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

第28章 用户策略

28.1 认证策略概述

为了方便用户配置和管理，通讯防火墙设备中引入了认证策略的概念。认证策略用来控制用户上网的认证方式。

28.1.1 配置认证策略

1、进入**策略>用户策略>认证策略**，点击**新建**

入接口/安全域：用户访问的源接口
源地址：用户访问的源地址
出接口/安全域：用户访问的目的接口
目的地址：用户访问的目的地址
相关行为：分为允许、本地 WEB 认证
时间：该用户策略生效的时间范围

2、配置成功后，点击**提交**

3、提交后，点击**编辑**按钮，对用户策略进行更改

4、点击**删除**按钮，删除策略

28.1.2 配置本地认证

1、进入**对象>认证服务器>本地认证**

用户唯一性检查：是否进行用户唯一性检查，分为单一账号登录和允许同一账号重复登录两种

单一账号登录：当选择单一账号登录时，可设置踢出已登录用户或禁止同名用户再次登录两种

允许重复登录：当选择允许重复登录时，可设置该账号允许同时登录个数，可设置为无限制或具体个数

客户端心跳超时：是否启用心跳超时检测。启用后可设置心跳超时时间

强制重登录间隔：是否强制用户重新登录间隔。启用后可设置间隔时长

重定向 URL：用户进行认证时其重定向的 URL

28.1.3 用户监控

1、进入**统计>在线用户统计**

用户组：系统默认生成的几类用户组和管理员添加的用户组

查询：根据 IP 地址查找用户在线信息

操作：清除、冻结和强制下线

第29章 应用策略

29.1 应用控制策略概述

随着宽带网络的不断普及，IM(即时聊天软件，如 MSN、QQ)，P2P(点到点传输软件，如 BitTorrent、eMule)，流媒体（视频点播软件，如 PPLive、QQLive），网络游戏（如搜狐游戏大厅、快乐西游）和股票软件（如大智慧、万点理财）在人们的工作、生活中也扮演了越来越重要的角色。

IM、P2P、流媒体、网络游戏和股票软件在给人们带来便利的同时，也给网络管理带来了新的挑战。一方面，这些软件随意滥用导致的网络拥堵、内部网络信息泄露、病毒传播等情况时有发生；另一方面，由于应用协议的复杂性，传统的防火墙对这些常用外联软件又无能为力，所以迫切需要针对外联软件进行有效管理的手段。

应用主要有以下类别：

即时通讯：MSN、QQ、雅虎通、Gtalk、Skype 等。

P2P 软件：迅雷、QQ 旋风、BitTorrent 等。

流媒体：优酷、土豆、新浪视频等。

网络社区：新浪微博、腾讯微博、猫扑论坛、百度贴吧等。

网络游戏：魔兽世界、英雄联盟、刀塔等。

搜索引擎：百度、谷歌、雅虎、搜狗等。

电子商务：淘宝、京东、一号店、亚马逊等。

其他类别：如股票软件、文件传输、电子邮件、远程控制、生活服务等。

应用只有在应用策略中引用，才能对相关的用户进行应用的控制和审计。应用对象只随着应用特征库的更新而更新，用户不能手动创建新的应用对象，也不能删除已有的应用对象。

29.1.1 配置应用控制策略

1、进入**策略>应用策略>控制策略**，点击**新建**。

状态：选择是否启用该策略

用户：匹配策略的用户对象

源地址：匹配策略的源地址

2、控制规则点击**新建**。

启用规则：选择是否启用该应用控制规则

应用审计：选择应用过滤规则匹配的应用，可以按应用分类匹配和按单个应用对象匹配

相关行为：选择选定的应用类或应用对象具备的行为

行为内容:选择选定的行为所具备的行为内容

匹配关键字：根据匹配类型的不同，分别选择被匹配的关键字对象或数字，其中关键字的匹配方式有：

包含，表示关键字对象的内容包含在行为内容中

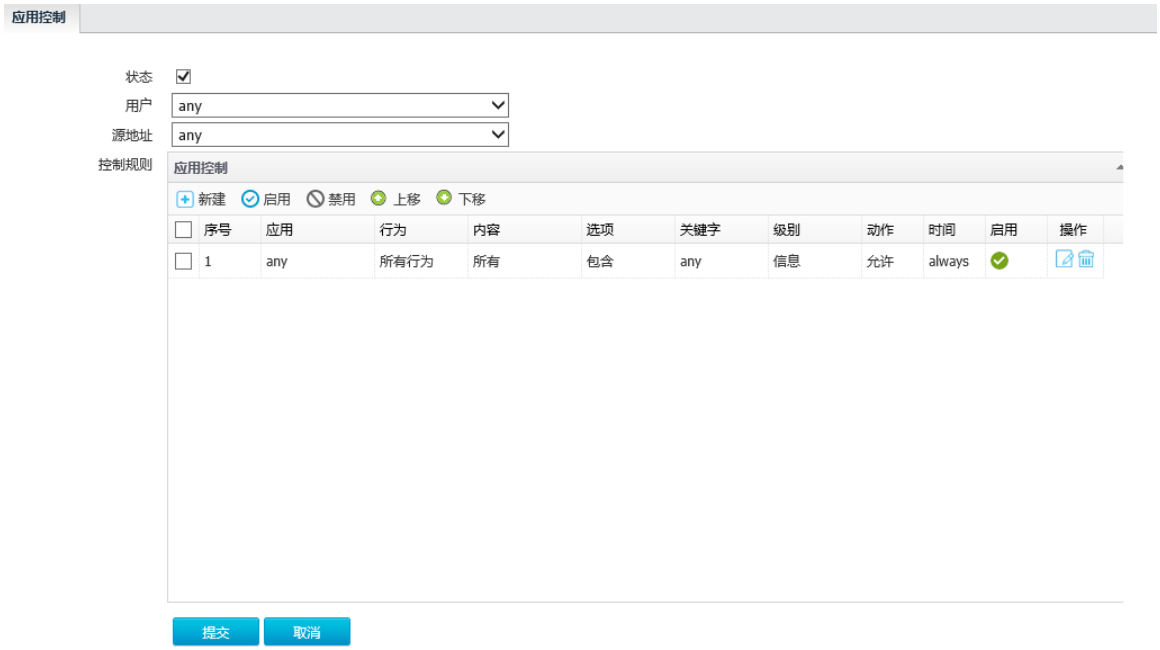
不包含，表示关键字对象的内容不包含在行为内容中

处理动作：选择该应用过滤规则匹配后的处理方式，分为如下两种：允许和拒绝

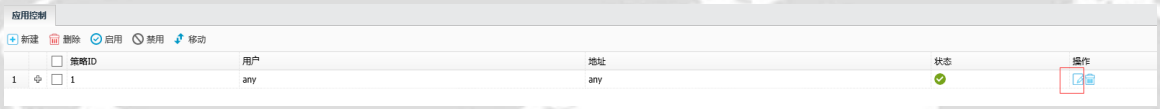
日志级别：选择该应用过滤规则匹配后上报日志的级别，分为如下几种：不记录、紧急、告警、严重、错误、警示、通知、信息

时间：选择策略生效的时间对象

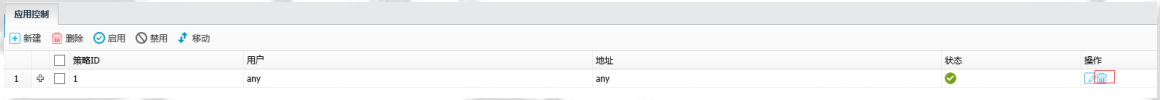
3、配置完成后，点击**提交**



4、进入**策略>应用策略>控制策略**，点击**编辑**，可以对策略进行更改。



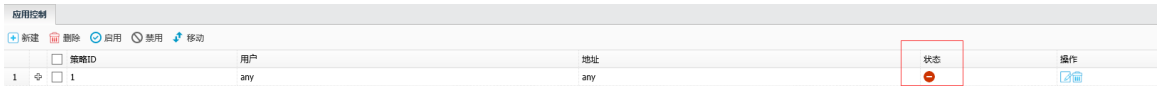
5、点击**删除**，可以删除策略



29.1.2 配置策略启用/禁用

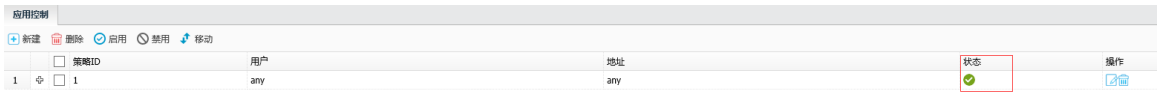
1、进入**策略>应用策略>控制策略**，选中策略，点击**禁用**。

2、提交后，查看策略状态为禁用。



3、选中策略，点击**启用**。

4、提交后，查看策略状态为启用。

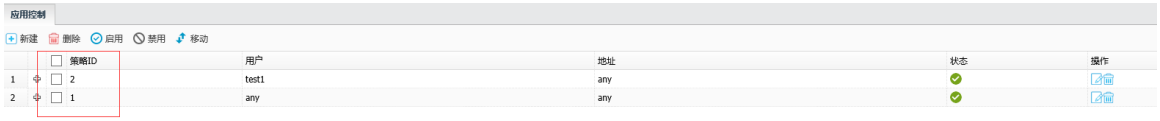


29.1.3 移动策略

1、进入**策略>应用策略>控制策略**，选中策略，点击**移动**。

2、配置移动到策略 ID 1 之前

3、点击**提交**，策略 2 在策略 1 之前



29.2 Web访问和控制策略

29.2.1 配置 web 访问策略

进入**策略>应用策略>web 访问策略**，点击**新建**建立策略

在策略中，配置匹配条件；

状态：只有勾选，这条策略才会生效

用户：可选用户或者用户组对象

地址：匹配地址对象/对象组

控制规则：具体的 web 控制内容

点击 

，建立 web 访问策略控制规则

启用规则：默认勾选，只有勾选的才能生效

URL 分类：匹配不同的 url，包括：娱乐、金融、游戏等分类，可在对象->url->url 分类中查看和修改

文件类型：匹配文件，可以在对象->文件类型中查看/修改

网页关键字：匹配关键字，可以在对象->关键字中查看修改

动作:如果配置“阻断”可以阻断匹配到的 web 访问，配置“允许”则只对匹配到的 web 访问做审计；

日志级别：设置不同级别的日志信息

时间：匹配时间，可在对象->时间对象中查看/编辑

点击 提交 ，建立 web 访问策略

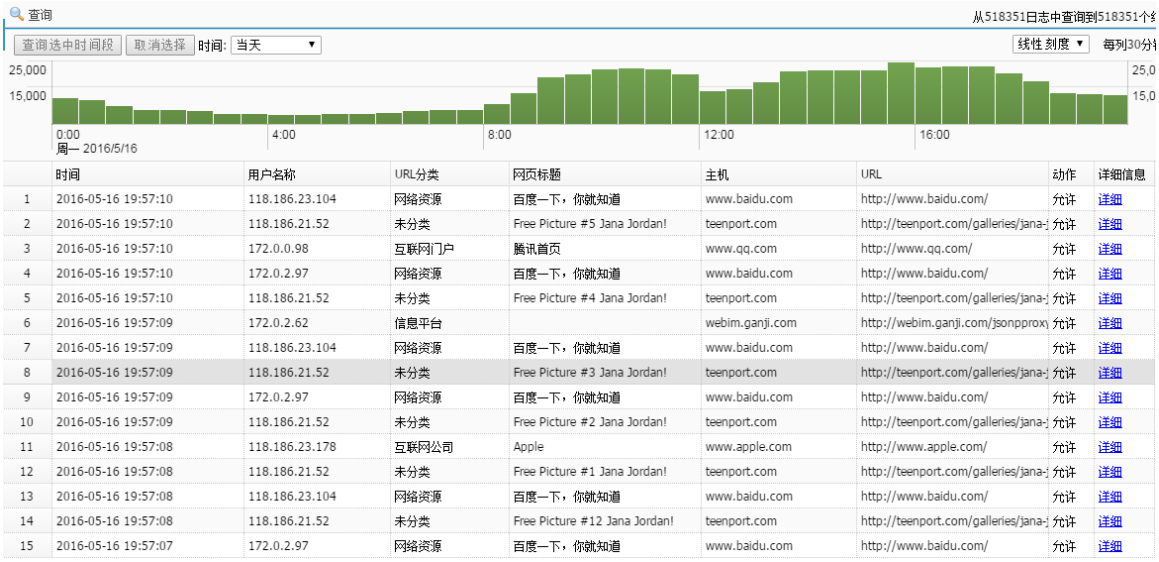
29.2.2 阻断提示页面

启用阻断提示页面之后，当用户的 Web 访问被阻断时，会显示相应的提示页面(通过页面关键字阻断除外)

29.2.3 Web 审计日志的查看

在**系统>日志设定**中开启需要的日志，然后配置审计功能。

进入**日志>网站访问日志**可以查看到 web 日志



	时间	用户名称	URL分类	网页标题	主机	URL	动作	详细信息
1	2016-05-16 19:57:10	118.186.23.104	网络资源	百度一下，你就知道	www.baidu.com	http://www.baidu.com/	允许	详细
2	2016-05-16 19:57:10	118.186.21.52	未分类	Free Picture #5 Jana Jordan!	teenport.com	http://teenport.com/galleries/jana-	允许	详细
3	2016-05-16 19:57:10	172.0.0.98	互联网门户	腾讯首页	www.qq.com	http://www.qq.com/	允许	详细
4	2016-05-16 19:57:10	172.0.2.97	网络资源	百度一下，你就知道	www.baidu.com	http://www.baidu.com/	允许	详细
5	2016-05-16 19:57:10	118.186.21.52	未分类	Free Picture #4 Jana Jordan!	teenport.com	http://teenport.com/galleries/jana-	允许	详细
6	2016-05-16 19:57:09	172.0.2.62	信息平台		webim.ganji.com	http://webim.ganji.com/jsonpprox	允许	详细
7	2016-05-16 19:57:09	118.186.23.104	网络资源	百度一下，你就知道	www.baidu.com	http://www.baidu.com/	允许	详细
8	2016-05-16 19:57:09	118.186.21.52	未分类	Free Picture #3 Jana Jordan!	teenport.com	http://teenport.com/galleries/jana-	允许	详细
9	2016-05-16 19:57:09	172.0.2.97	网络资源	百度一下，你就知道	www.baidu.com	http://www.baidu.com/	允许	详细
10	2016-05-16 19:57:09	118.186.21.52	未分类	Free Picture #2 Jana Jordan!	teenport.com	http://teenport.com/galleries/jana-	允许	详细
11	2016-05-16 19:57:08	118.186.23.178	互联网公司	Apple	www.apple.com	http://www.apple.com/	允许	详细
12	2016-05-16 19:57:08	118.186.21.52	未分类	Free Picture #1 Jana Jordan!	teenport.com	http://teenport.com/galleries/jana-	允许	详细
13	2016-05-16 19:57:08	118.186.23.104	网络资源	百度一下，你就知道	www.baidu.com	http://www.baidu.com/	允许	详细
14	2016-05-16 19:57:08	118.186.21.52	未分类	Free Picture #12 Jana Jordan!	teenport.com	http://teenport.com/galleries/jana-	允许	详细
15	2016-05-16 19:57:07	172.0.2.97	网络资源	百度一下，你就知道	www.baidu.com	http://www.baidu.com/	允许	详细

29.3 应用审计

29.3.1 配置应用审计

在**系统>日志过滤**中开启指定的日志类型，然后进入**策略>应用策略>应用审计**，点击 

，建立审计策略。

状态：是否开启，只有勾选才开启功能

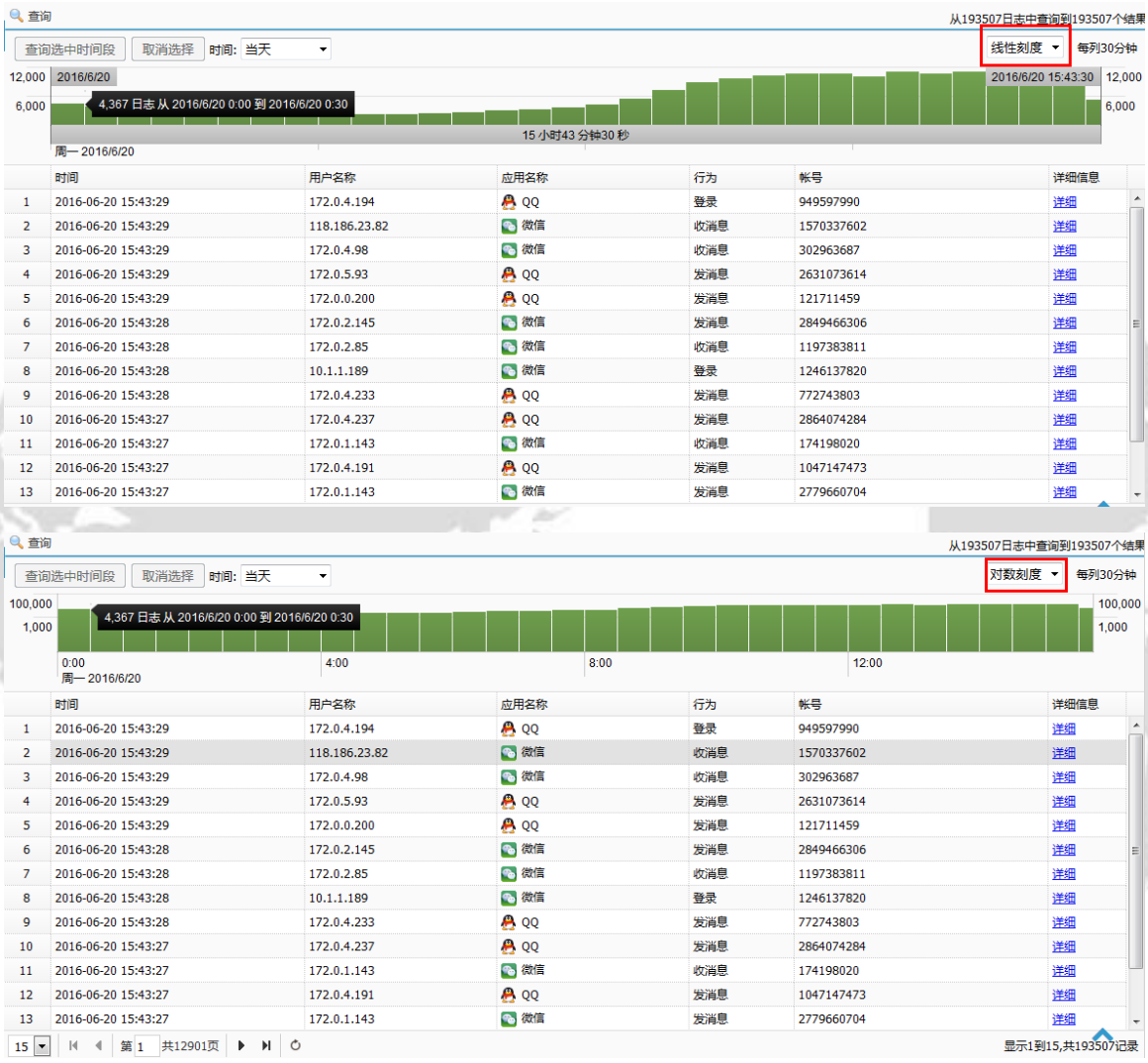
用户：匹配用户

地址：匹配地址

设计内容：不同的审计分类，注意，高级选项中其他应用如果开启会产生大量日志，不建议勾选

29.3.2 查看应用审计日志

进入**日志>应用审计日志**，可以查看不同分类的日志，同时支持日志查询



横轴表示时间，纵轴表示日志条数，纵轴刻度可以按线性刻度/对数刻度两种选择，若每个时间段产生的日志多少差异较大，则选择对数刻度更适合，若差异不大，可选择线性刻度。

29.4 白名单

29.4.1 配置白名单

白名单：应用控制策略、Web 访问策略、应用审计对白名单匹配的用户和地址不生效

进入**策略>用户策略>白名单**，点击**新建**建立白名单，选择用户和地址对象

29.5 配置案例

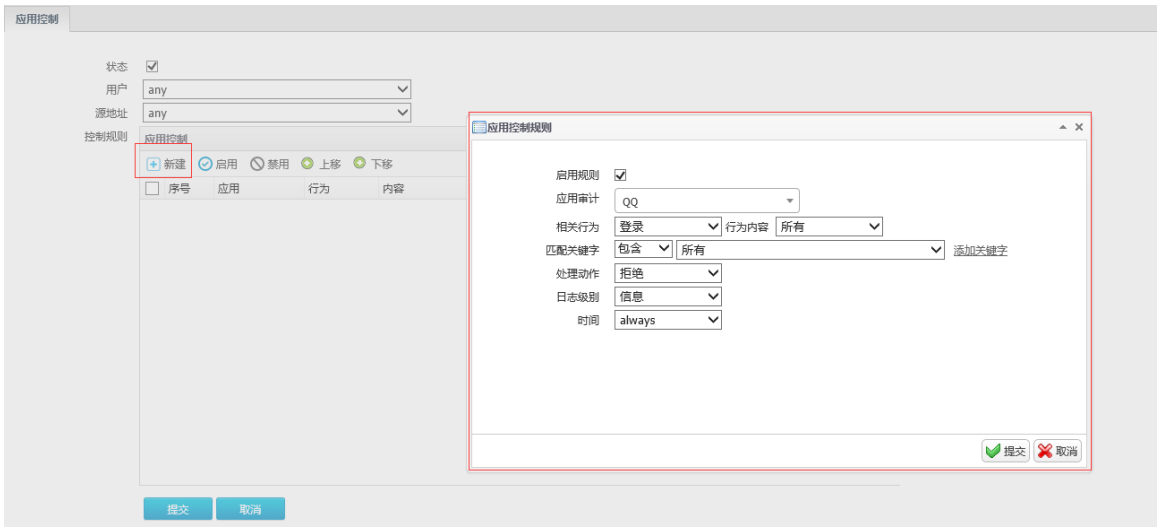
案例描述

配置上网行为策略，阻断 qq 的登录动作，并记录日志。

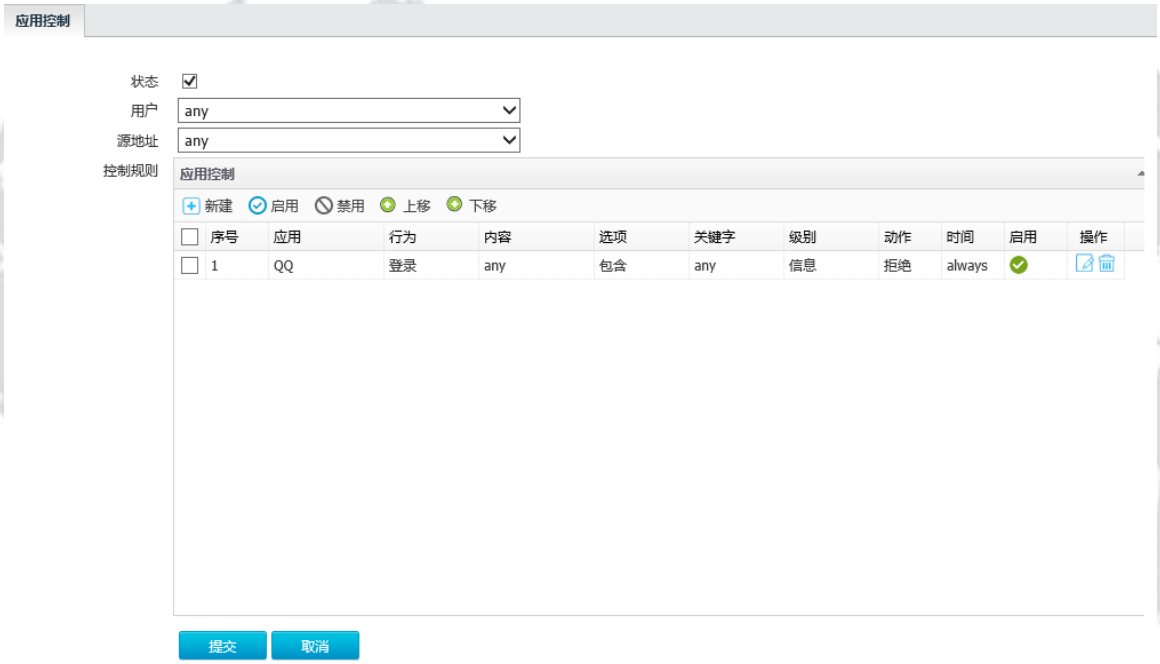
配置步骤：

1、进入**策略>应用策略>控制策略**，点击**新建**。

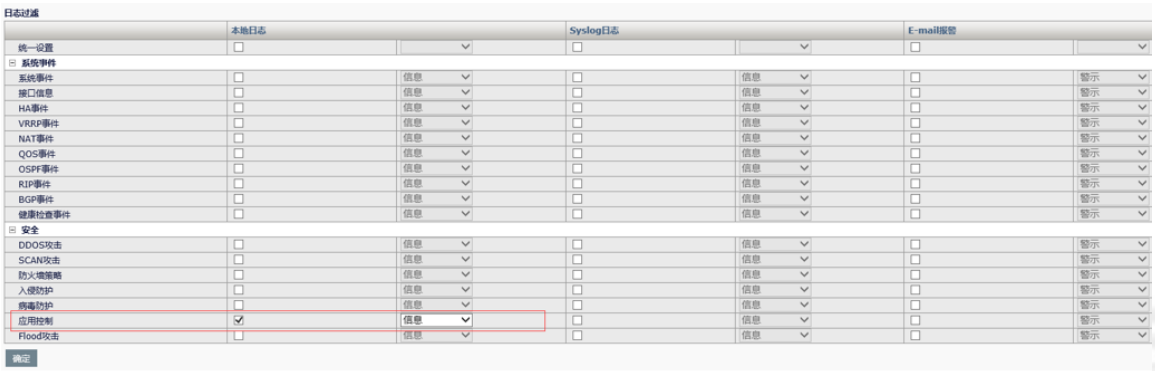
2、配置应用控制规则后，点击**提交**。



3、点击**提交**应用策略



4、进入**日志>日志设定>日志过滤**，勾选本地日志，级别选择信息，点击**确定**。



5、使用 pc 登录 QQ

6、进入**日志>应用控制日志**，查看日志

第30章 入侵防护

30.1 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，下一代防火墙的入侵防护模块则是提供深层防护体系的保障。

下一代防火墙的入侵防护模块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、报警等动作，以达到保护网络的功能。

30.2 配置事件集

30.2.1 默认事件集

入侵防护模块中引入了入侵防护事件集。事件集是一个或多个事件的集合。根据当前实际的网络情况，系统默认提供了 4 个事件集。

进入**策略>防护策略>入侵防护>入侵防护事件集**

默认事件集作为系统提供的资源，不能被删除，只能做有限的配置操作。

30.2.2 创建事件集

1、进入**策略>防护策略>入侵防护>入侵防护事件集**，点击**新建**。

参数说明：

名称：事件集的名称

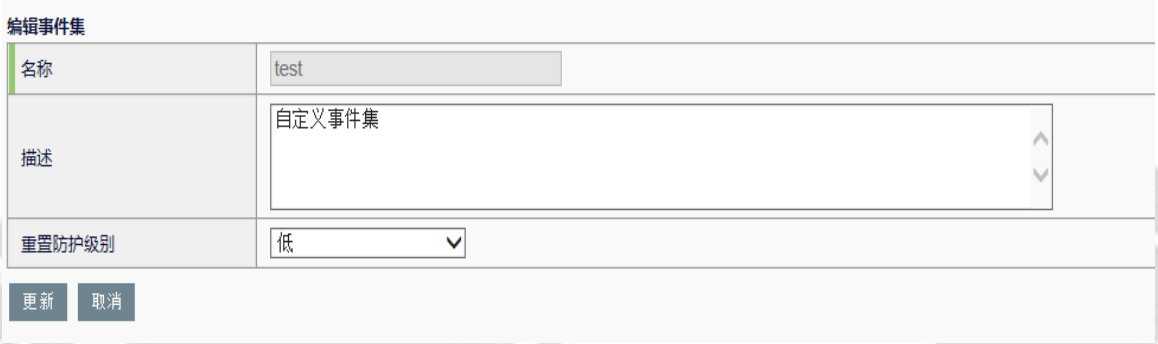
描述：事件集描述信息

防护等级：通过设置事件集的防护等级可以调整本事件集中所有事件的动作

2、点击**提交**，完成新事件集的创建。

30.2.3 编辑事件集

1、进入**策略>防护策略>入侵防护>入侵防护事件集**，点击事件集后面的  编辑按钮，进入编辑事件集页面



参数说明：

名称：事件集的名称，不可修改

描述：事件集描述信息，可以修改

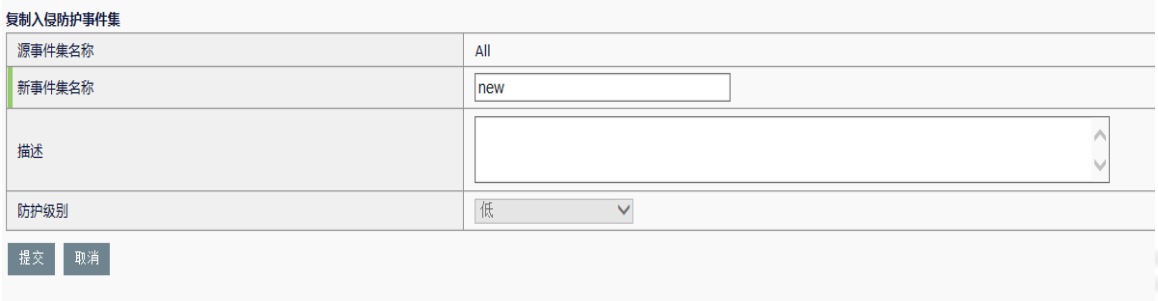
重置防护等级：根据用户需求，参考防护等级的描述，可重置对应事件集得防护等级

2、点击**更新**，完成对事件集的编辑修改。

30.2.4 复制事件集

用户可以根据已经存在的事件集—系统默认或自定义的事件集，复制出相同的自定义事件集。

1、进入**策略>防护策略>入侵防护>入侵防护事件集**，点击  复制图标。



参数说明：

新事件集名称：事件集的名称。

描述：事件集描述信息。

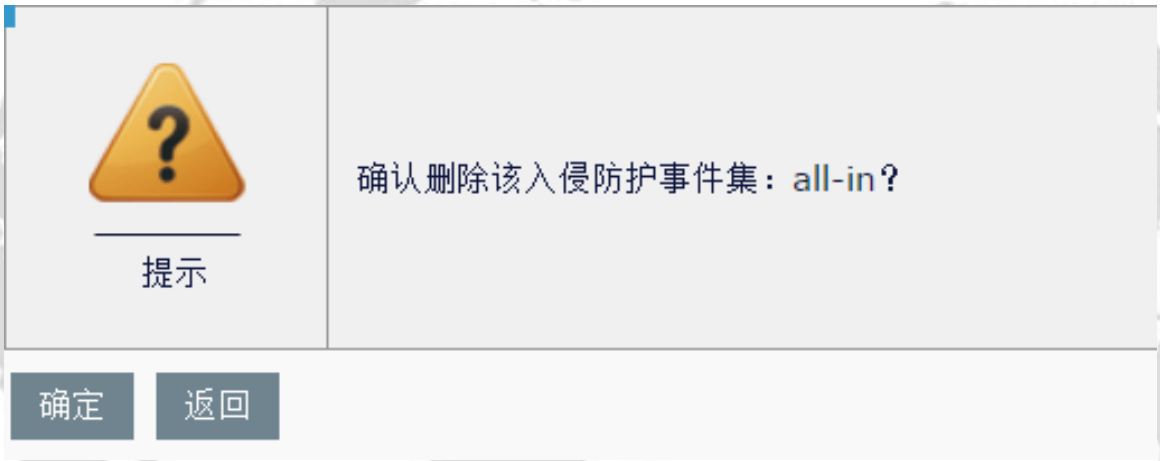
防护等级：复制过程不可以修改事件的防护等级，需要修改可以在复制完的事件集重新编辑修改。

2、点击**提交**，完成事件集的复制。

30.2.5 删除事件集

1、进入**策略>防护策略>入侵防护>入侵防护事件集**，点击自定义事件后面的删除按钮

2、点击**确认**，即可删除事件集。

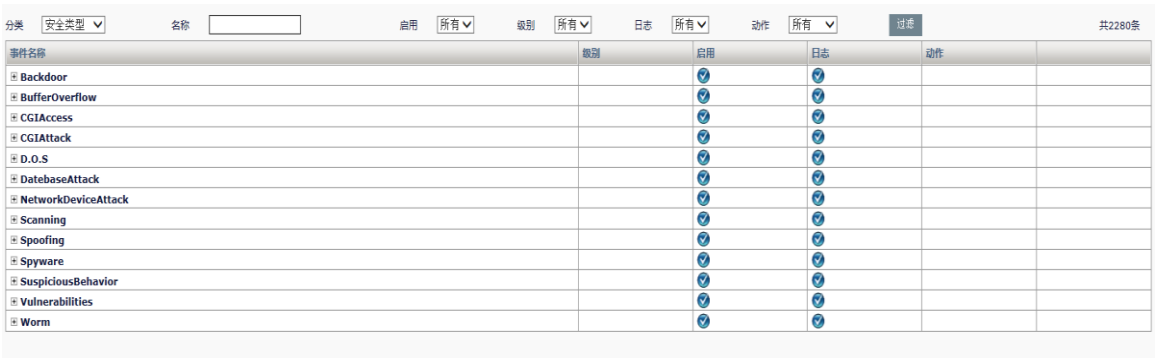


提示：

系统预定义事件集不能删除，被入侵防御策略引用的事件集不能被删除。

30.2.6 查看事件集内容

1、进入**策略>防护策略>入侵防护>入侵防护事件集**，点击事件集名称，即可查看该事件集的详细内容



参数说明：

分类：该事件集的分类方式，可按照**协议类型、系统、安全类型、来源、事件级别**来分类，默认是按照**安全类型**来分类的。

名称：输入事件名称，可检索出该条事件。

启用：按照启用方式检索事件。

级别：按照级别来检索事件。

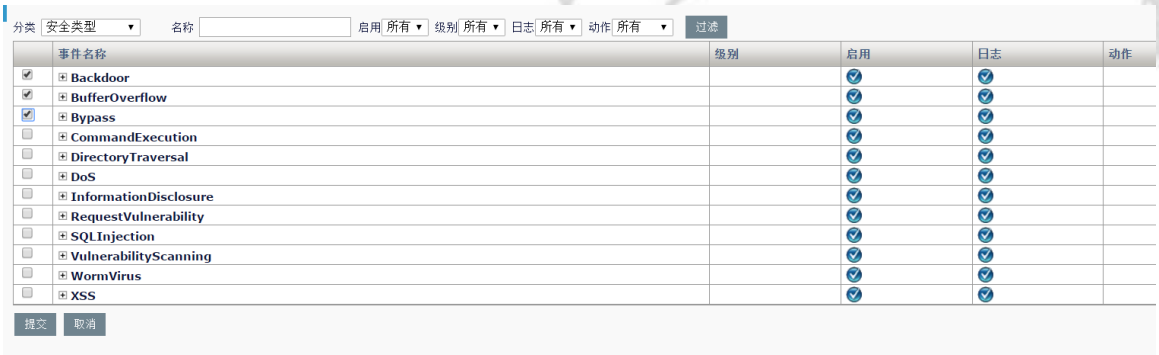
日志：按照是否发送日志来检索事件

动作：按照事件动作来检索事件。

30.2.7 添加事件集中事件

1、进入**策略>防护策略>入侵防护>入侵防护事件集**，选择一个自定义事件集，点击事件集名称。

2、点击**添加事件,**并勾选需要添加的事件。



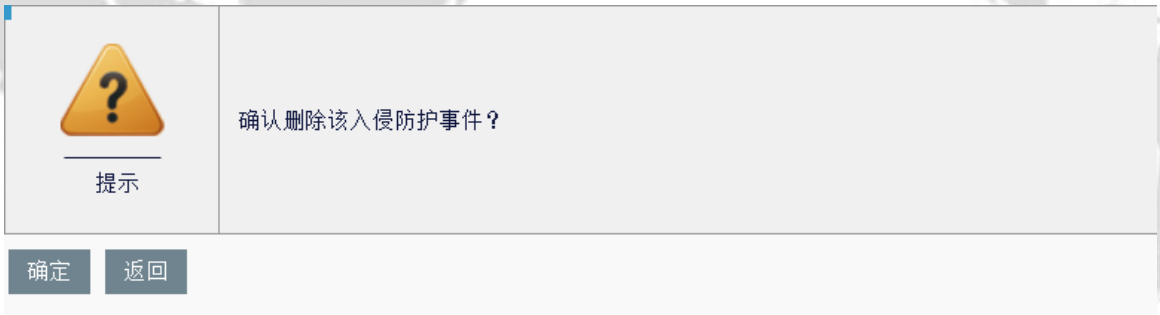
3、点击**提交**，显示已选中的事件信息。

30.2.8 删除事件集中事件

1、进入**策略>防护策略>入侵防护>入侵防护事件集**，选择一个自定义事件集，点击事件集名称。

2、点击 ⊞ 展开事件组

3、找到要删除的事件，点击该事件后面的 🗑 删除该事件。



4、点击**确定**，即可删除事件集中事件。

30.2.9 查询事件集中事件

入侵防护模块可以根据事件名及配置对事件集中的事件进行查询。

1、进入**策略>防护策略>入侵防护>入侵防护事件集**，选择一个事件集，点击事件集名称。

2、在上方输入过滤条件：

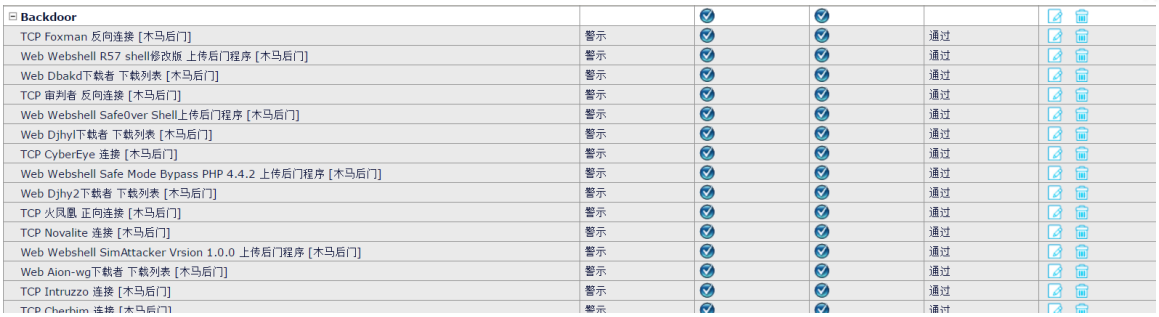
3、点击**过滤**，会列出所有符合条件的事件：

30.2.10 配置事件集中事件

入侵防护模块可以配置某一事件集中事件的级别、是否启用、是否记录日志、匹配事件后执行的动作。

1、进入**策略>防护策略>入侵防护>入侵防护事件集**，选择一个事件集，点击事件集名称。

2、点击展开事件组。



3、选择某个事件，点击  。

参数说明：

名称：事件名称。

级别：事件级别。

启用：启用或关闭该事件。

日志：开启或关闭日志功能。

动作：配置对匹配该事件的数据报或流执行的通过、丢弃或重置等动作。

点击**更新**提交修改。

提示：

只能对自定义事件集中的事件进行编辑，系统默认事件集中的内容无法编辑。

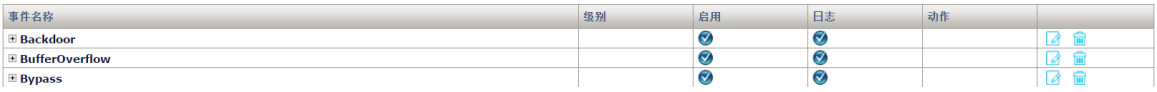
30.2.11 配置事件集中事件组

入侵防护模块可以根据协议类型、操作系统、安全类型、事件来源、事件级别这 5 种类型对事件进行分组。

可以对整个事件组进行配置，对本组内的所有事件都会生效。

配置步骤：

1、进入**策略>防护策略>入侵防护>入侵防护事件集**，选择一个事件集，点击事件集名称。



2、选择某个事件组，点击 。

参数说明：

分类：事件分类名称。

级别：该事件组内事件级别。

启用：启用或关闭该事件组内事件。

日志：开启或关闭该事件组内事件的日志功能。

动作：配置对匹配该事件组内事件的数据报或流执行的通过、丢弃或重置等动作。

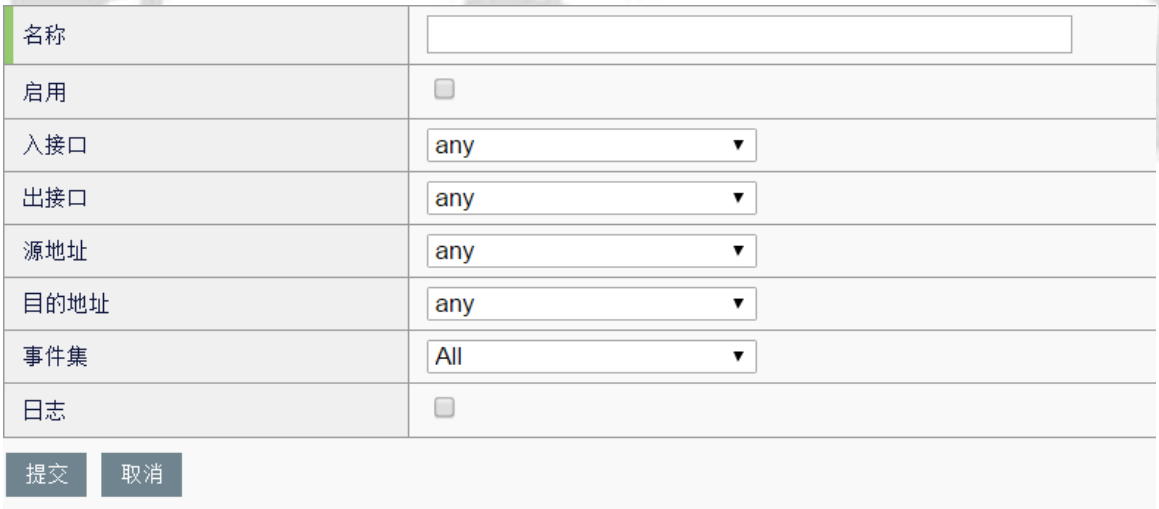
3、点击更新。

提交后，事件组内的所有特征都会配置成相同的级别、启用状态、日志及动作。

30.3 入侵防护策略

要想使入侵防御护生效，必须配置相应的入侵防护策略并引用相关的事件集。

1、进入**策略>防护策略>入侵防护>入侵防护策略**。点击新建按钮创建一条新的安全防护策略。



参数说明：

名称：入侵防护策略的名称。

启用：入侵防护策略启用或禁用。

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。

出接口：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。

事件集：引用预定义或自定义的入侵防护事件集。

日志：启用或禁用入侵防护日志

30.4 其他设备联动

1、进入**策略>防护策略>入侵防护>其他设备联动**，点击启用可启用设备联动功能，启用设备联动功能后，本设备一旦有阻断源地址的动作产生，便可以将该 ip 自动添加到联动设备的黑名单中。

联动设备 IP：联动设备的 ip 地址

联动设备端口：联动设备的端口号，为 8888

联动设备用户名：联动设备登录的用户名

联动设备密码：联动设备登录的密码

30.5 日志合并

1、进入**策略>防护策略>入侵防护>日志合并**，点击启用可配置合并条件和合并间隔。

合并条件：配置日志根据源 IP/目的 IP/源目的 IP 进行合并。

合并间隔：配置时间间隔。即日志在合并间隔内对符合合并条件的日志进行合并。

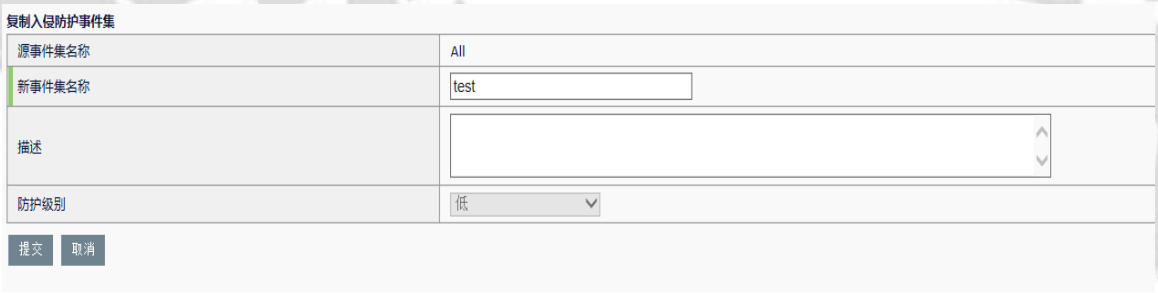
30.6 配置案例：启用入侵防护，对预定义事件检测

案例描述

将防火墙设备部署在实际网络环境中。在设备上配置事件集，利用事件特征检测到特定网络行为，从而对该行为采取通过、丢弃、阻断等动作。

配置步骤：

1、进入**策略>防护策略>入侵防护>入侵防护事件集**，点击 复制事件集 All。



2、进入**策略>防护策略>入侵防护>入侵防护策略**。点击**新建**按钮创建一条新的安全防护策略，引用步骤 1 中创建的事件集并启用日志。

名称	test
启用	☑
入接口	any
出接口	any
源地址	any
目的地址	any
事件集	test
日志	☑

提交 取消

3、进入**系统>日志设定>日志过滤**，启用入侵防护模块的本地日志记录。

日志过滤

	本地日志		Syslog日志		E-mail报警	
统一设置	☐		☐		☐	
⊞ 系统事件						
⊟ 安全						
DDOS攻击	☐	信息	☐	信息	☐	警示
SCAN攻击	☐	信息	☐	信息	☐	警示
防火墙策略	☐	信息	☐	信息	☐	警示
入侵防护	☑	信息	☐	信息	☐	警示
病毒防护	☐	信息	☐	信息	☐	警示
应用控制	☐	信息	☐	信息	☐	警示

确定

4、进入**日志>入侵防护日志**，可以看到防火墙系统对特定的网络行为进行了检测并记录日志。

	时间	级别	策略ID	名称	源IP	目的IP	协议	源端口	目的端口	安全类型	动作
1	2015-05-25 20:38:12	通知	1	HTTP_目录遍历[../]	10.0.0.158	10.0.0.163	TCP	32778	80	CGI访问	通过
2	2015-05-25 20:38:11	信息	1	HTTP_IIS_bdir_acce_访问	192.168.1.117	192.168.1.50	TCP	4885	80	CGI访问	通过
3	2015-05-25 20:38:11	信息	1	HTTP_IIS_bdir.htr_访问	192.168.1.117	192.168.1.50	TCP	4885	80	CGI访问	通过
4	2015-05-25 20:38:10	告警	1	TCP_RealServer_Win32缓冲区溢出	192.168.30.240	192.168.30.188	TCP	1127	554	缓冲溢出	丢弃
5	2015-05-25 20:38:10	警告	1	SMTP_命令参数_缓冲区溢出攻击尝试	192.168.10.66	192.168.10.50	TCP	2467	25	缓冲溢出	通过
6	2015-05-25 20:38:10	警告	1	TCP_后门_冰河_连接	192.168.10.30	192.168.10.27	TCP	1241	7718	木马后门	丢弃
7	2015-05-25 20:38:10	警告	1	TCP_后门_冰河_连接	192.168.10.27	192.168.10.30	TCP	2986	7626	木马后门	丢弃
8	2015-05-25 20:38:07	通知	1	HTTP_htsearch_任意文件读取尝试	192.168.1.117	192.168.1.50	TCP	3919	80	CGI攻击	通过
9	2015-05-25 20:38:07	通知	1	HTTP_目录遍历[../]	10.0.0.158	10.0.0.163	TCP	32778	80	CGI访问	通过
10	2015-05-25 20:38:07	信息	1	HTTP_IIS_bdir_acce_访问	192.168.1.117	192.168.1.50	TCP	4885	80	CGI访问	通过
11	2015-05-25 20:38:07	信息	1	HTTP_IIS_bdir.htr_访问	192.168.1.117	192.168.1.50	TCP	4885	80	CGI访问	通过
12	2015-05-25 20:38:06	信息	1	HTTP_/etc/passwd_访问	192.168.1.117	192.168.1.50	TCP	3919	80	CGI访问	通过
13	2015-05-25 20:38:06	警告	1	TCP_Microsoft网络共享器SMB请求远程缓冲区溢出漏洞利用[MS02-045]	192.168.23.131	192.168.23.143	TCP	3560	139	缓冲溢出	通过
14	2015-05-25 20:38:06	告警	1	TCP_RealServer_Win32缓冲区溢出	192.168.30.240	192.168.30.188	TCP	1127	554	缓冲溢出	丢弃
15	2015-05-25 20:38:06	警告	1	SMTP_命令参数_缓冲区溢出攻击尝试	192.168.10.66	192.168.10.50	TCP	2467	25	缓冲溢出	通过
16	2015-05-25 20:38:06	警告	1	Netbios_TRANSACTION命令Max_Param_Count字段为0攻击尝试	192.168.23.131	192.168.23.143	TCP	3560	139	拒绝服务	通过
17	2015-05-25 20:38:05	警告	1	TCP_后门_冰河_连接	192.168.10.30	192.168.10.27	TCP	1241	7718	木马后门	丢弃
18	2015-05-25 20:38:05	警告	1	TCP_后门_冰河_连接	192.168.10.27	192.168.10.30	TCP	2986	7626	木马后门	丢弃
19	2015-05-25 20:38:04	信息	1	HTTP_IIS_bdir.htr_访问	192.168.1.117	192.168.1.50	TCP	4885	80	CGI访问	通过
20	2015-05-25 20:38:04	通知	1	HTTP_目录遍历[../]	10.0.0.158	10.0.0.163	TCP	32778	80	CGI访问	通过
21	2015-05-25 20:38:04	信息	1	HTTP_IIS_bdir_acce_访问	192.168.1.117	192.168.1.50	TCP	4885	80	CGI访问	通过
22	2015-05-25 20:38:03	告警	1	TCP_RealServer_Win32缓冲区溢出	192.168.30.240	192.168.30.188	TCP	1127	554	缓冲溢出	丢弃
23	2015-05-25 20:38:03	警告	1	SMTP_命令参数_缓冲区溢出攻击尝试	192.168.10.66	192.168.10.50	TCP	2467	25	缓冲溢出	通过
24	2015-05-25 20:38:02	警告	1	TCP_后门_冰河_连接	192.168.10.30	192.168.10.27	TCP	1241	7718	木马后门	丢弃
25	2015-05-25 20:38:02	警告	1	TCP_后门_冰河_连接	192.168.10.27	192.168.10.30	TCP	2986	7626	木马后门	丢弃

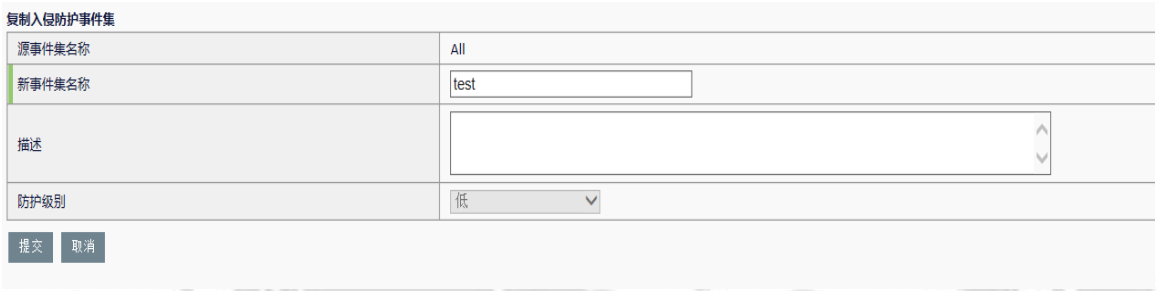
30.7 配置案例：启用入侵防护，开启日志合并

案例描述

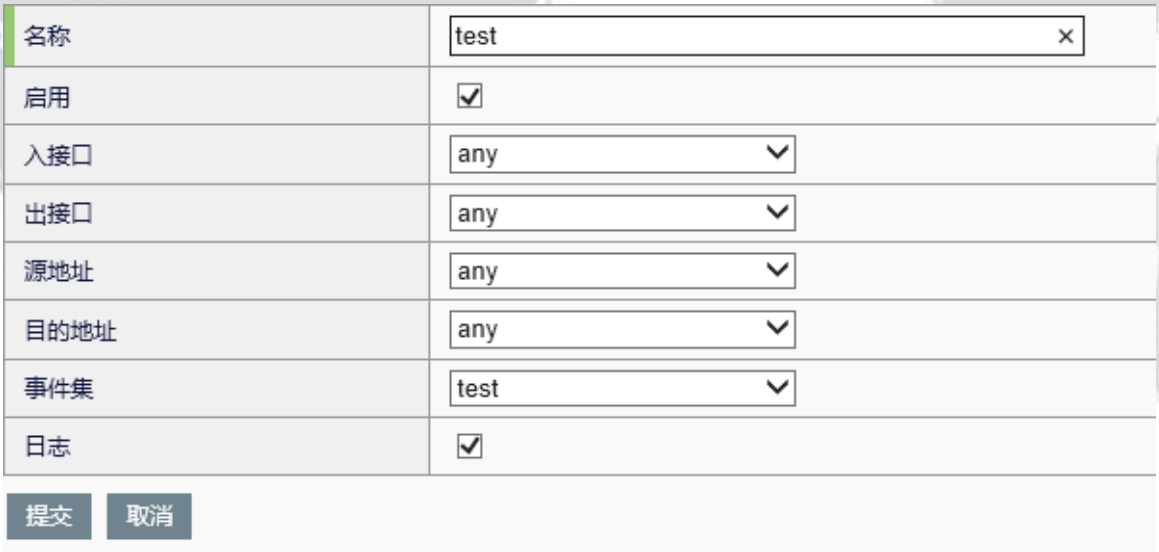
将防火墙设备部署在实际网络环境中。在设备上配置事件集，利用事件特征检测到特定网络行为，从而对该行为采取通过、丢弃、阻断等动作，并开启日志合并，在合并间隔内所有匹配合并条件的日志都被合并为一条。

配置步骤：

1、进入**策略>防护策略>入侵防护>入侵防护事件集**，点击 复制事件集 All。

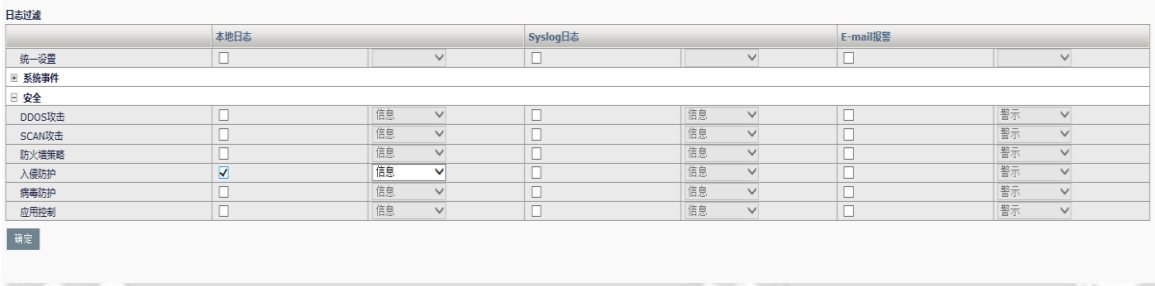


2、进入**策略>防护策略>入侵防护>入侵防护策略**。点击**新建**按钮创建一条新的安全防护策略，引用步骤 1 中创建的事件集并启用日志。

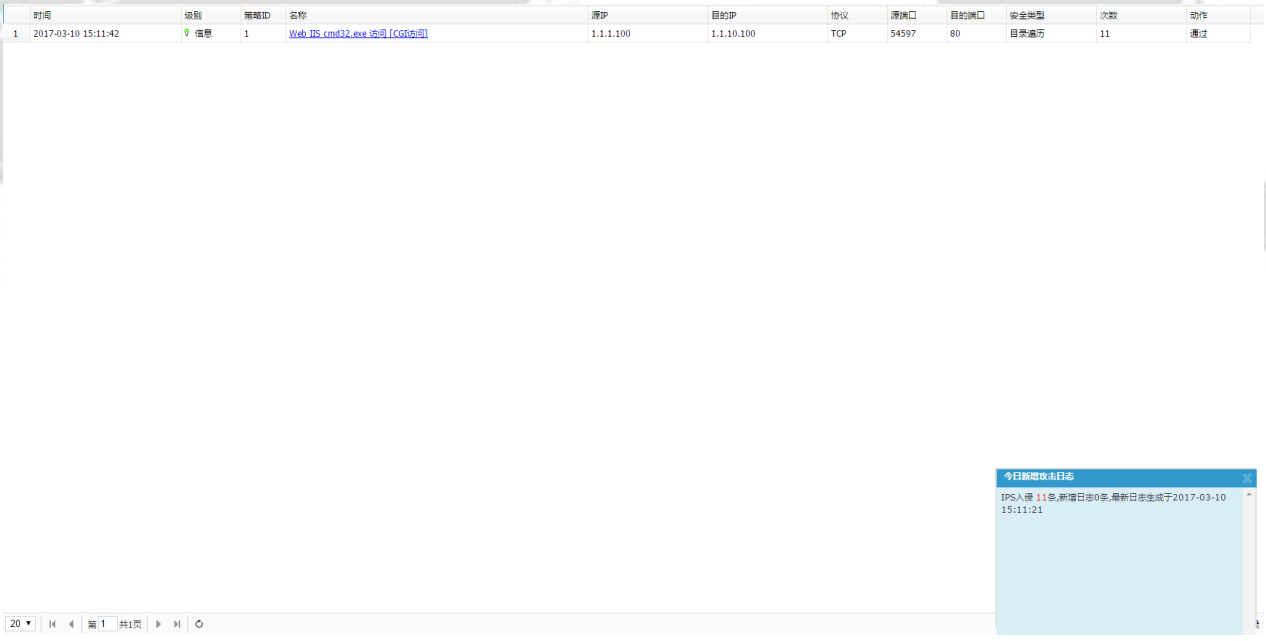


3、进入**策略>防护策略>入侵防护>日志合并**，点击启用可配置合并条件和合并间隔。

4、进入**系统>日志设定>日志过滤**，启用入侵防护模块的本地日志记录。



5、 进入**日志>入侵防护日志**，可以看到 30s 内相同源 ip 的日志仅显示为一条。



第31章 病毒防护

31.1 病毒防护

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。同时还提供文件屏蔽功能，可以对特定的文件类型进行屏蔽。我们可以在诸如 HTTP、FTP、IMAP、POP3、SMTP 等应用协议时进行文件扫描和文件屏蔽。

31.2 防病毒设定

31.2.1 配置扫描所有文件

配置对特定的文件类型进行文件扫描，这样系统只对配置的文件类型进行扫描，提高效率。

配置步骤：

1、进入**策略>防护策略>病毒防护>文件类型配置**

参数说明：

扫描所有文件：勾选扫描所有文件，即对所有文件进行病毒扫描。

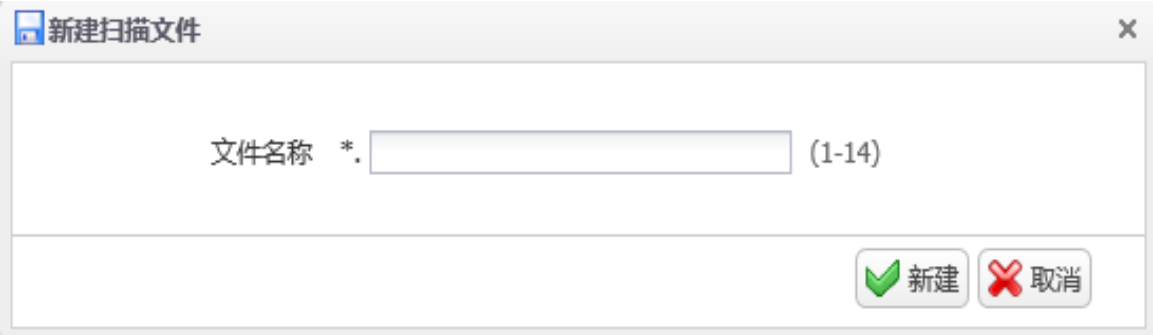
扫描文件列表：可以新建指定的文件类型，也可以通过启用/禁用扫描列表项对指定文件类型进行病毒扫描。

31.2.2 新建扫描列表项

点击扫描文件列表后面的新建按钮，弹出新建扫描文件对话框，可以添加新的需要扫描的文件类型。

配置步骤：

1、进入**策略>防护策略>病毒防护>文件类型配置**，点击**新建**。



输入需要扫描的文件的后缀名。比如 txt 后，点击新建，可以增加扫描文件类型，会对文件后缀为.txt 文件进行病毒扫描。

31.2.3 删除扫描列表项

点击文件名称后面的删除按钮，点击确定后即可删除对应的扫描列表项。**配置请参考系统管理>维护>升级管理章节**

提示：

只能删除用户自定义的扫描列表项，预定义的扫描列表项无法删除。

31.2.4 启用禁用扫描列表项

选中需要启用、禁用的文件名称。再点击工具栏上面的启用、禁用按钮，在弹出的对话框中点击确定。就可以完成文件扫描列项的启动或者是禁用。

配置步骤：

1、进入**策略>防护策略>病毒防护>文件类型配置**

31.3 病毒防护策略

要想使病毒防护生效，必须在相应的安全策略上面启用病毒防护策略。

配置步骤：

1、进入**策略>防护策略>病毒防护>文件类型配置**。新建或者编辑一条已经存在的策略。

参数说明：

启用：启用禁用病毒防护功能。

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。

出接口：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。

协议：支持五中协议的病毒文件扫描：HTTP、FTP、IMAP、POP3、SMTP

沙箱检测：使用沙箱配置检测病毒

行为：允许和阻断

31.4 沙箱检测概述

全系统模拟的沙箱(Sandbox)技术可以更为有效地帮助企业防御 APT 攻击，为一些不可靠的程序提供试验而不影响系统运行的环境有时也被称作沙盒。

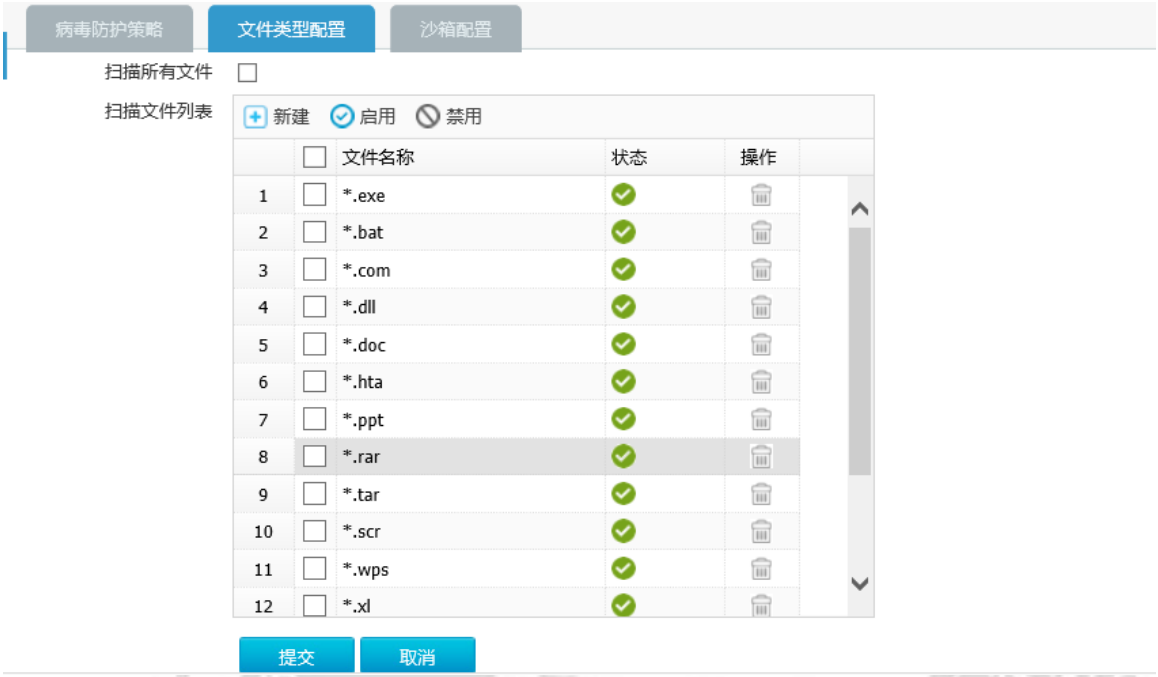
31.4.1 沙箱检测策略

1、进入**策略>病毒防护>病毒防护策略**，点击**新建**。

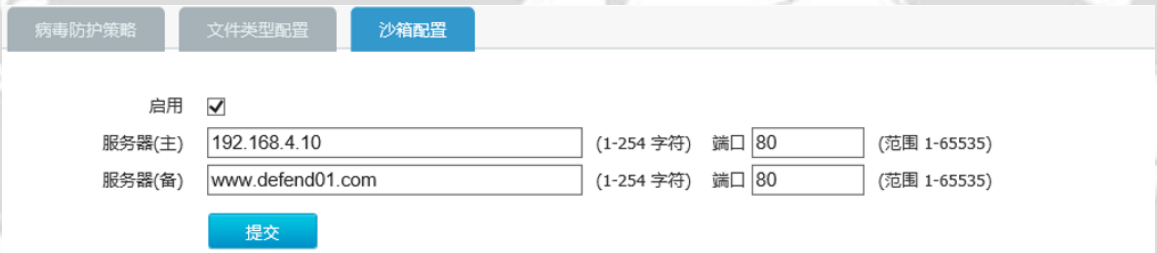
沙箱检测：当前病毒防护策略选择是否启用沙箱检测策略

点击提交按钮，完成病毒防护策略的配置。

2、进入**策略>病毒防护>文件类型配置**。



3、进入**策略>病毒防护>沙箱配置**。



启用：是否启用沙箱检测

服务器（主）：与主服务器联动的通讯地址（威胁检测服务器）

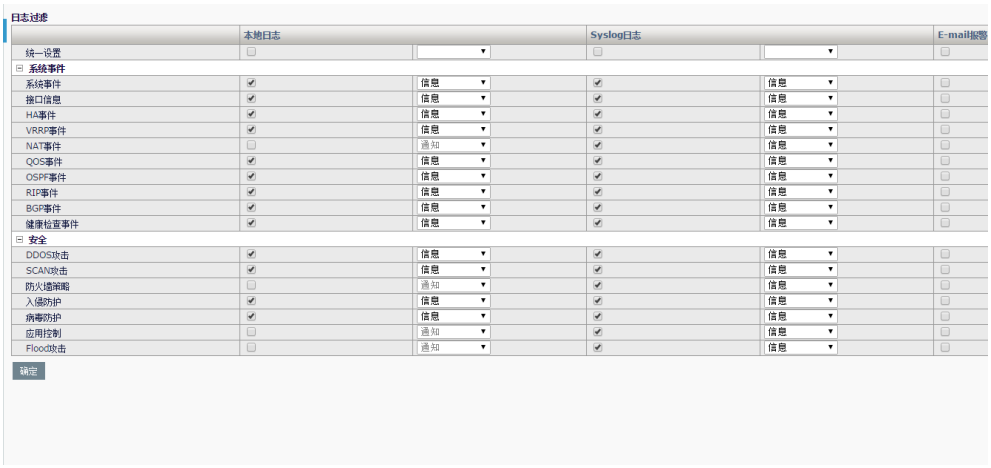
如果配置域名需要在防火墙上配置 DNS 服务器，保证防火墙与 DNS 服务器通讯正常

服务器（备）：与备服务器联动的通讯地址（威胁检测服务器）

端口：与服务器联动时目的主机端口

提交：提交下发沙箱配置

4、进入**系统>日志设定>日志过滤**，在病毒防护勾选本地日志，级别选择信息级别以上。



31.5 配置案例

31.5.1 案例 1：配置病毒防护

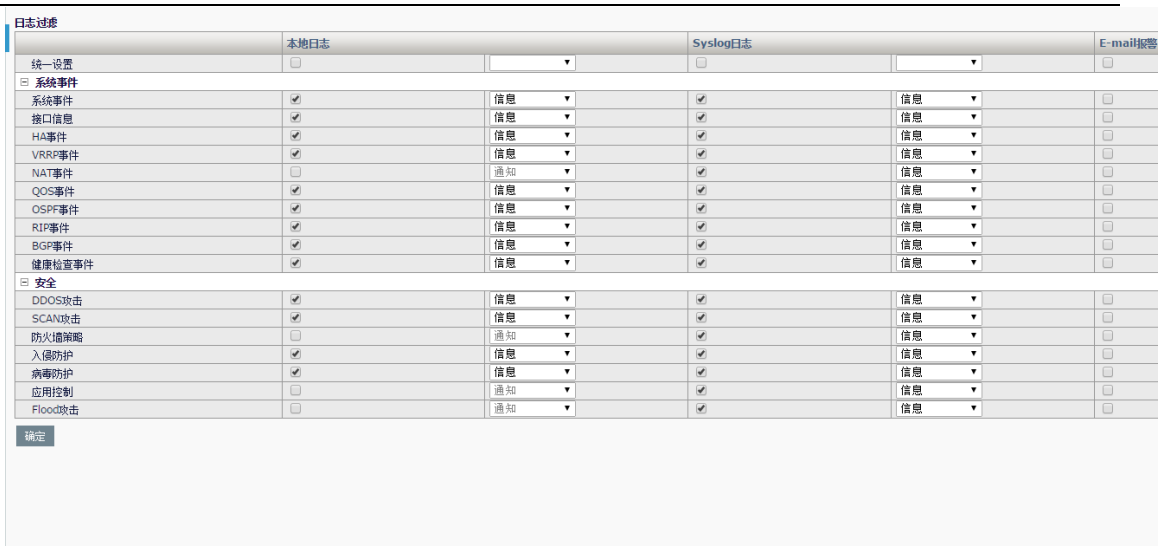
案例描述

有四台服务器通过 Internet 提供 web 和 FTP 服务，配置病毒防护策略来保护 Web 和 FTP 服务器。

配置步骤：

1、进入**策略>防护策略>病毒防护>文件类型配置**，勾选扫描所有文件。

2、进入**系统>日志设定>日志过滤**，在病毒防护勾选本地日志，级别选择信息级别以上。



3、进入**策略>防护策略>病毒防护>病毒防护策略**，点击**新建**。

勾选启用、日志。防护项目选中所有协议，行为选择阻断，点击确定，就可以完成病毒防护的配置。

31.5.2 案例 2：配置沙箱检测

案例描述

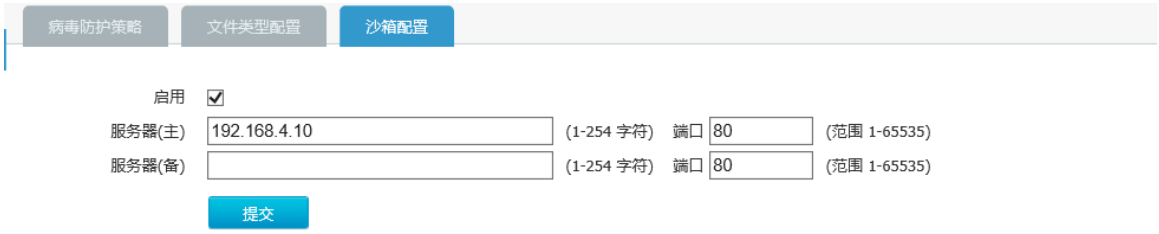
配置沙箱检测，与威胁检测服务器联动，分析检测现网 HTTP 流量中 exe 文件的安全性

配置步骤：

1、进入**策略>病毒防护>病毒防护策略**，点击**新建**。勾选启用策略，入接口出接口源地址目的地址配置 any，协议选择 HTTP，勾选沙箱检测，行为选择记录日志。

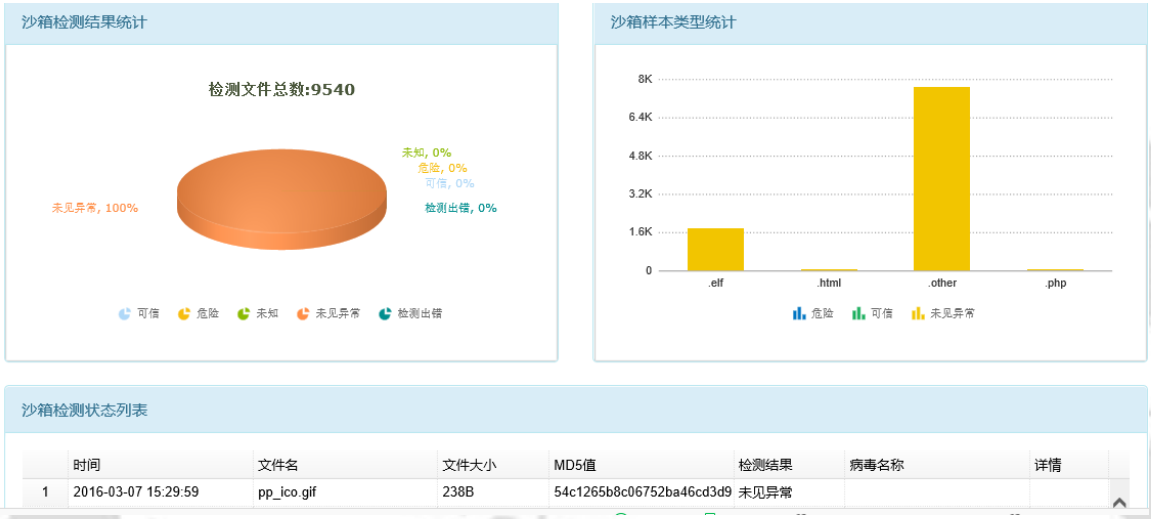
2、进入**策略>病毒防护>文件类型配置**，exe 文件类型勾选启用，其它文件类型禁用。提交配置

3、进入**策略>病毒防护>沙箱配置**，勾选启用策略，服务器主配置 192.168.4.10，端口 80（该功能需配合第三方产品共同使用）。提交配置



4、设备接入现网和威胁检测设备通讯正常，业务流量正常运行的情况下。

进入**统计>病毒防护统计>沙箱检测统计**，可观察到检测结果



第32章 防攻击

32.1 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、teardrop attack、jolt2 attack、syn flood、icmp flood、udp flood、arp flood、syn flag、land-base、winnuke 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：

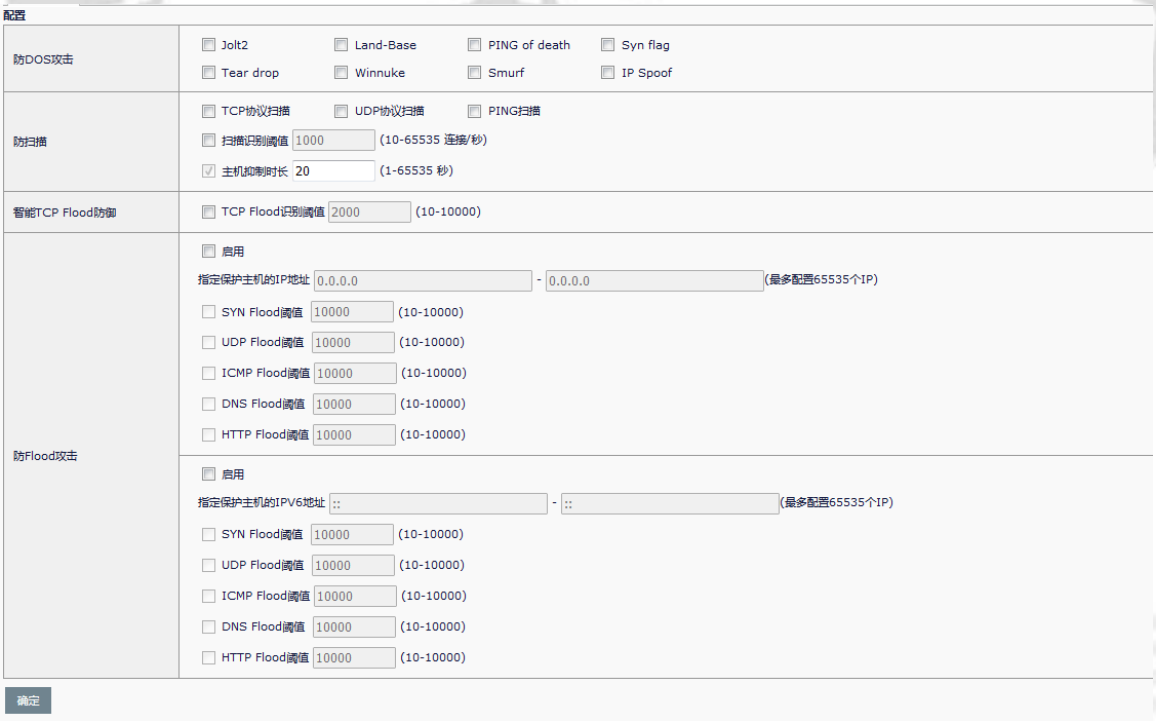
- 垂直（Vertical）扫描：针对相同主机的多个端口
- 水平（Horizontal）扫描：针对多个主机的相同端口
- ICMP (PING) sweeps：针对某地址范围，通过 PING 方式发现存活主机

下一代防火墙设备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。

32.2 配置防攻击

配置步骤：

1、进入**策略>防护策略>DOS 防护**。



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，下一代防火墙设备可以检测出 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，下一代防火墙设备可以检测出 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，下一代防火墙设备可以检测出 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，下一代防火墙设备可以检测出 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，下一代防火墙设备可以检测出 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，因此下一代防火墙设备不会丢弃该报文，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，下一代防火墙设备可以检测出 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。

IP Spoof:防护 IP 地址欺骗攻击，暂时用反向路由过滤来实现，如果反向路由不存在或者反向路由查询结果是存在，但是该 IP 为目的地址的数据包离开设备的接口和收到报文的接口不一致，则认为是攻击

防扫描：

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 地址的不同端口数量大于配置的阈值时，即认为其进行了端口扫描，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 地址的不同端口数量大于配置的阈值时，即进行了一次端口扫描，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。下一代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 100。

智能 FLOOD 防御：

TCP Flood：TCP Flood 即 SYN Flood 攻击，是众多 DOS 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。

下一代防火墙设备的防 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 TCP 半连接的阈值，即防 TCP Flood 攻击的启动门限，缺省配置为 300。

Ipv4/ipv6 Flood：

SYN Flood 攻击

由于资源的限制，TCP/IP 协议栈只能允许有限个 TCP 连接。SYN Flood 攻击者向服务器发送伪造源地址的 SYN 报文，服务器在回应 SYN ACK 报文后，由于目的地址是伪造的，因此服务器不会收到相应的 ACK 报文，从而在服务器上产生一个半连接。若攻击者发送大量这样的报文，被攻击服务器上会出现大量的半连接，耗尽其系统资源，使正常的用户无法访问，直到半连接超时。

ICMP Flood 攻击

ICMP Flood 攻击是指，攻击者在短时间内向特定目标发送大量的 ICMP 请求报文，使其忙于回复这些请求，致使目标系统负担过重而不能处理正常的业务。

UDP Flood 攻击

UDP Flood 攻击是指，攻击者在短时间内向特定目标发送大量的 UDP 报文，致使目标系统负担过重而不能处理正常的业务。

2、按照需要启用防攻击相关功能，并输入合法参数。

3、配置完成后，点击**提交。**

32.3 配置案例

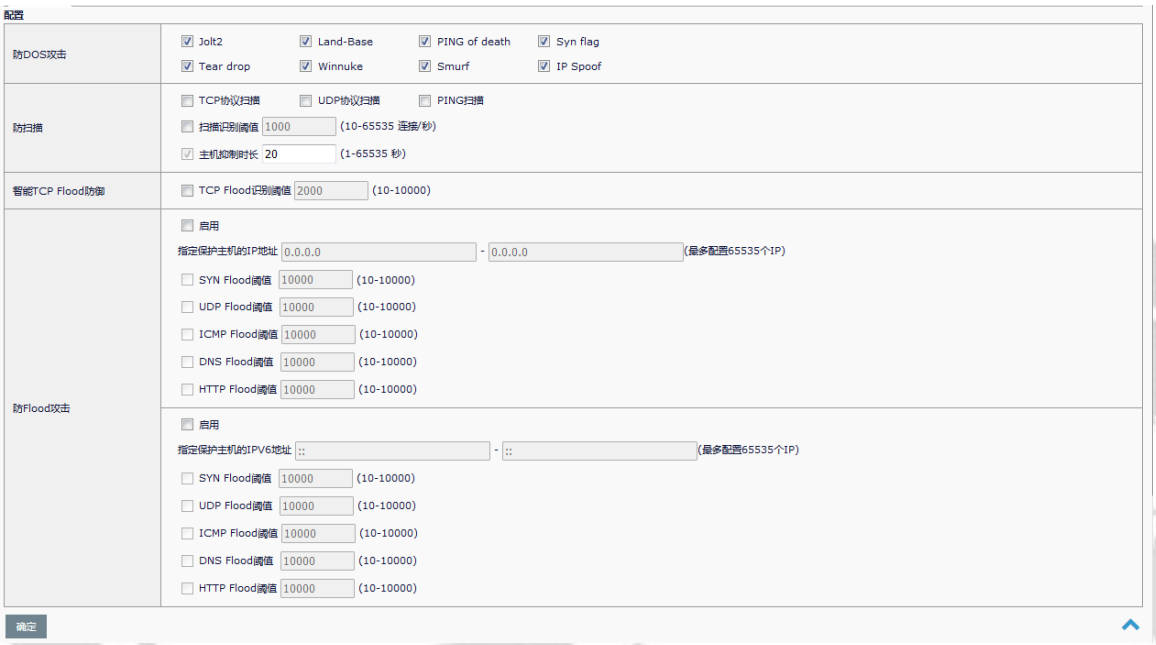
32.3.1 案例 1：配置防 DOS 攻击

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。

配置步骤：

1、进入**策略>防护策略>DOS 防护**，如下图：



2、启用防 DOS 攻击功能，输入参数。

3、点击**确定**完成设置。

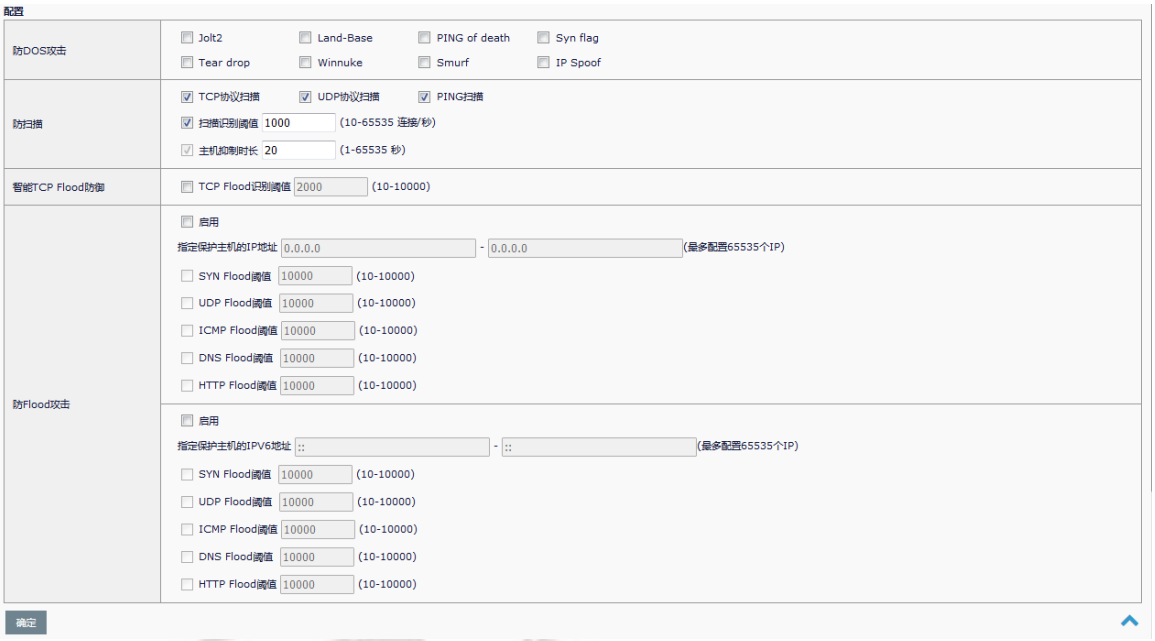
32.3.2 案例 2：配置防扫描

案例描述

当网络上出现扫描攻击时，通过所收集的流信息我们可以看到当前设备上来自于某台主机的半连接信息，如果流信息中有大量源 IP，目的 IP 不变，而对应的目的端口变化的流，可以认为受到了扫描攻击，这时我们可以看一下是什么类型的扫描，然后通过配置对应的防扫描攻击以保护内网和设备。

配置步骤：

1、进入**策略>防护策略>DOS 防护**，如下图：



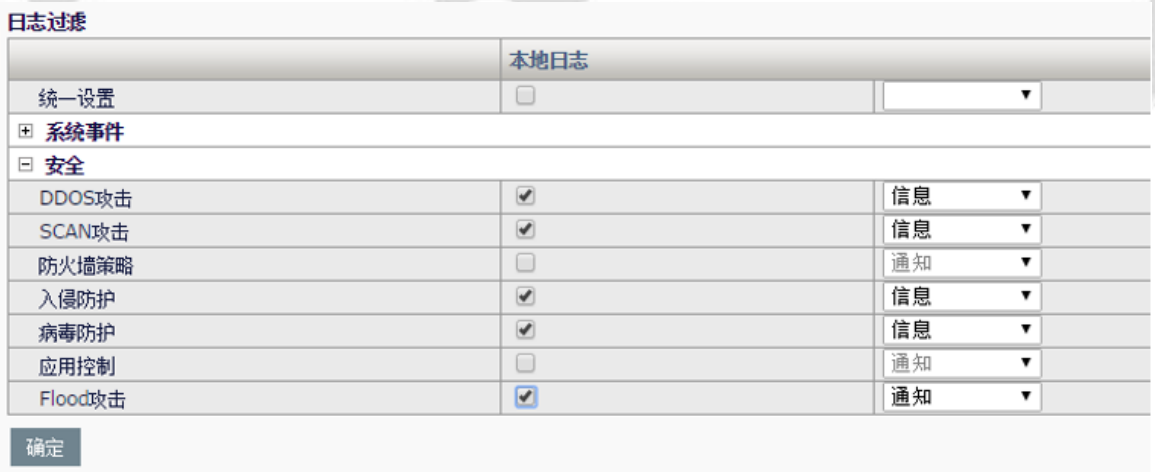
2、启用防扫描功能，输入参数。

3、点击**确定**完成设置。

32.4 防攻击监控与维护

32.4.1 查看防攻击日志

1、进入**系统>日志设定>日志过滤**，勾选出模块的相关日志，设置日志的级别。



2、进入**系统管理>日志管理>安全**里查看相关的安全日志。

查询 导出日志

	时间	类型	级别	消息
1	2015-07-28 11:56:04	SCAN攻击	通知	SrcIP=192.168.1.21 InInterface= Content="TCP block list expired"
2	2015-07-28 11:56:04	SCAN攻击	通知	SrcIP=192.168.2.100 InInterface= Content="TCP block list expired"
3	2015-07-28 11:56:04	SCAN攻击	通知	SrcIP=192.168.10.209 InInterface= Content="TCP block list expired"
4	2015-07-28 11:56:02	SCAN攻击	警告	SrcIP=192.168.2.100 InInterface=ge0/1 Content="Packet is blocked, protocol:UDP"
5	2015-07-28 11:56:01	SCAN攻击	警告	SrcIP=192.168.10.209 InInterface=ge0/1 Content="Packet is blocked, protocol:TCP"
6	2015-07-28 11:56:01	SCAN攻击	警告	SrcIP=192.168.10.209 InInterface=ge0/1 Content="TCP block list created"
7	2015-07-28 11:56:01	SCAN攻击	警告	SrcIP=192.168.2.100 InInterface=ge0/1 Content="TCP block list created"
8	2015-07-28 11:56:01	SCAN攻击	警告	SrcIP=192.168.1.21 InInterface=ge0/1 Content="Packet is blocked, protocol:TCP"
9	2015-07-28 11:56:01	SCAN攻击	警告	SrcIP=192.168.1.21 InInterface=ge0/1 Content="TCP block list created"
10	2015-07-28 11:56:01	SCAN攻击	警告	SrcIP=192.168.2.123 InInterface=ge0/1 Content="Packet is blocked, protocol:TCP"
11	2015-07-28 11:56:01	SCAN攻击	警告	SrcIP=192.168.2.123 InInterface=ge0/1 Content="TCP block list created"
12	2015-07-28 11:56:00	SCAN攻击	警告	SrcIP=192.168.2.156 InInterface=ge0/1 Content="Packet is blocked, protocol:TCP"
13	2015-07-28 11:56:00	SCAN攻击	警告	SrcIP=192.168.10.217 InInterface=ge0/1 Content="Packet is blocked, protocol:TCP"
14	2015-07-28 11:56:00	SCAN攻击	警告	SrcIP=192.168.10.217 InInterface=ge0/1 Content="TCP block list created"
15	2015-07-28 11:56:00	SCAN攻击	警告	SrcIP=192.168.2.156 InInterface=ge0/1 Content="TCP block list created"
16	2015-07-28 11:56:00	SCAN攻击	警告	SrcIP=2.1.1.2 InInterface=ge0/2 Content="Packet is blocked, protocol:TCP"
17	2015-07-28 11:56:00	SCAN攻击	警告	SrcIP=2.1.1.2 InInterface=ge0/2 Content="TCP block list created"
18	2015-07-23 20:12:28	DDOS攻击	警告	SrcIP=172.16.100.240 DstIP=140.207.123.162 InInterface=ge0/0 Content="syn-flag attack"
19	2015-07-23 20:12:27	DDOS攻击	警告	SrcIP=172.16.100.240 DstIP=140.207.123.162 InInterface=ge0/0 Content="syn-flag attack"
20	2015-07-23 20:12:26	DDOS攻击	警告	SrcIP=172.16.100.240 DstIP=140.207.123.162 InInterface=ge0/0 Content="syn-flag attack"

32.5 常见故障分析

32.5.1 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 报文穿过下一代防火墙设备。
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。

32.5.2 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。

第33章 威胁情报

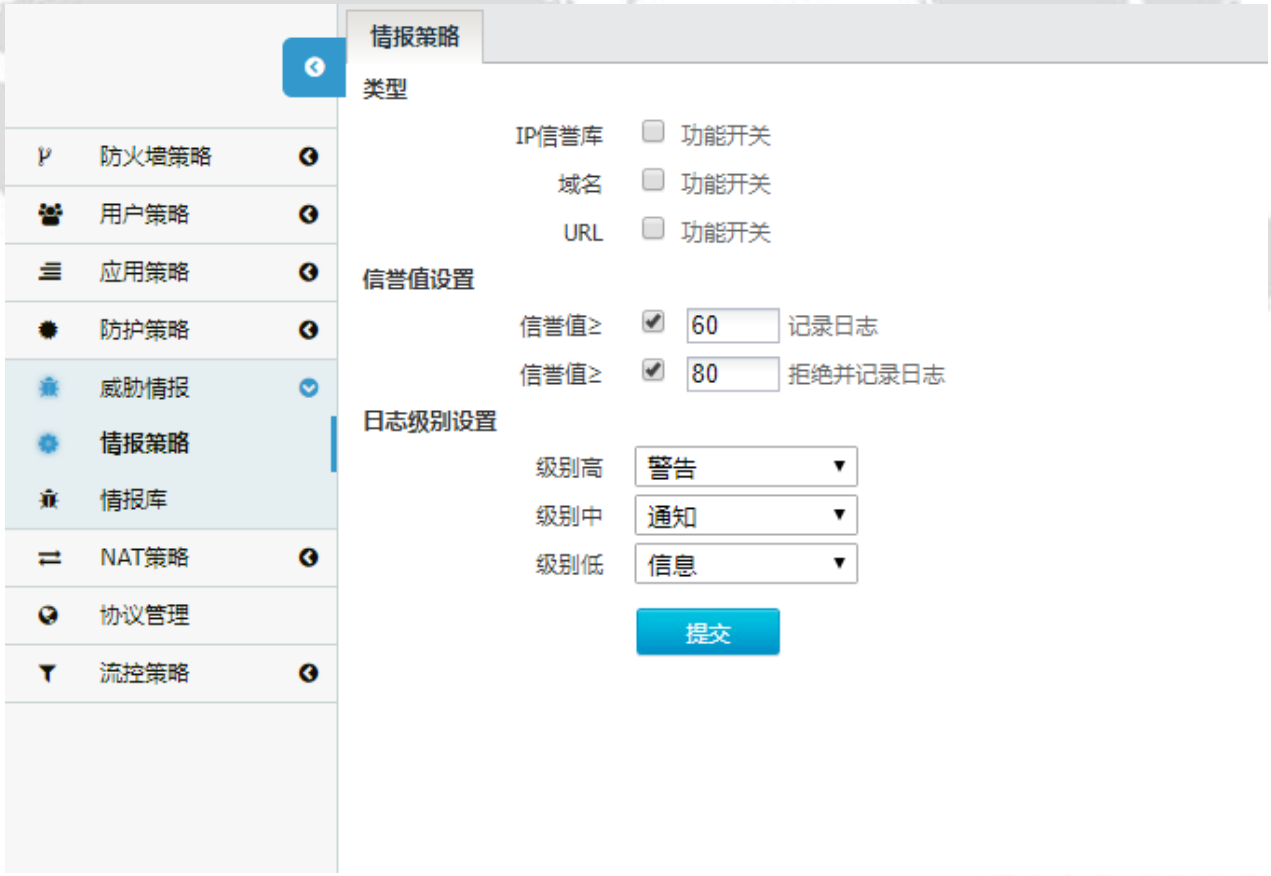
33.1 威胁情报概述

威胁情报也称协同防御，本质是安全共同体内成员共享一份黑名单，可以阻断恶意的 IP、域名和 URL，相比于防火墙的黑名单功能，威胁情报着重检测对已知恶意目标的访问，再根据情报的信誉值作出相应的操作。本机支持 RestfulAPI 自动情报推送功能（仅接收），也可手动添加禁止访问的地址，即时生效，重启情报不丢失。此功能实现的是安全厂家的信息共享，因此也可能会受伙伴推送污染，可通过手动添加高优先级情报强制放通误报流量。

33.2 配置威胁情报

33.2.1 配置情报策略

1、进入**策略>威胁情报>情报策略**



参数说明

IP 信誉库 ：禁止访问情报库内 IP 地址。

域名 ：禁止访问情报库内域名，表现为解析 DNS 失败。

URL ：禁止访问情报库内 URL，同时不阻断同一域名下其余访问。
信誉值（记录日志） ：信誉值高于此阈值则记录日志
信誉值（拒绝并记录日志）：信誉值高于此阈值则阻断
级别高 ：高威胁产生日志级别
级别中 ：中威胁产生日志级别
级别低 ：低威胁产生日志级别

2、点击**提交**，完成配置。

33.2.2 配置情报库

进入**策略>威胁情报>情报库**

该处默认显示本地添加情报，“来源”框可以下拉，当收到推送情报时自动将来源加入下拉列表中。

若远端推送情报和本地或者其余远端情报重复，仅信誉值最高的产生效果，信誉值相同则比较优先级，本地优先级高于远端，先推送的高于后推送的。

2、进入**策略>胁情报>报库>定义情报 ，**点击**新建**

参数说明：

类型 ：可选 IP、域名、URL
内容 ：情报内容
信誉值 ：情报的核心属性，对应于情报策略
生效时间：单位为分钟，1-999,999 代表永久
威胁级别：高中低三种，对应产生日志级别

描述 ：描述

点击**提交** ，完成配置。

33.3 配置案例

33.3.1 配置阻断 IP 地址的场景

应用场景：已知一个恶意 IP，使用威胁情报功能阻断内网主机与此 IP 通信。

1、进入**策略>胁情报>情报策略**，勾选 IP 信誉库：

点击**提交。**

2、***策略>情报库>自定义情报：***

点击 **新建:**

类型选择 IP，内容栏填入 IP 地址，确认信誉值大于情报策略的拒绝阈值即可，其余选择默认。点击提交。

33.3.2 配置阻断域名的场景

应用场景：已知一个恶意域名，使用威胁情报功能阻断内网主机解析此域名 IP 地址。

1、进入**策略>威胁情报>情报策略**，勾选**域名**：

2、进入**策略>情报库>自定义情报**，点击**新建**:

类型选择域名，内容填入域名内容，信誉值需大于情报策略配置的拒绝阈值，其余可默认。点击提交。

33.3.3 配置阻断 URL 的场景

应用场景：已知一个恶意 URL，使用威胁情报功能阻断内网主机与此 URL 通信。

1、进入**策略>威胁情报>情报策略，**勾选 **URL：**

点击**提交**。

2、进入**策略>情报库>自定义情报，**点击**新建：**

类型选择 URL，名称填入 URL，确保信誉值大于情报策略拒绝阈值，其余选择默认。点击**提交**。

第34章 配置 NAT

34.1 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。

下一代防火墙提供了源地址转换和静态地址转换功能。

34.2 配置NAT

系统中把 NAT 的配置分为：源地址转换（Source）及静态地址转换（Static）两种类型。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。

提示：

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。

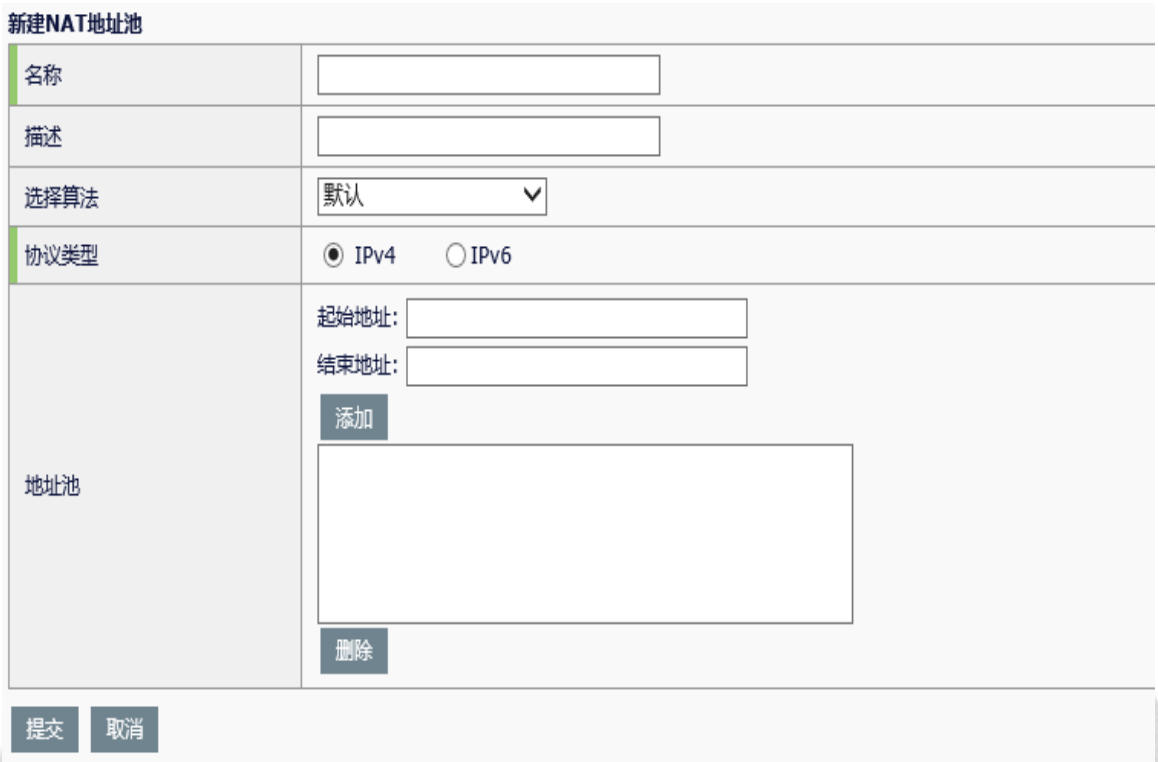
34.2.1 配置地址池(NATPool)

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**策略>NAT 策略>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 64 个字符。

描述：关于该 NAT 地址池的描述，可以是中文，不得超过 128 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，对相同源地址的数据报，会分配相同的地址池地址。

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。

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。IPv6 协议类型的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**。

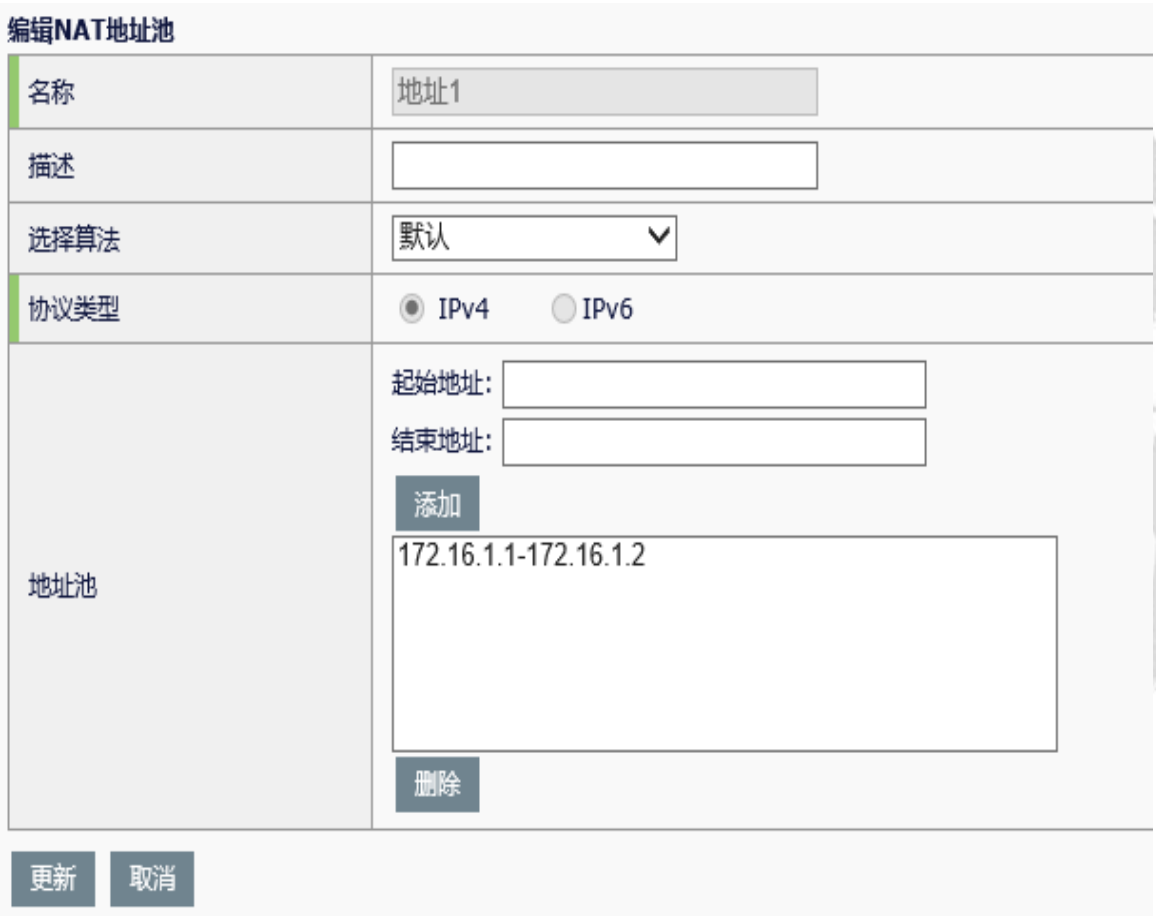
34.2.2 编辑地址池

已经创建的地址池可以编辑修改。

编辑步骤：

1、进入**策略>NAT 策略>NAT 地址池**。

2、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。

3、点击**更新**。

34.2.3 删除地址池

地址池删除步骤：

1、进入**策略>NAT 策略>NAT 地址池**。

2、点击  ，删除选定的地址池。

提示：

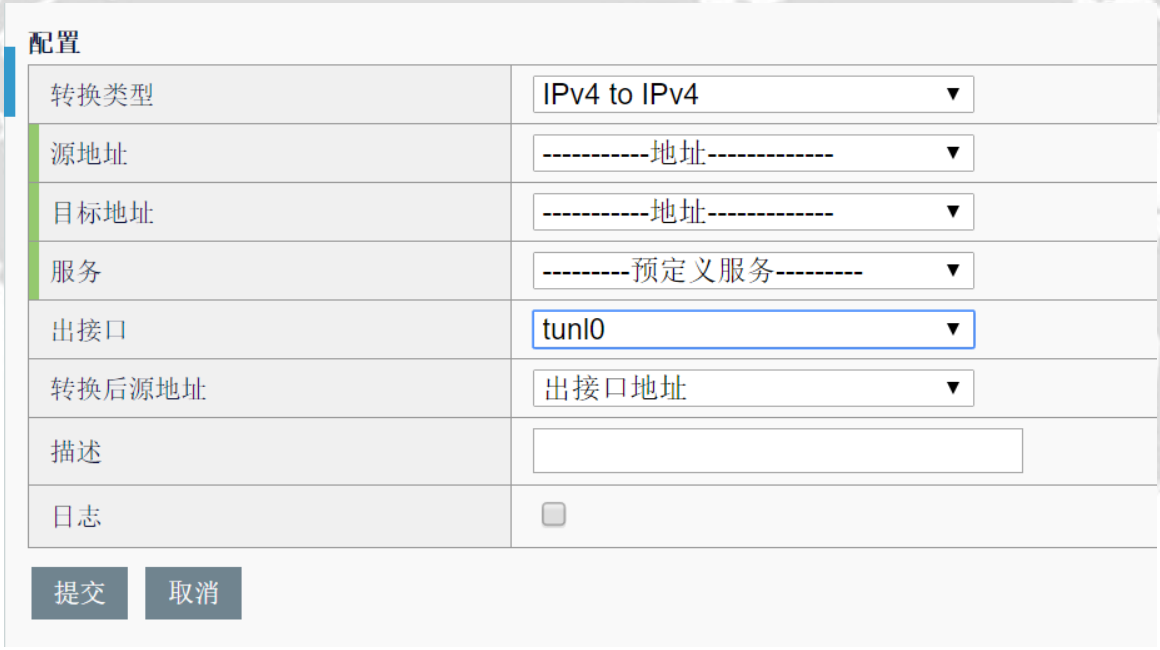
当删除按钮为灰色时，表明该地址池正在被某处引用，不能被删除。

34.2.4 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**策略>NAT 策略>源 NAT**，点击**新建**。



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。选择的地址池类型必须与转换类型一致。

描述：对该转换规则的描述，最长不得超过 128 个字符。

日志：是否需要对该规则启用日志。

2、点击提交。

34.2.5 配置目的地址转换

进入**策略>NAT 策略>目的 NAT**，点击**新建**。

源地址：转换前的源地址对象

目标地址：转换前的目标地址

服务：转换前的服务

入接口：流量进入设备的接口

转换后的目的地址：转换后的目的地址

转换后的端口：转换后的端口号，可选；如果不选则对于非知名端口，转换后会用随机端口。

描述：可以添加备注

日志：勾选后，并且在系统中开启日志过滤，可以记录日志

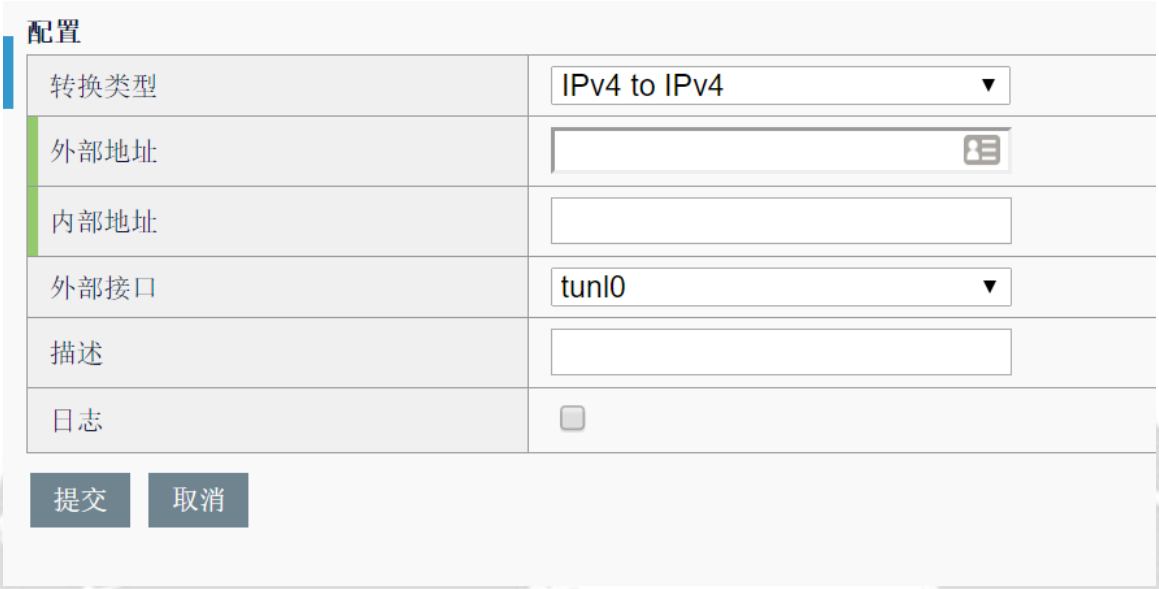
注意！目的 nat 会将匹配到的流中的目的地址全部转换，因此一般匹配规则中不配置 any

34.2.6 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**策略>NAT 策略>静态 NAT**，点击**新建**。



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。

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**。

34.2.7 编辑 NAT 规则

已经创建的 NAT 规则可以编辑修改。

源地址转换的 NAT 规则编辑步骤：

1、进入**策略>NAT 策略>源 NAT**。

#	转换类型	源地址	目标地址	出接口	转换后源地址	日志	描述	操作
1	IPv4 to IPv4	198.16.20.250	any	ge1/7	出接口地址	启用		
1	IPv6 to IPv6	6a8a::2	6a8b::2	ge1/2	6a8b::3/32	启用		

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。

34.2.8 删除 NAT 规则

源地址转换的 NAT 规则删除步骤：

1、进入**策略>NAT 策略>源 NAT**。

点击  ，删除选定的 NAT 规则。

34.2.9 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。

1、进入**策略>NAT 策略>源 NAT**。

源NAT

新建 共2条

#	转换类型	源地址	目标地址	出接口	转换后源地址	日志	描述	操作
1	IPv4 to IPv4	198.16.20.250	any	ge1/7	出接口地址	启用		
1	IPv6 to IPv6	6a8a::2	6a8b::2	ge1/2	6a8b::3/32	启用		

点击规则后的  ：

移动NAT规则

规则ID	2
移动到	(规则ID)
	之前 之后

提交 取消

规则 ID：移动的目标规则 ID。
移动到：指定要移动的位置。

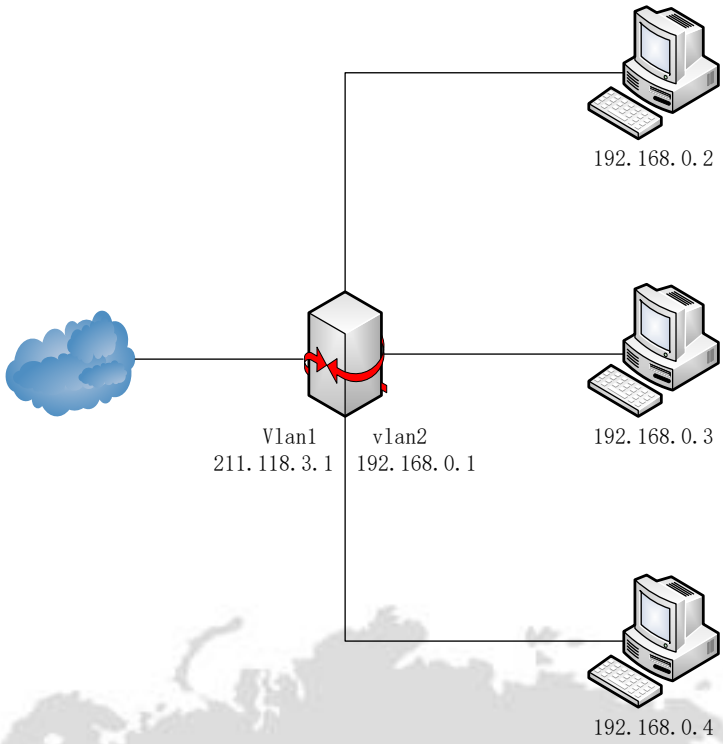

提示：

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，Pv6 to IPv6 类型的规则只能移动到 IPv6 to IPv6 类型的规则前后。

34.3 配置案例

34.3.1 配置源地址转换

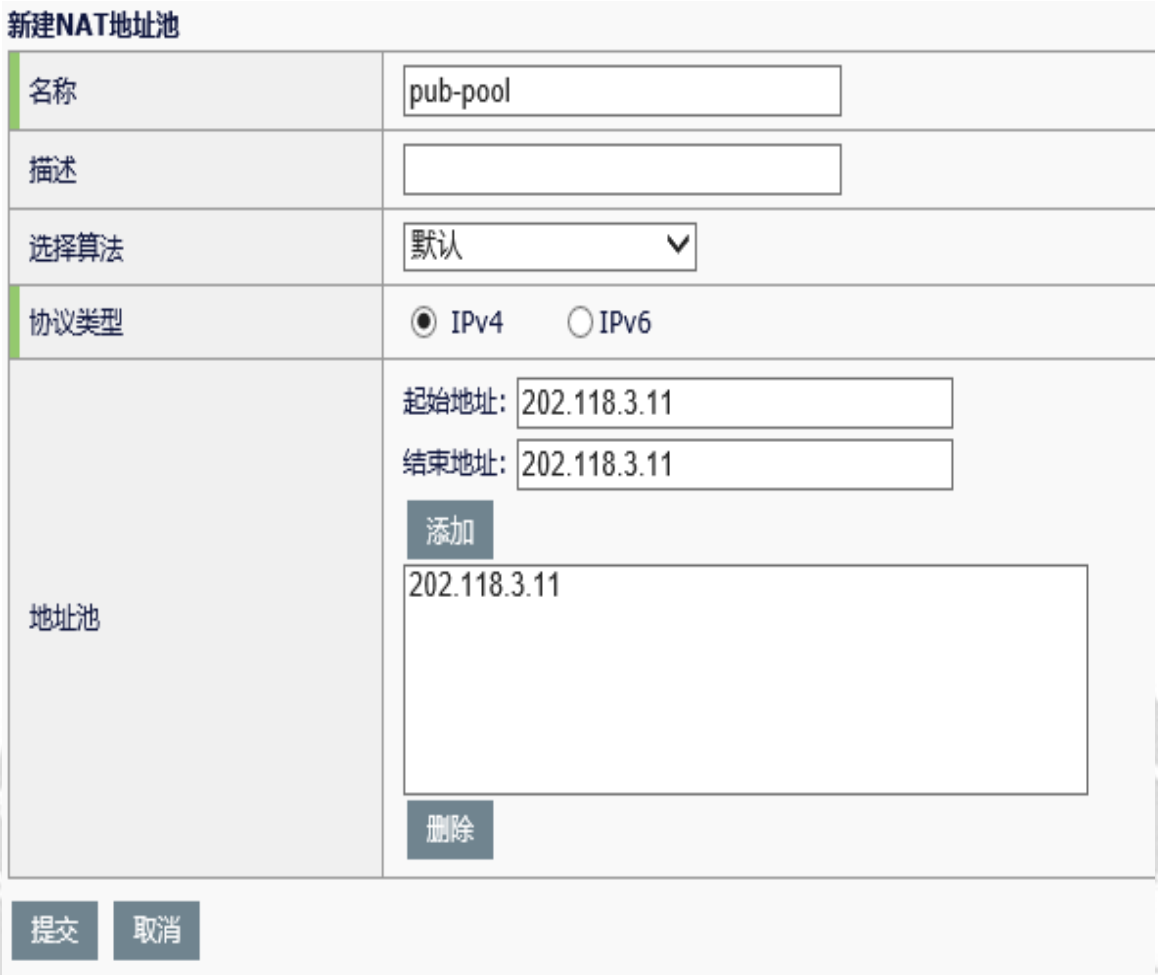
案例描述：
公司内部局域网需要通过应用设备访问外部网络。内网地址为 192.168.0.0/24 网段，公网地址为 202.118.3.1
案例组网图：



配置步骤：

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

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



3、点击**提交**。

4、进入**策略>NAT 策略>源 NAT**，点击**新建**。

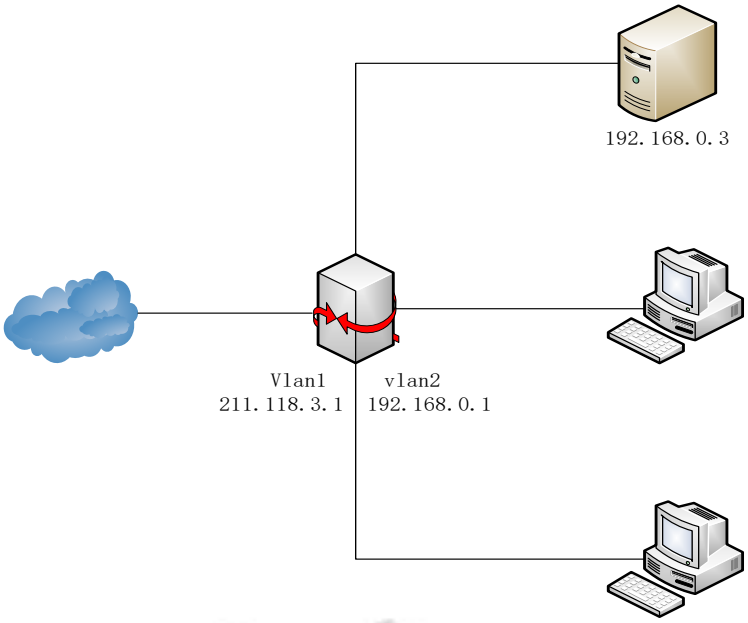
5、点击**提交**。

34.3.2 配置静态地址转换

案例描述：

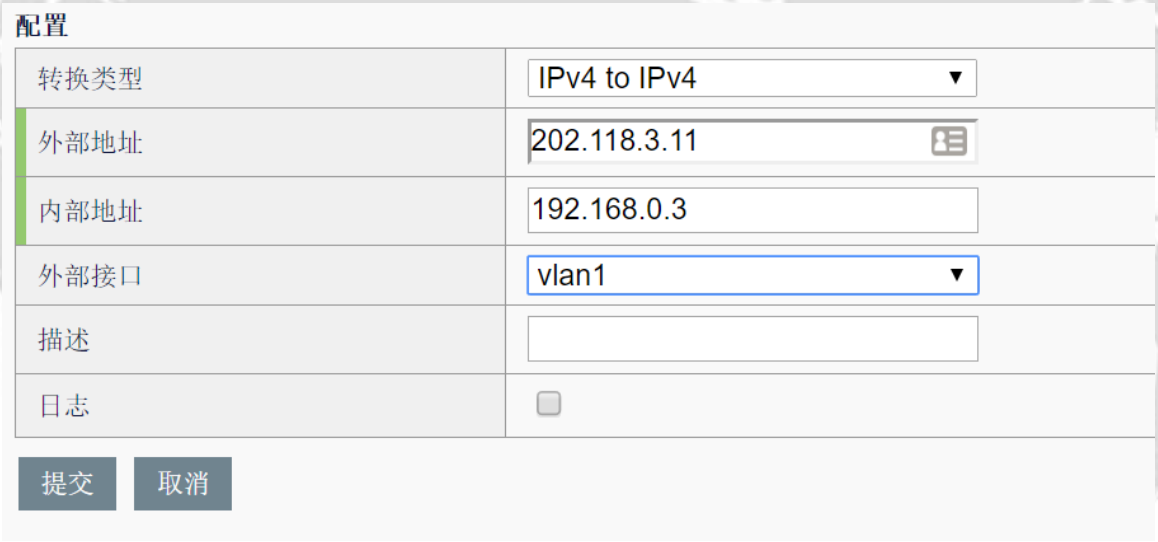
内网有一台服务器对外提供服务，服务器的内网地址为 192.168.0.3，映射的公网地址为 202.118.3.1。

案例组网图：



配置步骤：

1、进入**策略>NAT 策略>静态 NAT**，点击**新建**。



2、点击**提交**，显示如下界面。

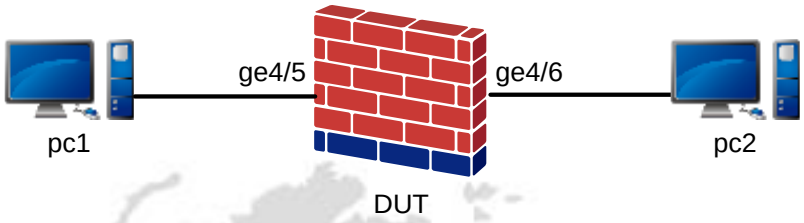
34.3.3 配置源地址转换的透明 NAT

案例描述：

内网有一台服务器对外提供服务，pc1 地址为 192.168.0.10/24，pc2 地址为 192.168.0.100/24。

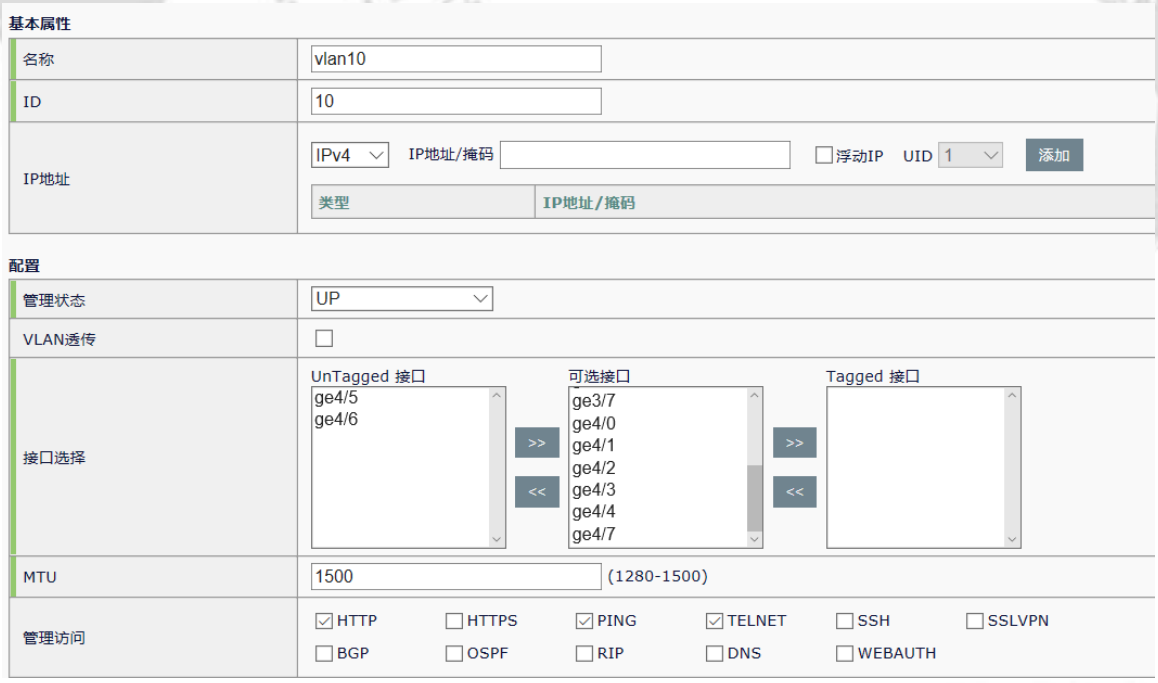
PC1 访问 PC2 时源地址转换成 192.168.0.50

案例组网图：



配置步骤：

1、进入**网络>vlan**，点击**新建**。



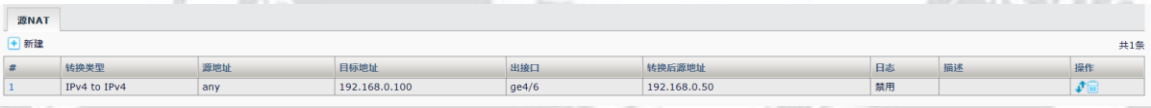
2、进入**策略>NAT 策略>源 NAT**，点击**新建**。

配置

转换类型	IPv4 to IPv4
源地址	any
目标地址	192.168.0.100
服务	any
出接口	ge4/6
转换后源地址	192.168.0.50
描述	
日志	☐

提交 取消

3、点击**提交**，显示如下界面。



4、配置防火墙策略

地址类型	IPv4
入接口	ge4/5
出接口	ge4/6
源地址	any
目的地址	any
服务	any
用户	所有用户
应用	any
时间表	always
动作	PERMIT
日志	☐
源主机连接限制	0 (0-10000000)
源主机连接速率限制	0 (0-10000000)/秒
流量统计	☐
流量镜像	-
描述	

提交 取消

注意：做透明 NAT 时，只与物理接口相关联。

34.4 NAT监控与维护

34.4.1 查看地址池和 NAT 规则

进入**策略>NAT 策略**，可以分别查看已经配置的地址池和 NAT 规则。

34.5 常见故障分析

34.5.1 连接时通时断

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	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。
解决	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。

第35章 协议管理

35.1 管理协议概述

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。

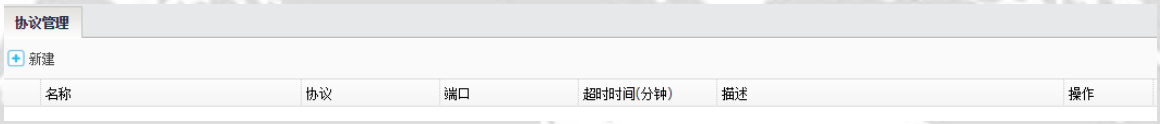
有些应用程序在全连接建立后，报文只会根据实际的数据进行交互，而没有保活机制，往往会导致连接超时删除，后续的数据无法通过设备。

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。

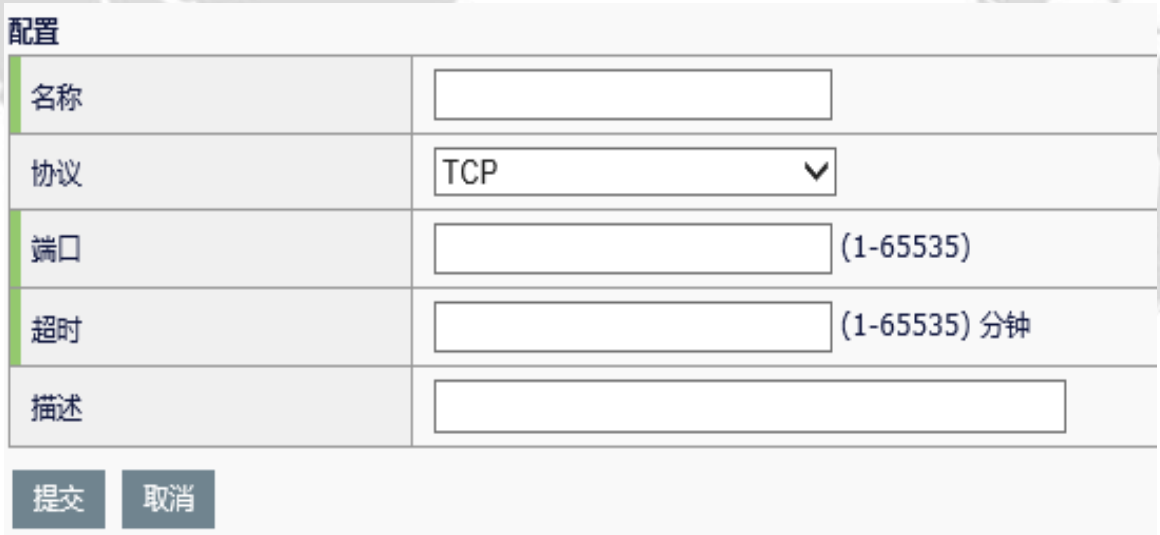
35.2 协议管理配置

配置步骤：

1、进入**策略>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。

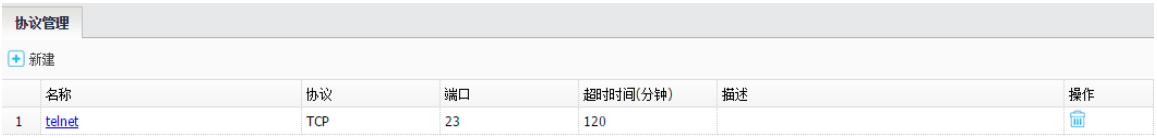
协议：选择该协议管理的协议类型，TCP 或 UDP。

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。

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。



提示：

配置协议管理后，对新建的连接才会生效。

第36章 流量控制

36.1 流量控制概述

下一代防火墙支持流量控制功能，通过选择用户、应用、地址、服务过滤条件，在物理接口上实现对流量准确控制，同时通过设置排除策略，通过地址对源 IP 进行排除，使其不受流量控制影响。详细功能如下：

36.2 线路设置

36.2.1 添加线路设置

1、进入**策略>流控策略>线路设置**，如下图所示：

2、点击**新建**，创建线路如下图所示：

启动：该条线路是否启用

通道名称：所创建线路的名称

绑定接口：绑定需要进行流量控制的接口

带宽管理（出）：对出带宽进行限制，范围为 8kb~10Gb

带宽管理（入）：对入带宽进行限制，范围为 8kb~10Gb

3、点击**提交**完成线路设置。

注意：

一个接口只能绑定一条线路，出方向和入方向可同时开启。

36.2.2 修改线路设置

1、进入**策略>流控策略>线路设置**，查看已经创建的线路通道：

2、点击 进行修改：

3、点击**更新**完成修改。

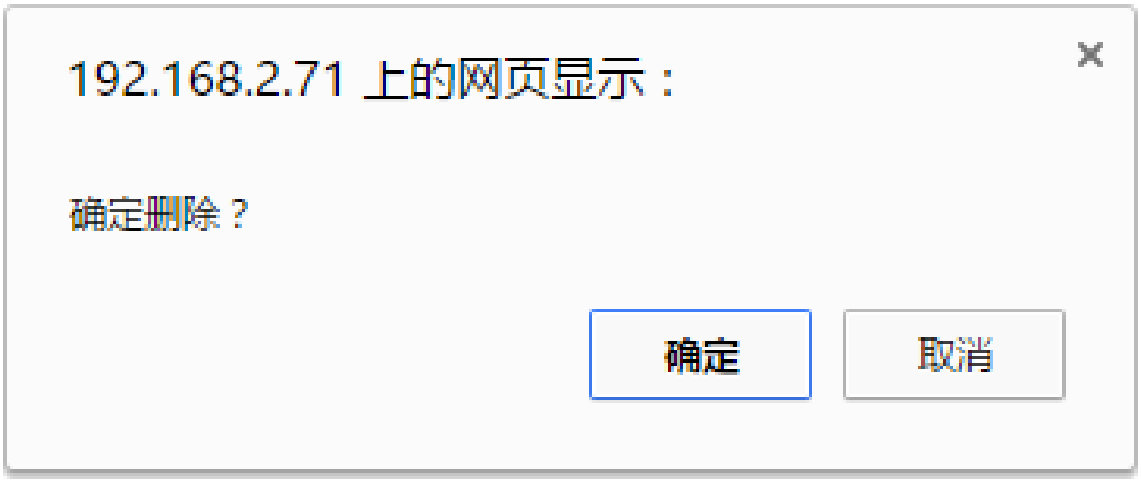
提示：

修改线路时，通道名称不能修改。

36.2.3 删除线路通道

1、进入**策略>流控策略>线路设置**，如下如所示：

2、点击 删除线路通道，如下图所示：



3、点击**确定**删除。

36.3 流量控制

36.3.1 新建流量控制策略

1、选择线路名称，点击**新建**，创建流量控制通道：

启动：该条线路是否启用

名称：所创建子通道的名称

级别：向父节点申请带宽的优先级

带宽设定

最大带宽（出）：该通道的最大出带宽，范围为 8kb~10Gb，小于父节点带宽

上行保障带宽：该通道的最低保障出带宽，范围为 8kb~10Gb，小于该通道的最大带宽

最大带宽（入）：该通道的最大入带宽，范围为 8kb~10Gb，小于父节点带宽

上行保障带宽：该通道的最低保障入带宽，范围为 8kb~10Gb，小于该通道的最大带宽

每个 IP 限速

出：选择启用后，可配置范围为 8kb~10Gb，小于该通道最大出带宽

入：选择启用后，可配置范围为 8kb~10Gb，小于该通道最大入带宽

匹配条件

匹配用户/组：选择启用后，可选择已经创建的用户或用户组，默认为 any

匹配应用：选择启用后，可以选择应用、应用分类、应用组，默认为 any

服务：选择匹配的服务，默认为 any

地址：选择匹配地址对象，默认为 any

时间：选择匹配时间表，默认为 always

2、点击**提交**，完成创建流量控制策略。

提示：

最大带宽的输入受父节点控制，如果父节点未启用，则不可编辑。

匹配条件中，匹配地址为源地址，是 SNAT 之前的地址。

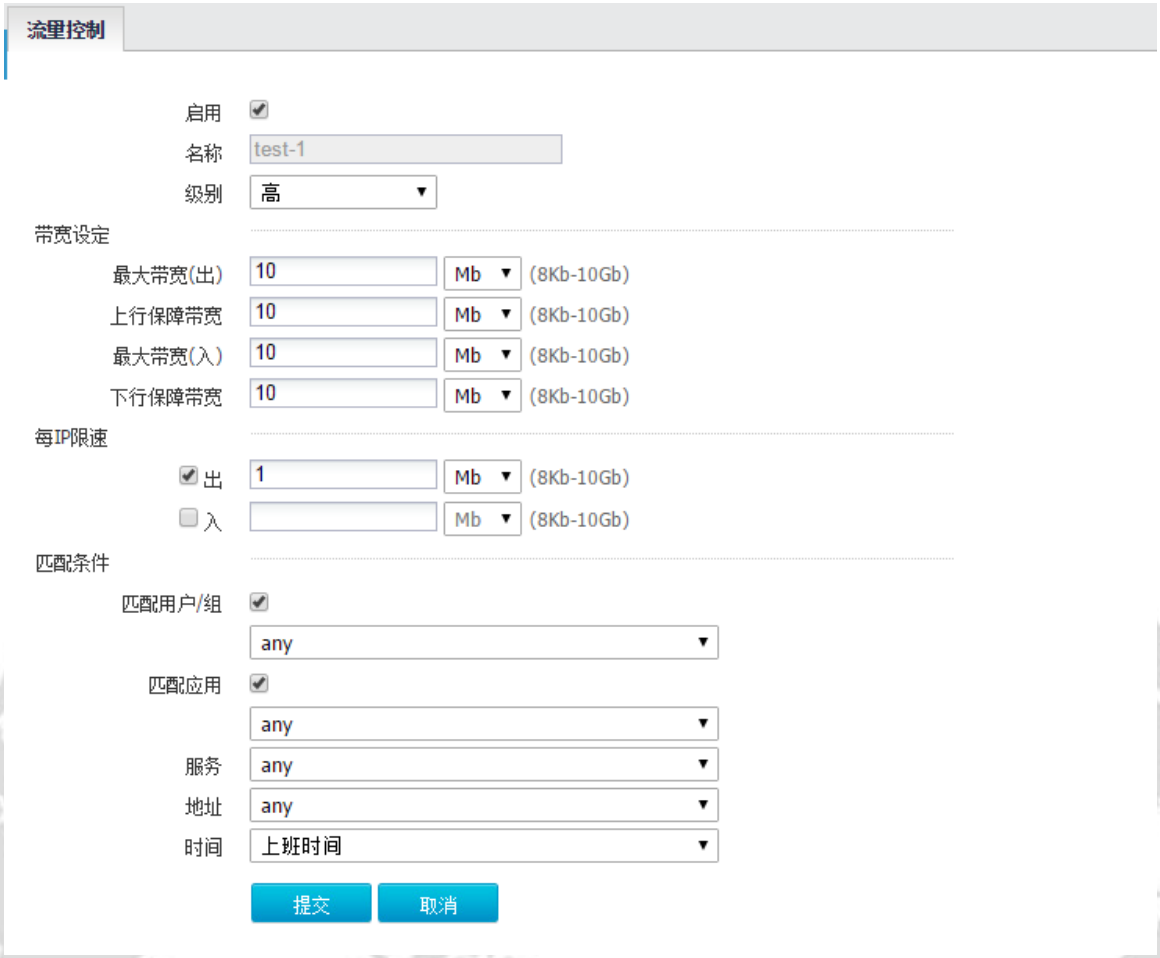
Qos 线路最多支持 4 层嵌套。

最大保障带宽为该线路的最低保障带宽，多通道同时匹配是，优先级高的通道保障带宽优先保障。

36.3.2 修改流量控制策略

1、进入**策略>流控策略>流量控制**，查看已经创建的流量控制策略：

2、点击 进行修改：



3、点击**更新**完成修改。

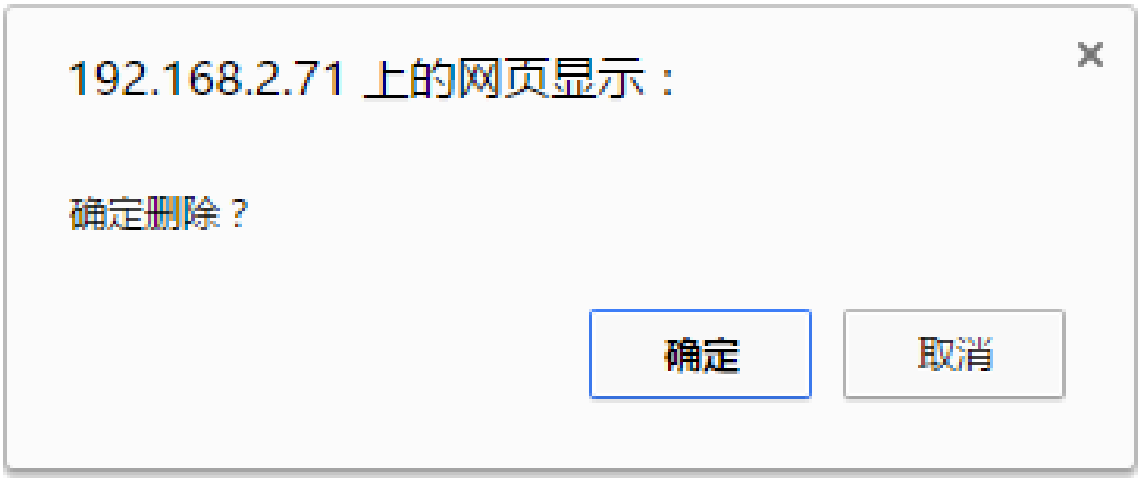
提示：

修改流量控制策略时，通道名称不能修改。

36.3.3 删除流量控制策略

1、进入**策略>流控策略>流量控制页面**，如下如所示：

2、点击删除流量控制策略，如下图所示：



3、点击**确定**删除。

36.4 流量监控

36.4.1 查看流量监控

1、进入**策略>流控策略>流量监控**，查看已经创建的通道流量情况：

线路名称	带宽管理(出)				带宽管理(入)				优先级	状态
	配置保障带	生效保障带	最大带宽	实时速率	配置保障带	生效保障带	最大带宽	实时速率		
1	↑6.00M	↑6.00M	↑6.00M	0(b/s)	↓6.00M	↓6.00M	↓6.00M	0(b/s)	-	
• 6	↑6.00M	↑5.00M	↑6.00M	0(b/s)	↓6.00M	↓5.00M	↓6.00M	0(b/s)	高+	
• 默认通道(名称:def_1)	↑1.20M	↑1.00M	↑6.00M	0(b/s)	↓1.20M	↓1.00M	↓6.00M	0(b/s)	低	

2、进入**策略>流控策略>流量监控**，点击**刷新**，实时查看流量信息：

36.5 排除策略

36.5.1 新建排除策略

1、进入**网络>流控策略>排除策略**，点击**新建**，进入排除策略创建页面：

用户：选择需要排除的用户

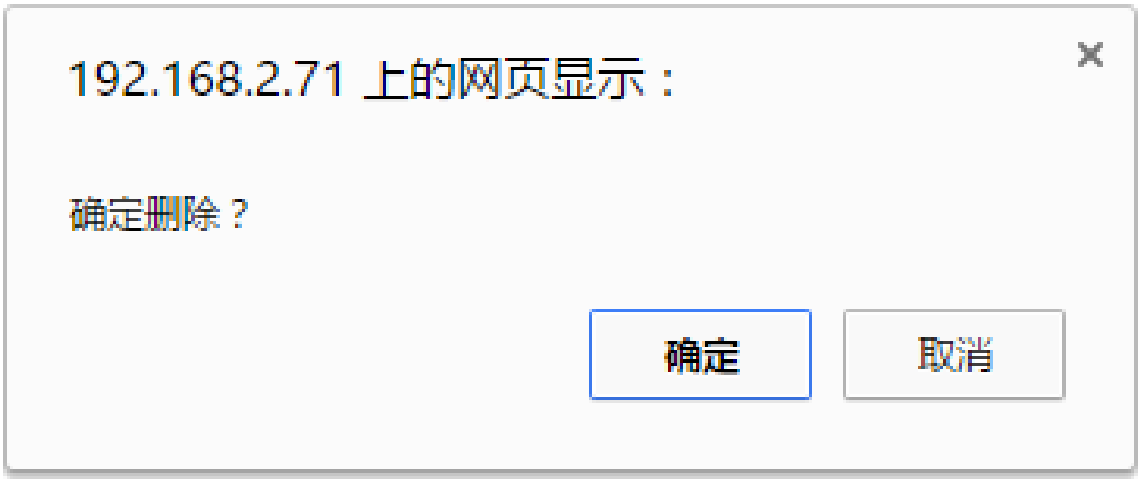
地址：选择排除的地址

2、点击**提交**创建排除策略。

36.5.2 删除排除策略

1、进入**策略>流控策略>排除策略**，查看排除策略列表：

2、点击  删除排除策略，如下图所示：



3、点击**确定**完成删除。

第37章 系统设置

37.1 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：配置设备管理 IP，主机名称，管理员登录限制、web 配置实时保存。

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。

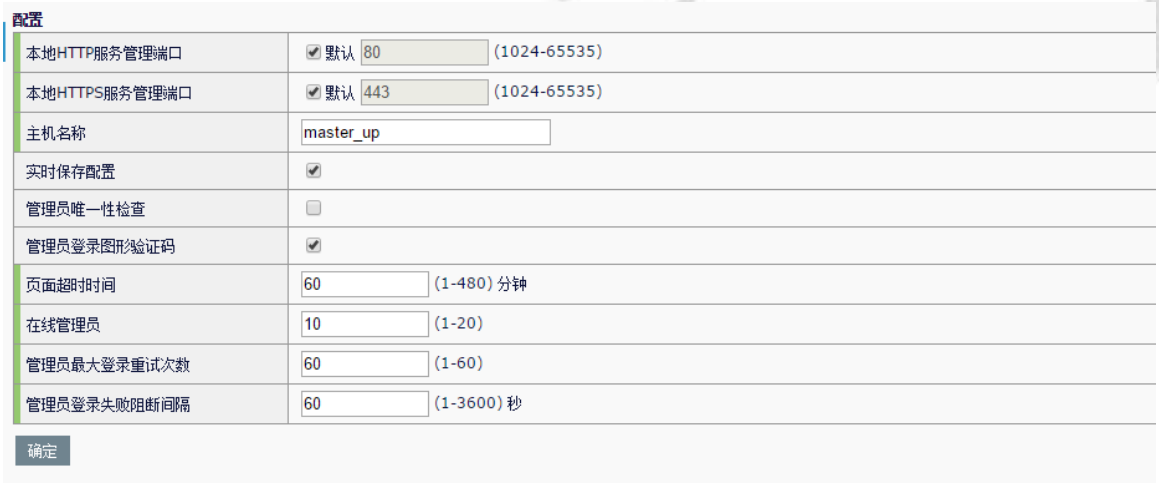
设备重启：可以重启设备或者恢复出厂配置并重启设备。

37.2 配置说明

37.2.1 配置设备

配置步骤：

1、进入**系统>系统设置>设备**



IP 地址：设备的管理地址，即 mgt 接口地址。

IPv6 地址：设备的管理 IPv6 地址，即 mgt 接口 IPv6 地址。

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。

主机名称:设备的名称。

实时保存配置:选择此项后，web 上的配置可以实时保存。

管理员唯一性检查:选择此项后，一个管理员只能在一台 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。

在线管理员：最多可以同时登录的管理员个数。

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。

配置步骤：

2、配置 **IP 地址**该地址作为设备的管理地址，用来 http/https/telnet/ssh 访问。

3、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。**

4、配置**主机名称**，默认为 host。

5、如果需要实时保存配置，勾选**实时保存配置**。

6、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**。

7、输入**页面超时时间**，默认为 10 分钟。

8、输入**在线管理员**个数。

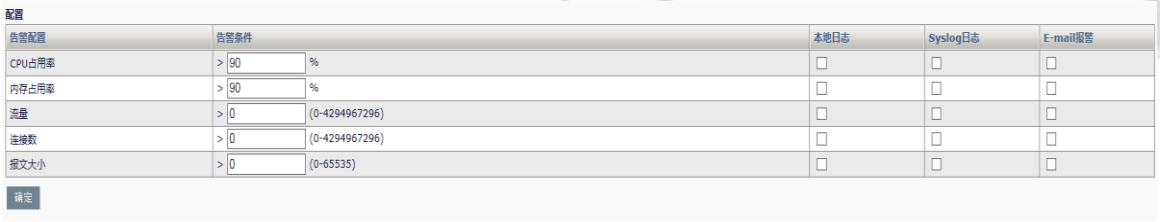
9、输入管理员最大登录重试次数。

10、输入管理员失败登录阻断间隔。

11、点击**确定**。

37.2.2 系统监控

进入**系统>系统维护>系统监控**



此界面可以设置 CPU 占用率及内存占用率的阈值，并可配置当达到阈值后，产生告警日志，该告警日志默认 5 分钟发送一次。

配置步骤：

1、输入 cpu 告警阈值，指业务核平均使用率。

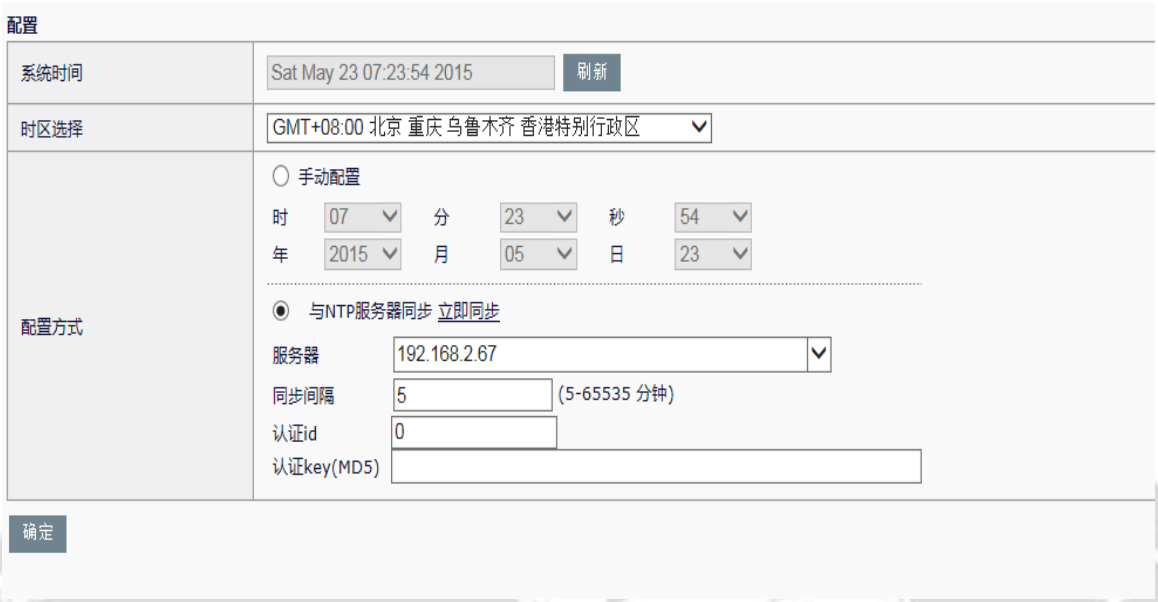
2、输入内存告警阈值，指共享内存使用率。

3、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。

4、点击**确定**。

37.2.3 时间配置

进入**系统>系统设置>时间设置**



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。

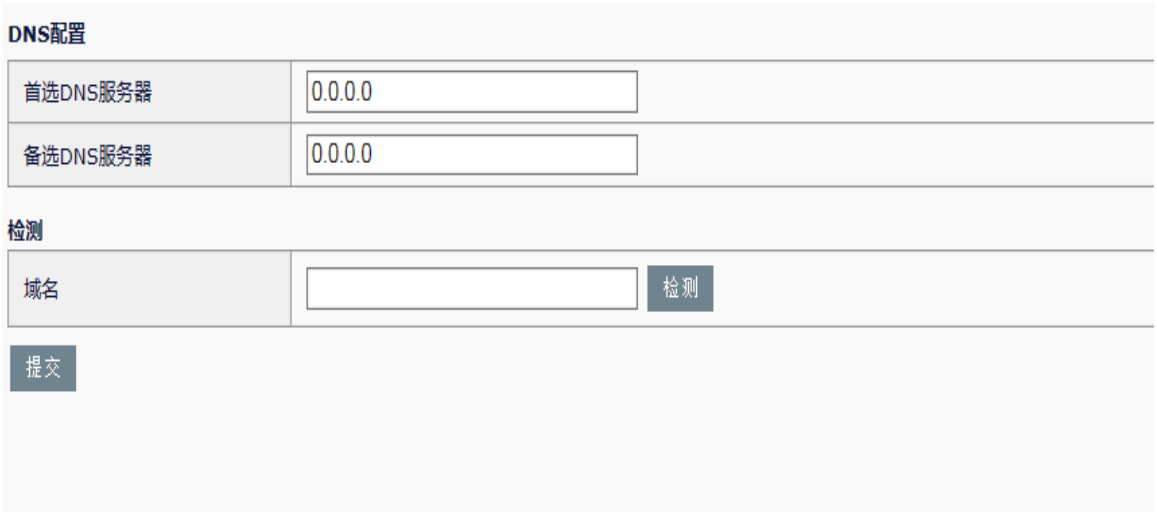
2、手动配置时，用户自己设定具体的时间。

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)配置下节描述的 DNS 配置。

4、点击**确定**。

37.2.4 DNS 配置

进入**系统>系统设置>DNS**



首选 DNS 服务器: dns 服务器地址。

备选 DNS 服务器: dns 服务器地址。

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或默认路由到 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。

37.2.5 配置文件

进入**系统>系统设置>配置文件**

系统配置导入: 选择配置文件导入到设备中。

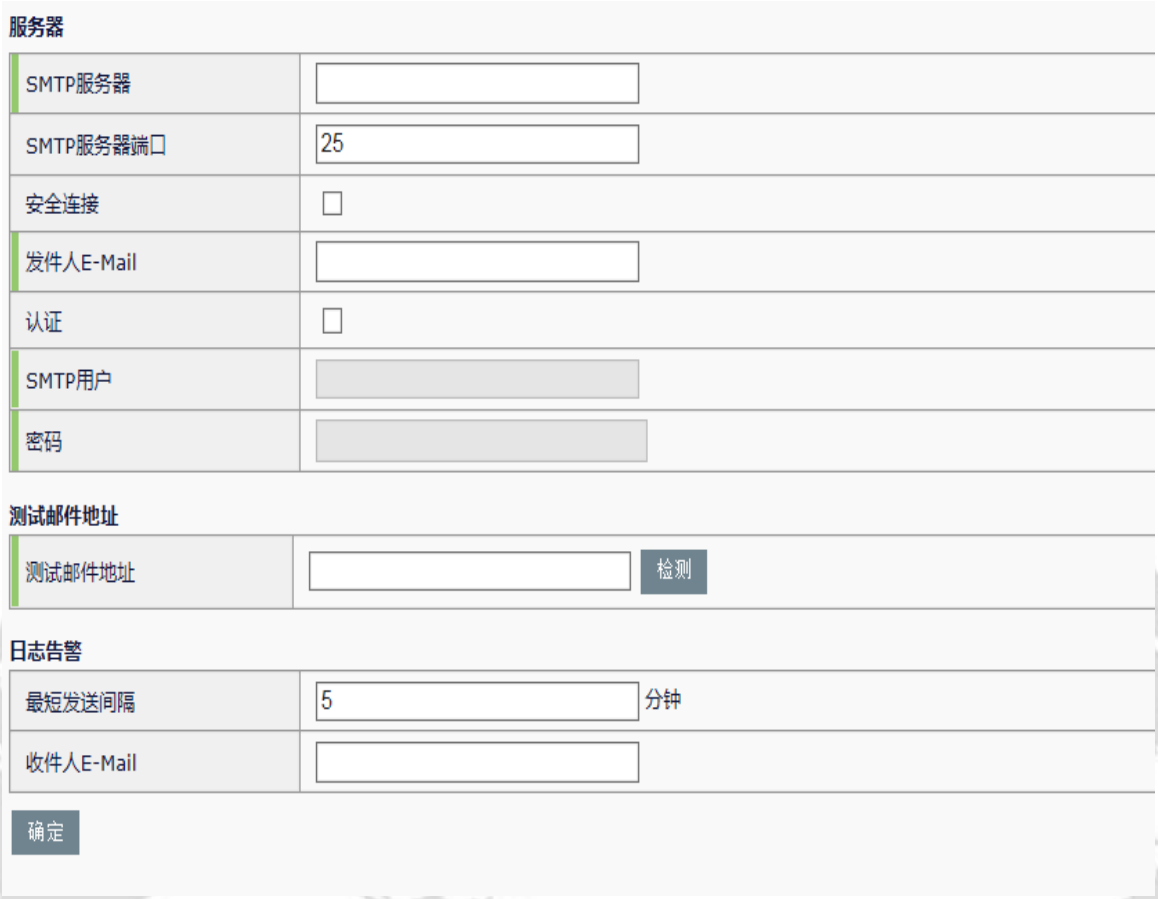
恢复备份配置到主配置文件: 设备内的备份配置覆盖主配置。

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。

37.2.6 告警邮件配置

进入**系统>日志设定>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**。

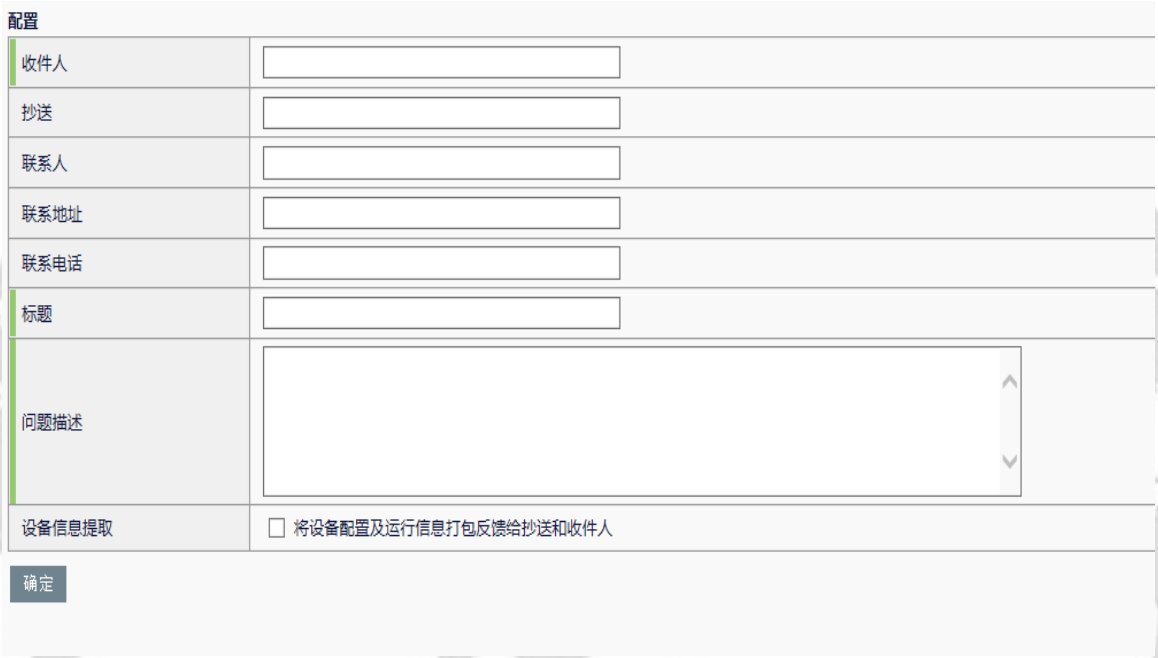
9、填写日志信息收件人 E-Mail。

10、点击**确定**。

37.2.7 信息反馈

配置步骤：

进入**系统>系统维护>信息反馈**



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。

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、点击**确定**。

37.2.8 升级与重启

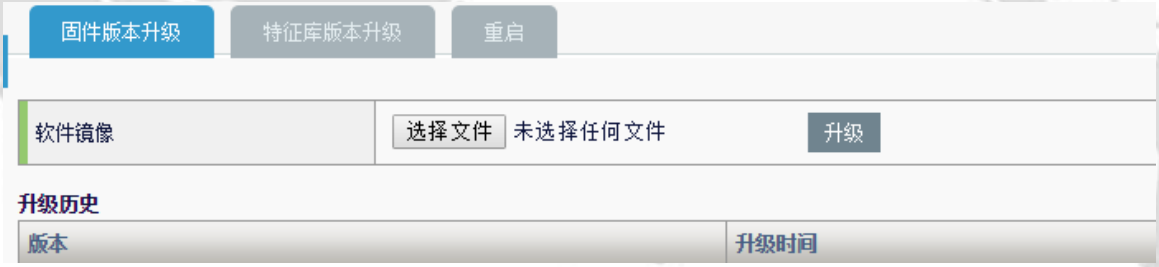
进入**系统>系统设置>升级与重启>重启**

该界面可以重启设备或者恢复出厂设置并重启设备。

37.3 版本管理

37.3.1 版本管理

1、进入**系统>系统设置>升级与重启>固件版本升级**：



通过浏览选择正确的升级包，点击升级进行版本升级。下方会显示最近的 10 条升级记录。

配置步骤：
2、通过**浏览**选择需要的升级包。
3、点击**升级**。
4、根据弹出的提示框，选择**确定**升级或**取消**升级。

37.3.2 特征库升级

下一代防火墙设备可以手动、自动升级应用特征库版本。

该特征库是“应用控制”的基础，系统由此可识别出各个具体的应用，具体使用及配置请参阅“应用对象”章节。

提示：

设备出厂时，已经默认加载了基础特征库。

1、选择**系统>系统设置>升级与重启>特征库版本升级**，如下图：

手动升级:

选择文件：选中对应的特征库文件，点击“**升级**”即可。

注意：

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。

星期数: 按星期定期自动升级。

日期: 按每月日期自动升级。

时间: 每次自动升级的当天时间。

2、配置好后，点击**提交**。

37.4 SNMP

37.4.1 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：输入 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。

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。

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。

2、勾选启用 SNMP 代理。

3、选择是否启用 **v1、v2c、v3** 版本的 SNMP

4、输入位置。

5、输入 trap 地址。

6、输入 SNMP 团体。

7、点击确定。

8、如果是 V3 版本需要用户认证，点击**新建**。

9、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。

10、点击更新。

37.4.2 配置案例

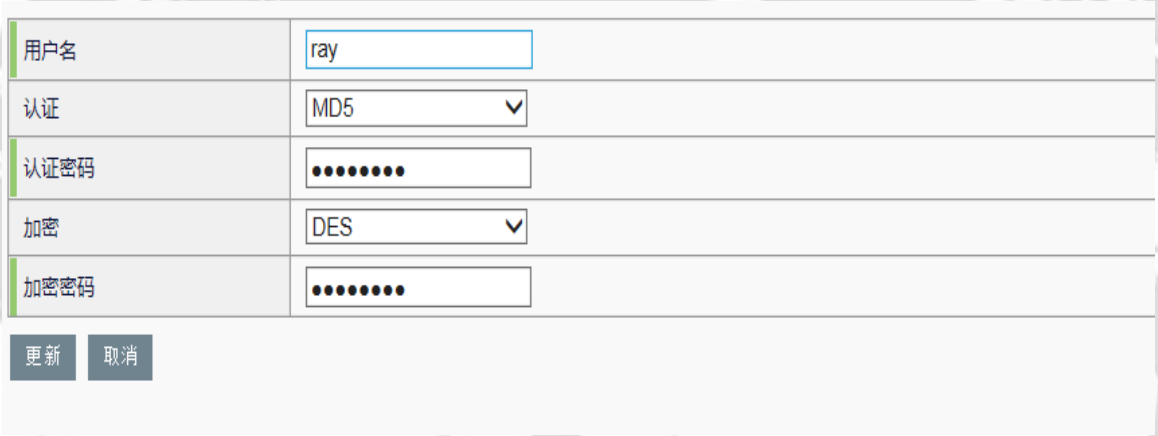
配置案例：配置 SNMP

案例描述:

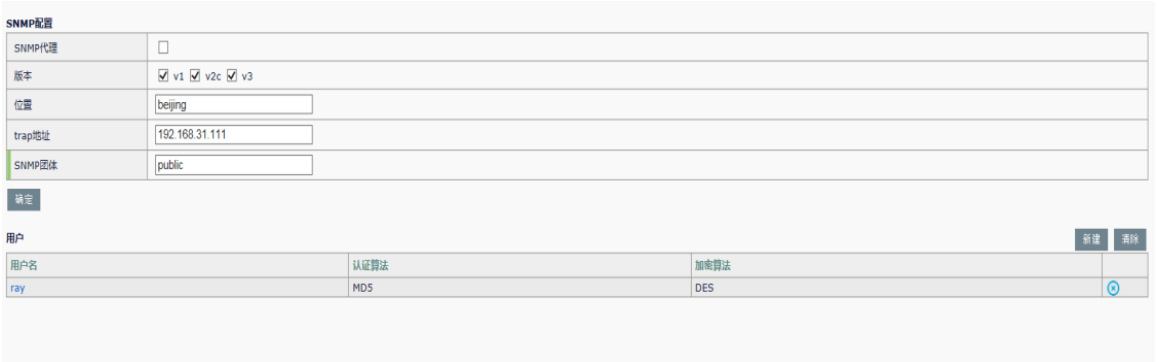
设置启动 snmp 代理，物理位置为 beijing，trap 地址为 192.168.31.111，snmp 团体为 public，建立一个 V3 认证用户，用户名为 ray，采用 MD5 认证算法和 DES 加密算法，认证密码与加密密码均为 1234578。

配置步骤：

1、进入**系统>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。

第38章 管理员

38.1 管理员概述

下一代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。

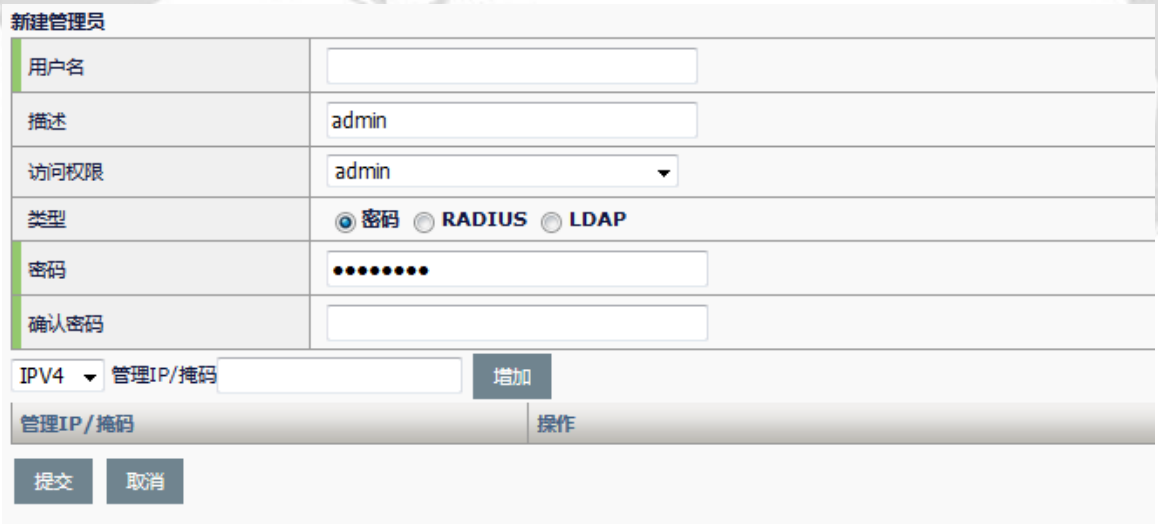
如果选择的是 LDAP，而且配置了 LDAP 支持，用户名和密码与 LDAP 服务器中的用户名和密码相匹配，则认证通过。

38.2 配置管理员

38.2.1 配置管理员

配置用于认证的管理员用户。

进入**系统>管理员设置>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。

管理 IP/掩码：允许哪些网段的用户登录，最多可添加 16 条。

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。

第39章 认证服务器

39.1 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，下一代防火墙将连接 RADIUS 服务器以获得认证。

39.1.1 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：

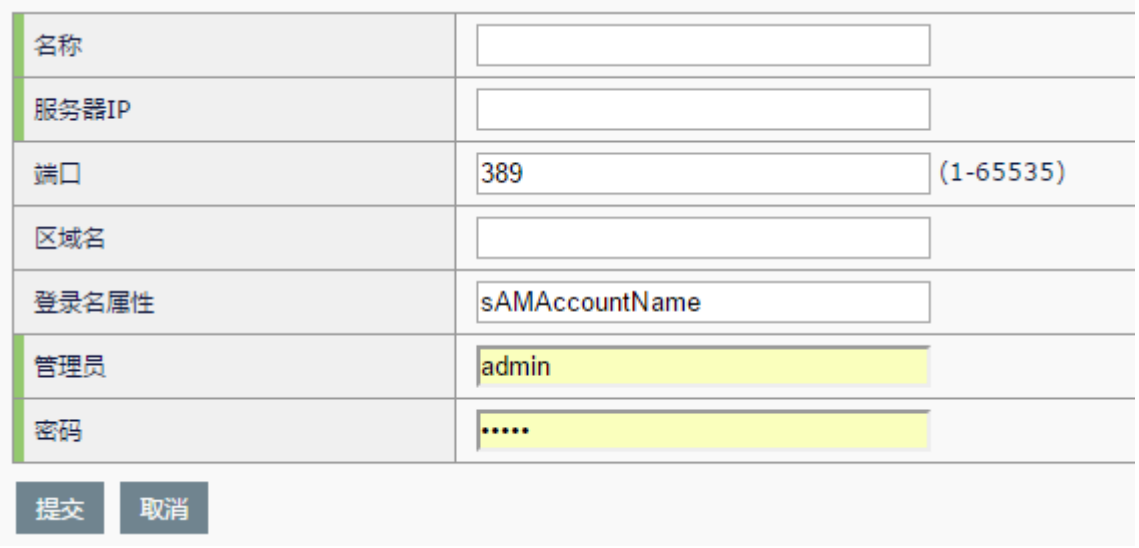
点击**认证服务器**下的 **RADIUS** 配置标签页，显示当前系统中配置的所有 RADIUS 服务器。

39.2 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，下一代防火墙将连接 LDAP 服务器以获得认证。

39.2.1 配置 LDAP 服务器

1、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。

提示：

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。

39.3 配置本地认证

39.3.1 配置本地认证

1、进入**对象>认证服务器>本地认证**

用户唯一性检查：用户唯一性检查的配置方式

单一账户登录：同一时间只允许同一账号登录一次

踢出已登录用户：如果新用户登录，老的用户将会被踢下线

禁止同名用户再次登录：如果老用户已经登录，新用户将不能以此用户名登录

允许重复登陆：同一时间允许同一账号登录多次

客户端超时：配置 WEB 心跳间隔时间

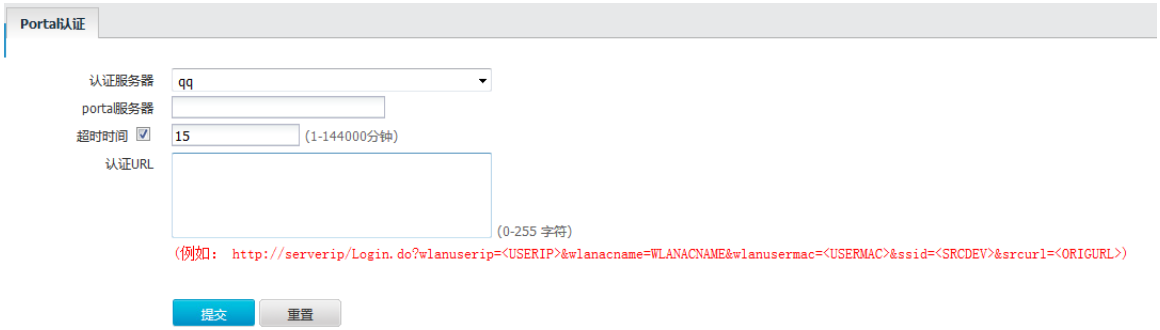
强制重登录时间：WEB 强制重新认证时间

重定向 URL：WEB 认证重定向 URL

39.4 配置portal认证

39.4.1 配置 portal 认证

1、进入**对象>认证服务器>portal 认证**



认证服务器：Portal 认证使用的 radius 服务器或 radius 服务器组名称

Portal 服务器：设置 portal 服务器 ip

超时时间：用户认证的超时时间，在时间段内没有流量设备会强制用户下线

认证 URL：Portal 认证时重定向的 URL

39.5 认证用户监控与维护

39.5.1 查看管理员信息

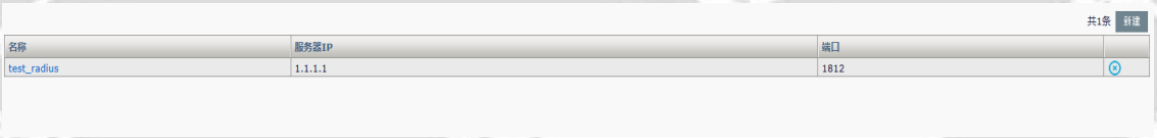
进入**系统>管理员设置>管理员**，查看管理员信息。

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。

39.5.2 查看 RADIUS 服务器信息

进入**系统管理>管理员>认证服务器>RADIUS**，查看 RADIUS 服务器信息。

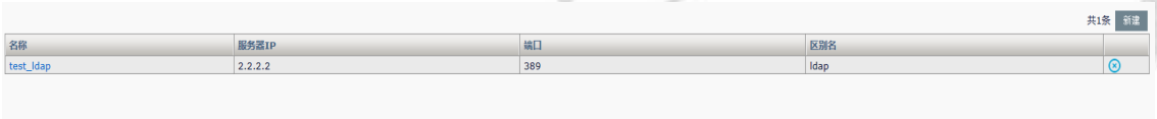


名称	服务器IP	端口	
test_radius	1.1.1.1	1812	

可以查看 RADIUS 服务器名称，服务器 IP，端口。

39.5.3 查看 LDAP 服务器信息

进入**系统管理>管理员>认证服务器>LDAP**，查看 LDAP 服务器信息。



名称	服务器IP	端口	区别名	
test_ldap	2.2.2.2	389	ldap	

可以查看 LDAP 服务器名称、服务器 IP、端口、区别名。

39.6 常见故障分析

39.6.1 故障现象：系统用户使用 radius 认证失败

现象	使用 radius 用户登陆下一代防火墙系统失败。
分析	密码错误 RADIUS 服务器配置错误（比如：共享密钥，IP 等）

	RADIUS 服务器连接不上（比如：PING 不通） RADIUS 服务器上没有这个用户
解决	检查用户密码，输入正确的用户名和密码 修改该 RADIUS 服务器的配置 首先确保下一代防火墙和 RADIUS 服务器能通讯，能 PING 通 为该 RADIUS 服务器添加该用户

第40章 高可用性

40.1 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，下一代防火墙支持两台设备以主-备或主-主两种工作模式运行，满足不同的组网需要。

在主-备工作模式下，只有状态为“主”的设备转发流量，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，以及设备上的相关配置，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。

两台设备通过用户设置 IP 地址发送心跳报文来检测对端设备的工作状态，同时下一代防火墙产品支持另外三个附加因素可选项：“故障监控”，“链路聚合监控”和“健康检查监控”作为切换条件。正在工作中的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，当链路正常的情况下，由指定的主备配置决定主备状态。

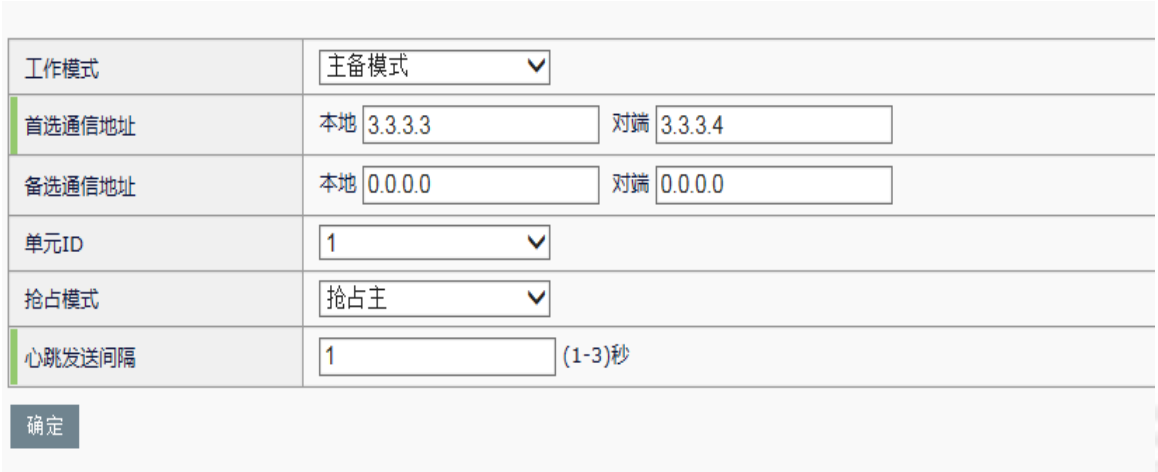
本章涉及 HA 功能的配置，阐述了如何通过 Web 管理界面配置 HA，实现 HA 功能。

40.2 HA基本配置

下一代防火墙设备 HA 的基本配置包括工作模式，心跳通信地址、单元 ID 等。

配置步骤：

1、进入**系统>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 1 秒。

2、点击**确定**。

注意：

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。

主主模式下，两台设备的单元 ID 必须指定为不同。

主备模式下，两台设备的抢占模式必须成对配置。

两台设备的心跳发送间隔必须配置为相同。

40.3 配置配置同步

下一代防火墙设备 HA 功能可实现配置的手动同步，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：

1、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。

配置自动同步：启用后，设备会将 web 页面的操作自动同步到另一台设备上。

2、点击**确定**。

注意：

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。

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。

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。

两台设备中，只要有一台启用实时监测即可。

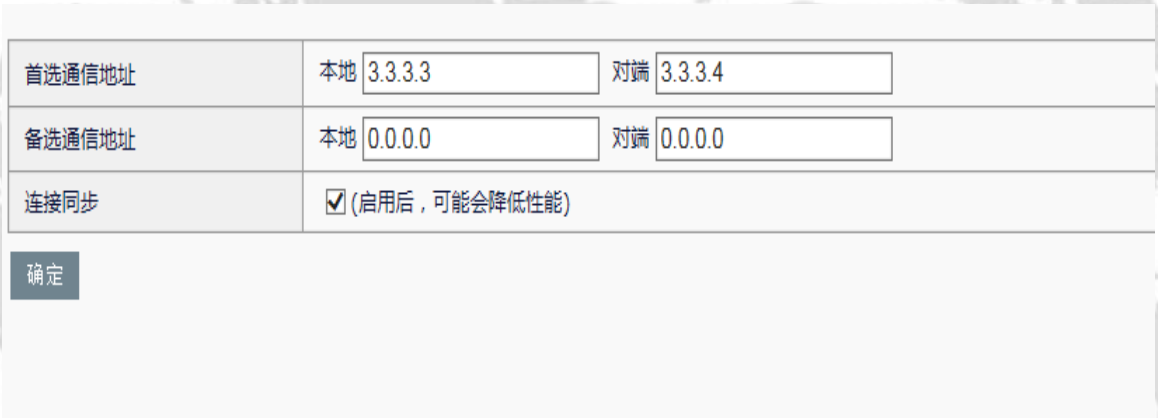
配置同步功能，不会同步 HA 本身的配置，以及接口、设备 IP 相关的配置。

40.4 配置连接同步

连接同步包括四层流同步，七层会话保持同步，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。

配置步骤：

1、进入**系统>高可用性>连接同步**，进入连接同步界面。



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：同上

对端：同上

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。

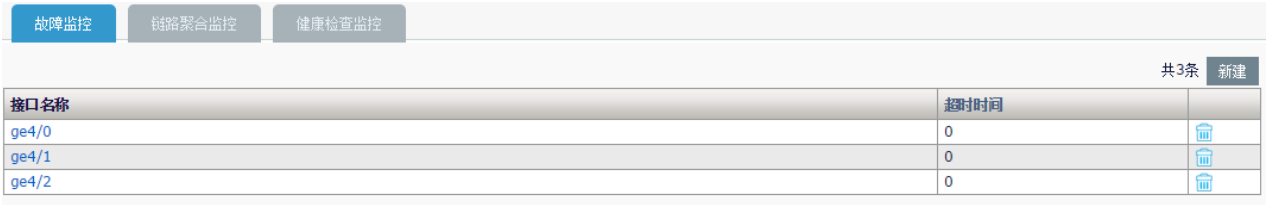
2、点击**确定**。

40.5 配置故障检测

HA 故障检测分接口监控、链路聚合监控和健康检查监控，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。

配置步骤：

1、进入**系统>高可靠性>故障检测**，进入故障检测界面。



点击 **删除**监控。

2、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/donw，引起 HA 状态频繁切换，造成设备不稳定。

3、点击**提交**。

4、进入**系统>高可用性>故障检测**，进入链路聚合监控界面。

点击 **删除**监控。

5、点击新建。

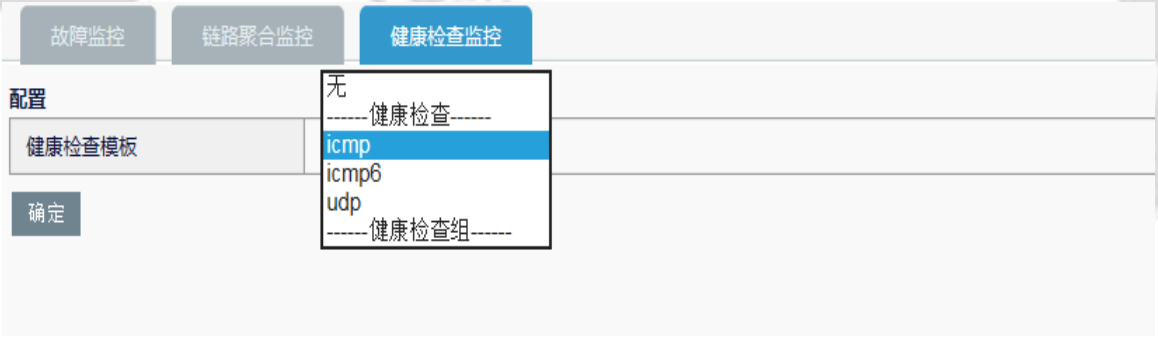
链路聚合：需要监控的链路聚合名称，监控链路聚合接口中的物理接口。

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。

6、点击**提交**

7、进入**系统>高可用性>故障检测**，进入健康检查监控界面。

点击下拉框可以选择并引用已创建的健康检查对象



8、点击**提交**。

40.6 接口联动

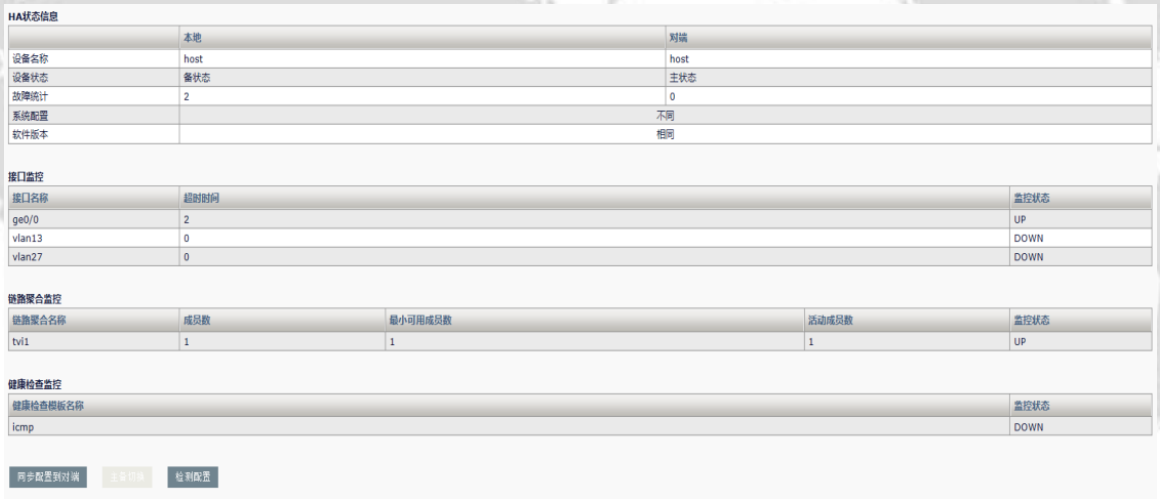
在接口联动组内一个接口 down 掉，组内所有接口都为 down

进入**系统>高可用性>接口联动**，点击**新建**，左侧为待选接口，右侧为选中的接口

40.7 HA状态监控

40.7.1 查看 HA 监控

进入**系统管理>高可靠性>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：

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。

同步配置到对端后，需要重启对端设备，配置才能生效。

主主模式下不支持主备切换。

主备模式下配置了抢占模式，不支持主备切换。

40.8 配置案例

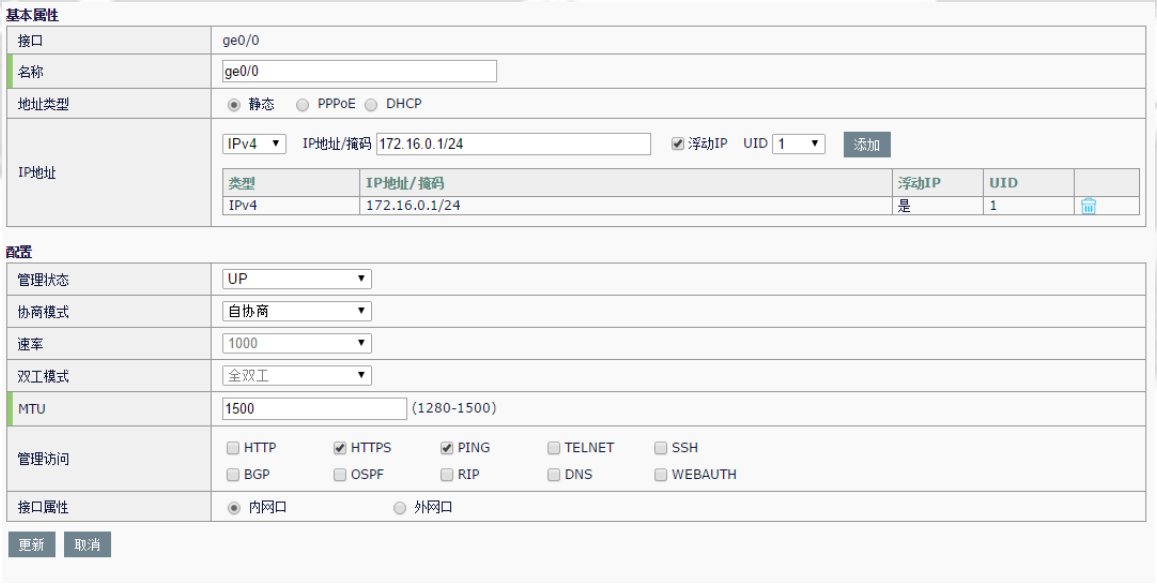
40.8.1 案例 1：配置主备模式基本配置

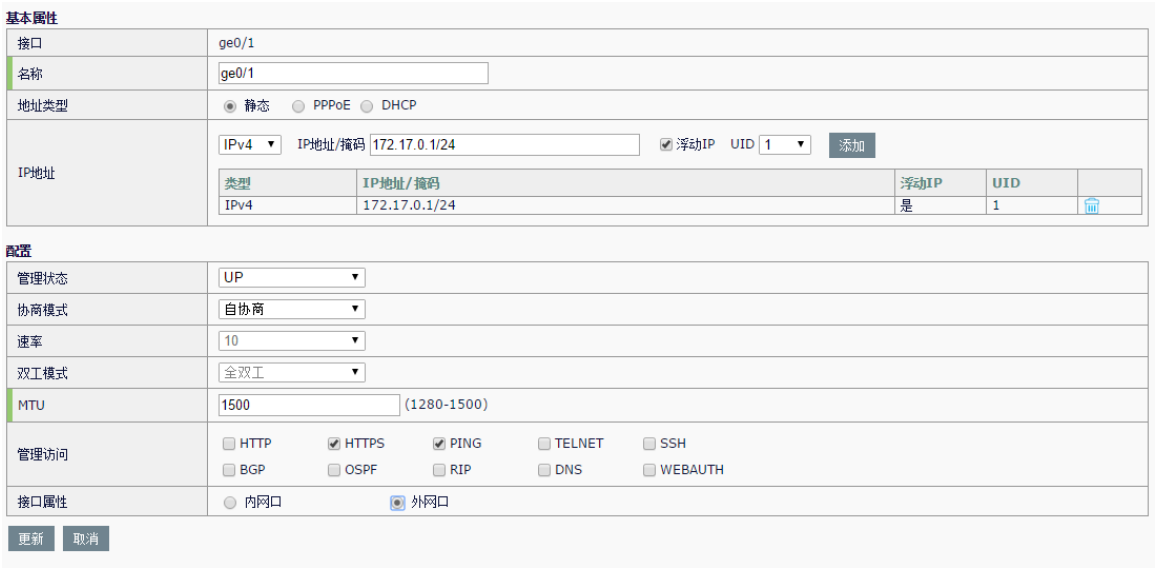
案例描述：

两台设备，host_A,host_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 host_A 为主设备，在 host_A 上完成所有的配置后，再配置 host_B 上 HA 模块相关配置，然后手工同步配置，这样 host_B 上将拥有和 host_A 一样的配置信息。

配置步骤：

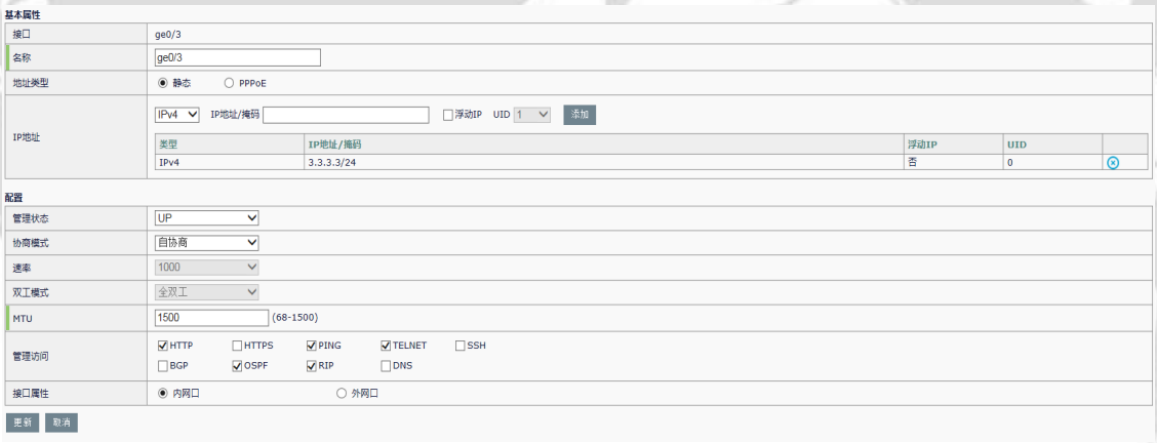
1、配置 host_A 进入网络>接口配置，点击编辑与上下游连接的接口，配置业务转发接口所需的接口 IP。





业务转发接口的 IP 必须配置为浮动 IP，浮动 IP 仅用于 HA 环境下进行业务转发。主备环境下，浮动 IP 在主设备上生效，备设备上浮动 IP 不生效。主备环境下单元 ID 没有意义，所以配置浮动 IP 时 UID 使用默认即可。

2、配置 host_A 进入**网络>接口配置**，点击**编辑** HA 通信接口，配置 HA 所需的接口 IP。

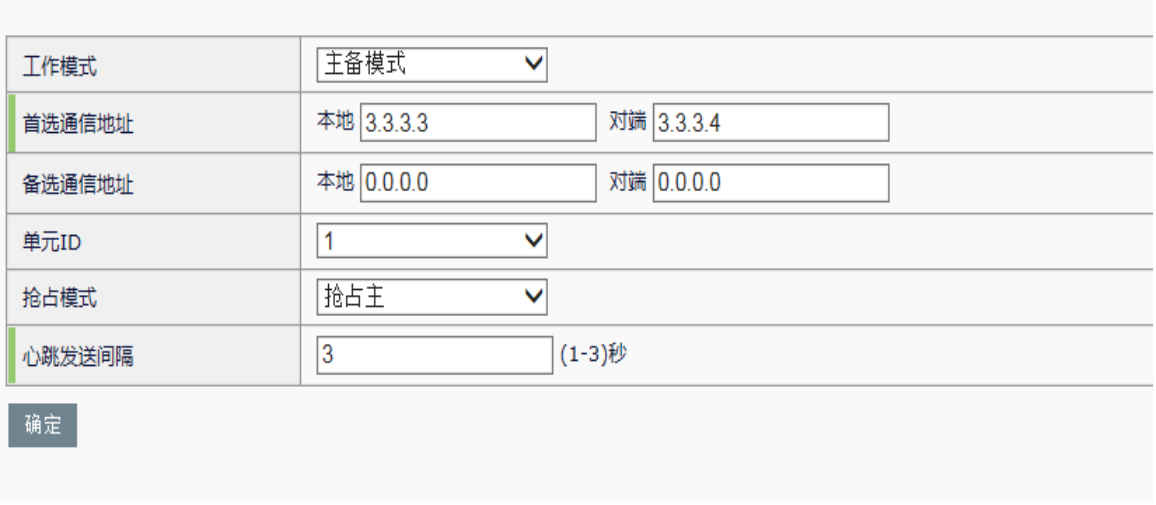


IP 地址：配置 IP 地址 3.3.3.3

掩码：24 位网络掩码，**浮动 IP：**不勾选，其他相关参数请见**网络**具体章节

点击更新，完成新建设备 IP3.3.3.3。

3、配置 host_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 中创建的 3.3.3.3 地址，作为本地通信地址，对端设备需要创建 IP 地址 3.3.3.4。

备选通信地址：为可选配置，本例中仅配置首选通信地址。

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。

4、配置 host_A,进入**系统管理>高可靠性**，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：3.3.3.4。

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。

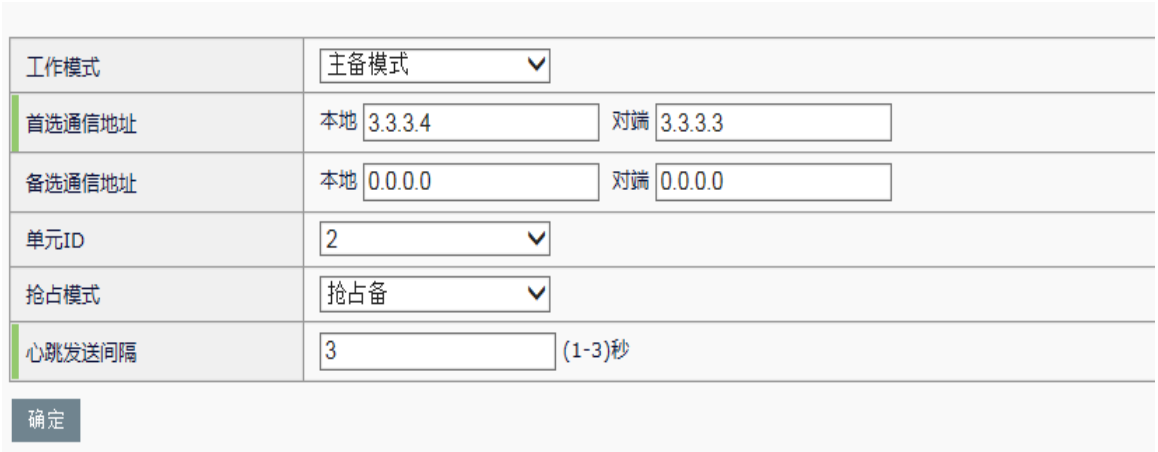
配置自动同步：勾选，自动同步 web 页面操作。

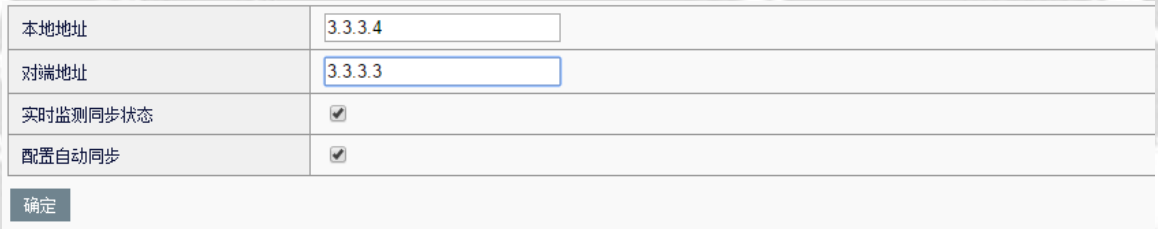
5、配置 host_A,进入**系统>高可用性**，进入连接同步界面。

首选通信地址：配置首选通信地址 3.3.3.3 为本地地址，对端设备需要配置设备 IP3.3.3.4。

备选通信地址：可选配，本实例中没有配置。

6、配置 host_B,配置步骤请参照设备 host_A，这里不再重复介绍，其中 host_B 上的业务口浮动 IP 配置与 host_A 配置一致，以下是设备 host_B 配置完成后 HA 相关的配置页面。

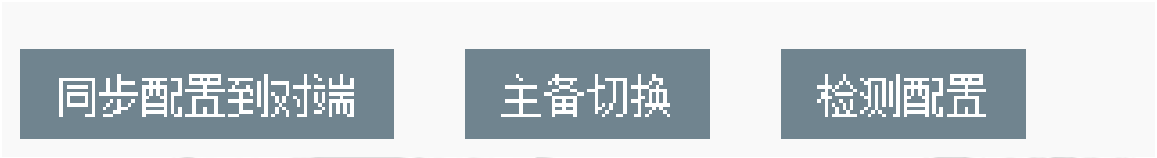




到此 HA 主备工作模式配置完成。

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**系统管理>高可靠性>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。

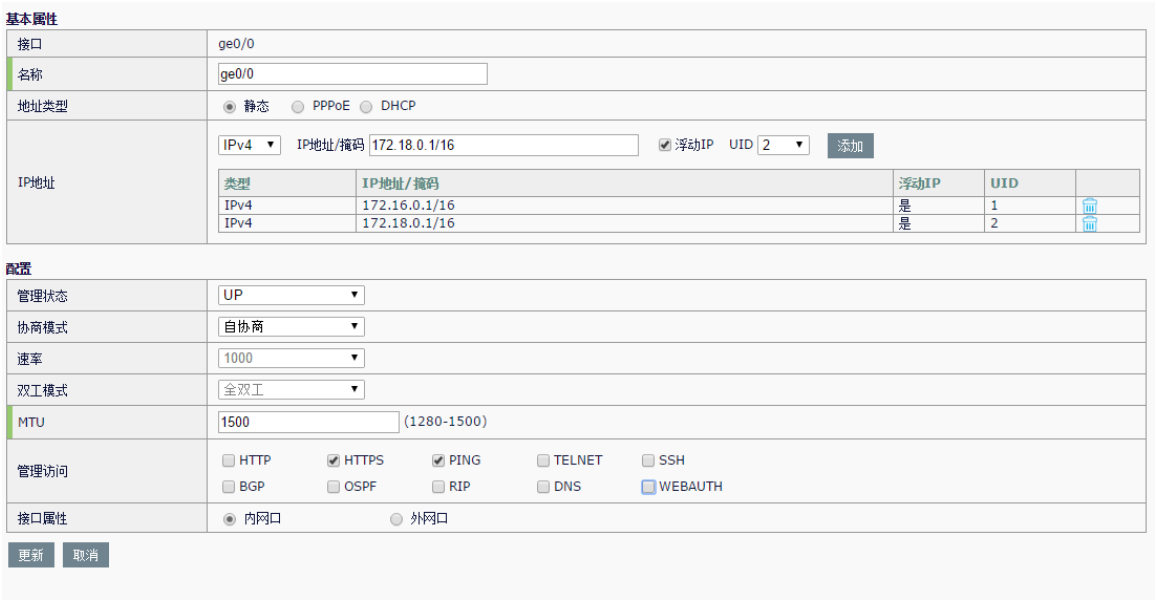
40.8.2 案例 2：配置主主模式基本配置

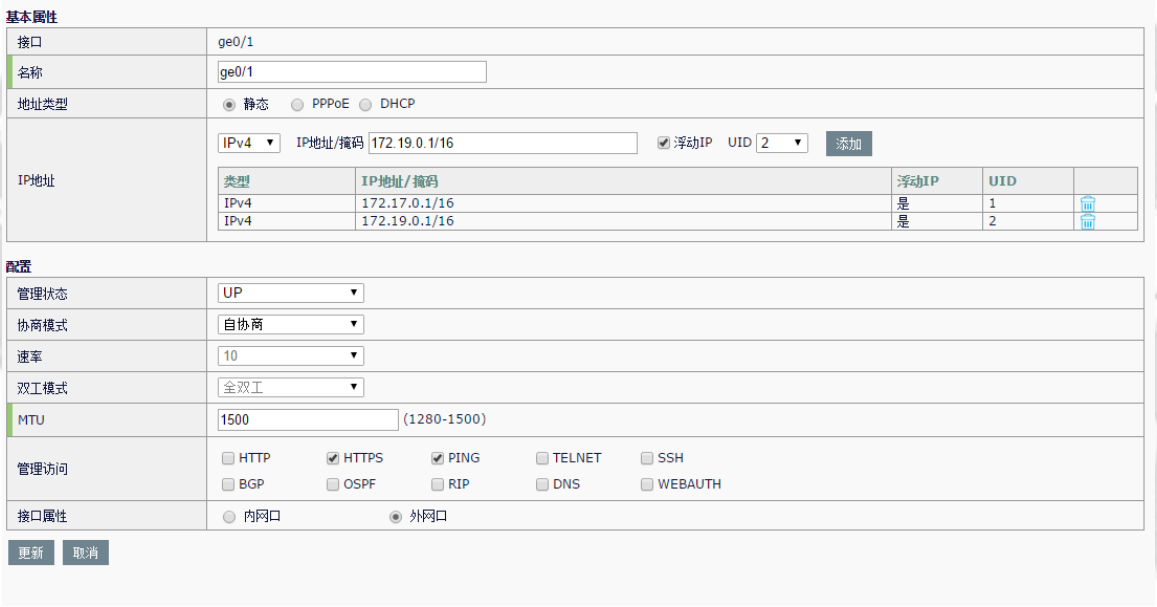
案例描述：

两台设备，host_A,host_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，也可以进行配置同步。

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。其中业务转发口浮动 IP 配置如下：

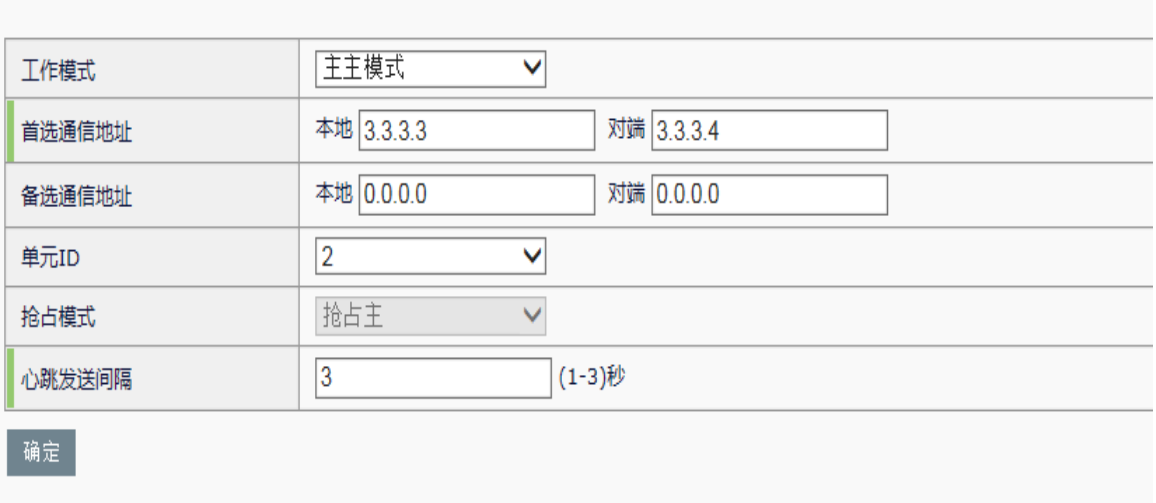




业务转发接口的 IP 必须配置为浮动 IP，浮动 IP 仅用于 HA 环境下进行业务转发。

主主环境下，当两台设备都处于主状态时，浮动 IP 在与其单元 ID 相同的设备上生效，在对端设备上浮动 IP 不生效。当其中一台设备由于宕机或其他原因切换为备状态时，主状态上的所有浮动 IP 均生效且承载业务流量的转发。

2、配置 host_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：可选配置，本例中仅配置首选通信地址。

单元 ID：设置设备单元 ID 号为 2，两台设备必须不一样。NAT 策略、浮动 IP 也会有自己的 ID 号，只有与设备单元 ID 号相同的 NAT 策略、浮动 IP 才会在本设备上生效，否则不会生效。

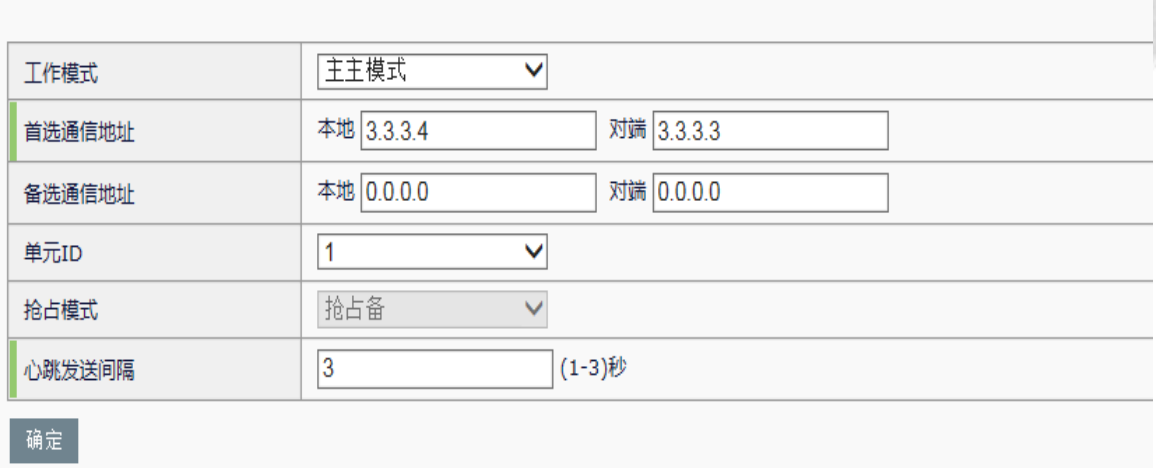
抢占方式：主主模式下，抢占方式不生效。

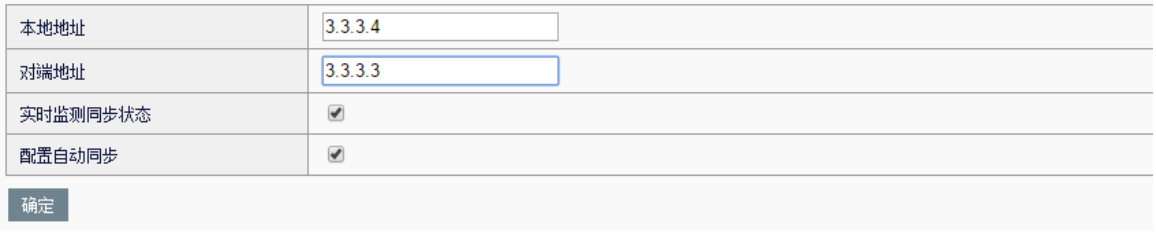
心跳发送间隔：每 3 秒发送一次心跳。

3、配置 host_A，进入系统>高可用性，进入配置同步界面。配置步骤同主备模式一致，请参照主备模式配置步骤。

4、配置 host_A，进入系统>高可用性，进入连接同步界面。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 host_B，配置步骤请参照设备 host_A，这里不再重复介绍，其中 host_B 上的业务口浮动 IP 配置与 host_A 配置一致，以下是设备 host_B 配置完成后 HA 相关的配置页面。





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，NAT 的 ID 也需要修改。

以上是 HA 主主模式的配置过程，需要让设备实现业务转发功能。

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，主备切换操作失效，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。

第41章 VRRP

41.1 VRRP概述

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。

提示：

在 VRRPv3 版本模式下，不支持认证。

VRRP 定时器：

- 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。

- 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。

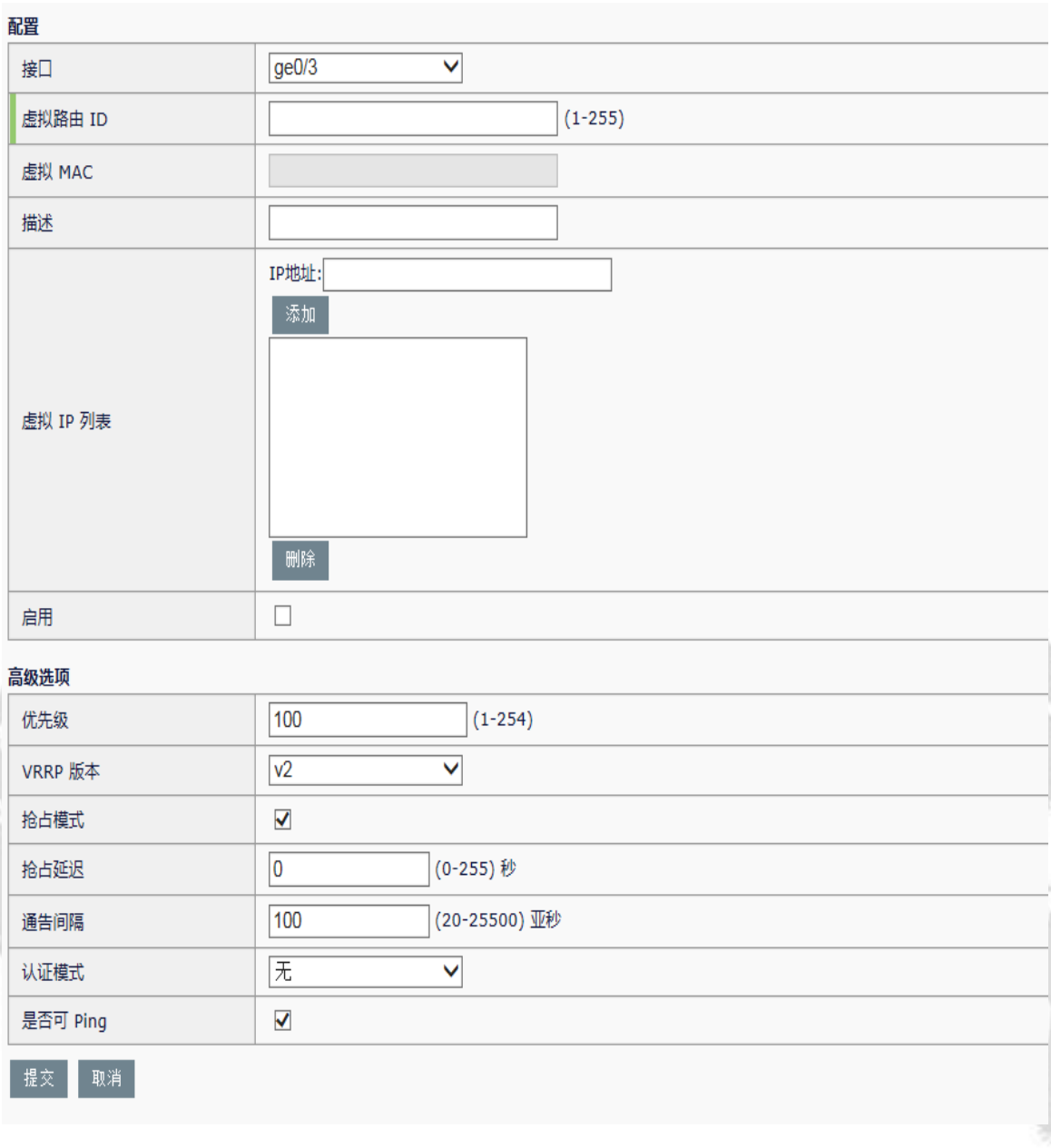
41.2 配置VRRP

41.2.1 配置 VRRP

配置步骤：

1、在**网络>接口配置>物理接口列表**中，为一个接口配置好 IP 地址。

2、新建 VRRP 备份组，进入**系统管理> VRRP**，点击对应接口下的“**新建**”按钮。如下图：



接口：接口列表中包含所有的接口。

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：为配置虚拟路由 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。

提示：

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。

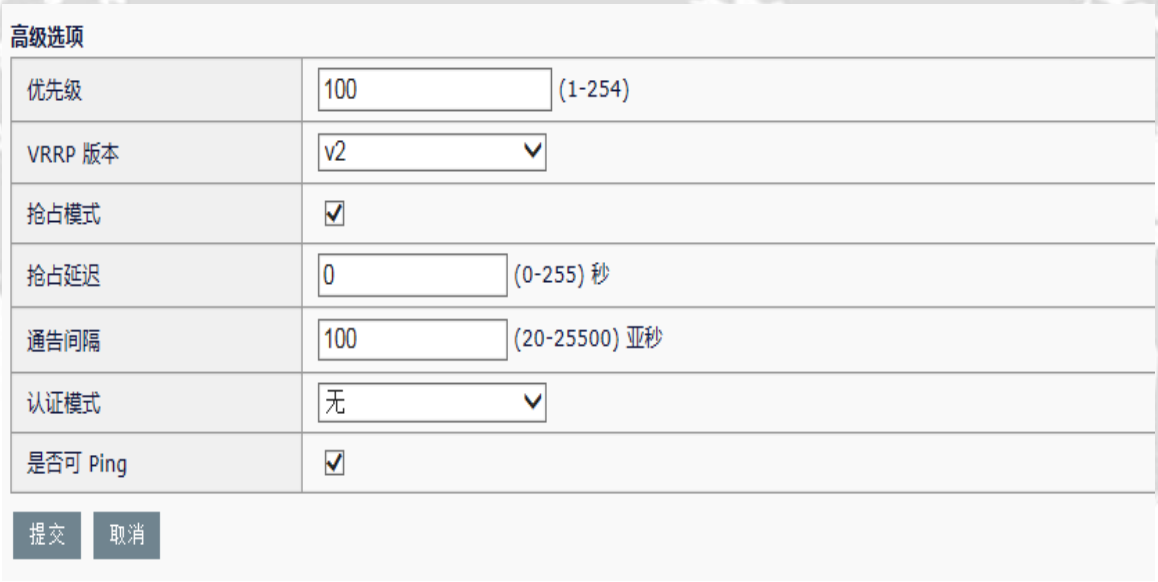
如果接口连接多个子网，则可以为一个备份组配置多个虚拟 IP 地址，以便实现不同子网中路由器的备份。

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，点击“高级选项”按钮。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。

注意：

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：

接口处于 UP 状态

接口网线上能检测到载波信号

接口上至少配置了一个真实 IP 地址

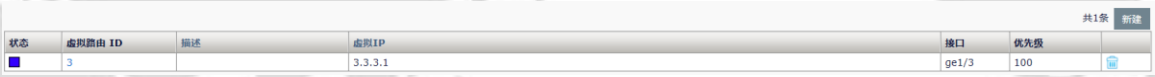
备份组至少配置了一个虚拟 IP 地址

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。

41.2.2 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：



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。

41.2.3 删除 VRRP 备份组

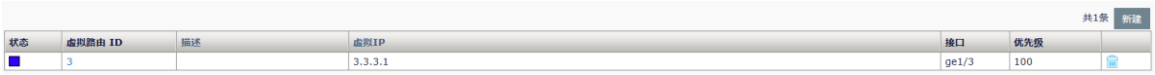
在已经建立好的备份组的操作选项中，点击“ ”按钮，经确认后删除。

注意：

如果备份组所属的接口被“注销”，如物理接口被拔除或者 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。

41.2.4 查看 VRRP 备份组

进入 VRRP 配置页面，如下图：



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。

41.3 配置案例

41.3.1 配置案例 1（单备份组）

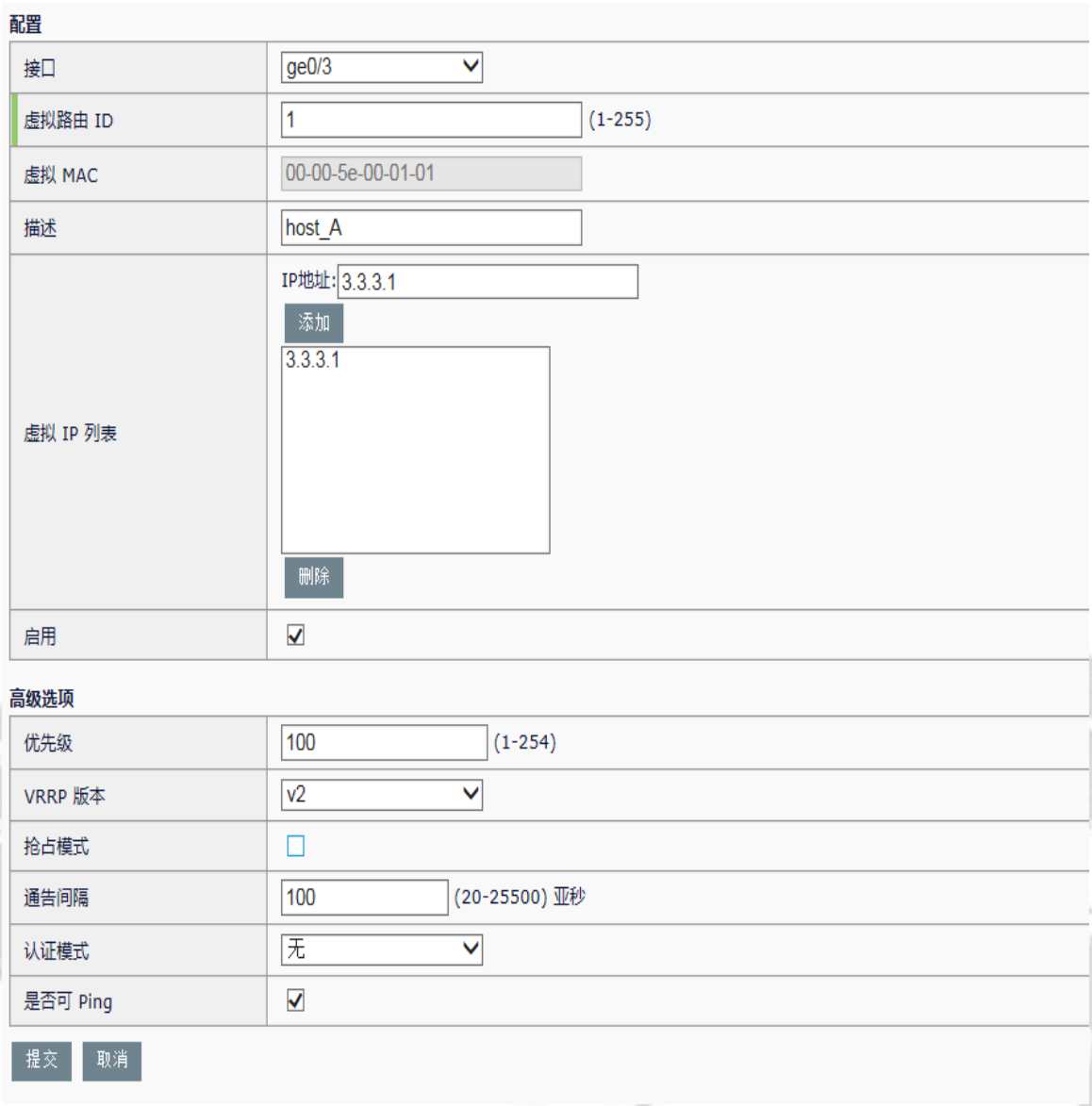
案例描述：

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 3.3.3.1 这个 IP 地址作为它们的默认网关。把 host_A 和 host_B 两台路由器组成一个备份组 1。

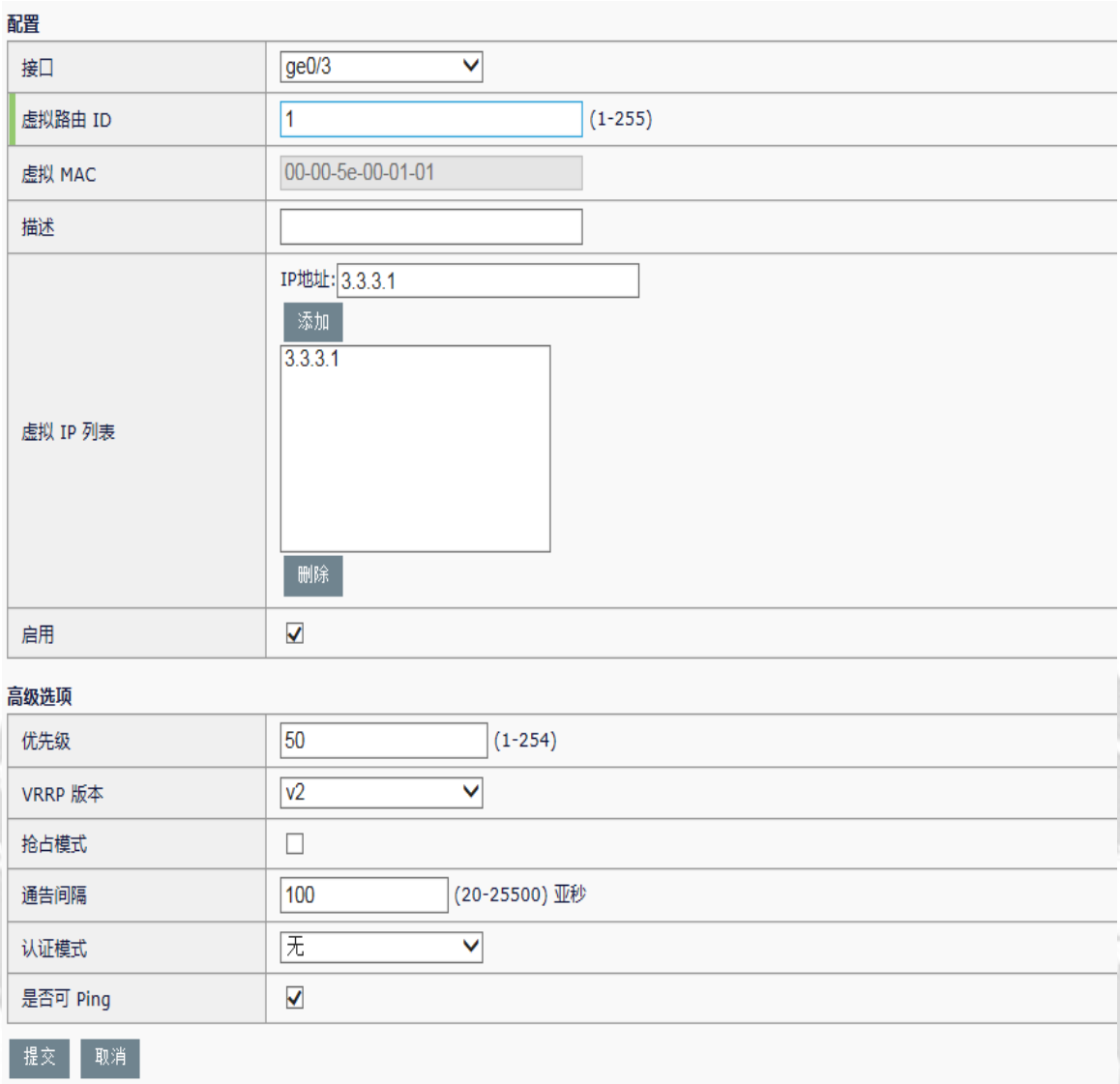
配置步骤：

1、在 host_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 3.3.3.1，提交后启用此备份组。

2、在 host_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，提交后启用此备份组。

41.3.2 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 host_A 和 host_B 两台路由器创建两个备份组：

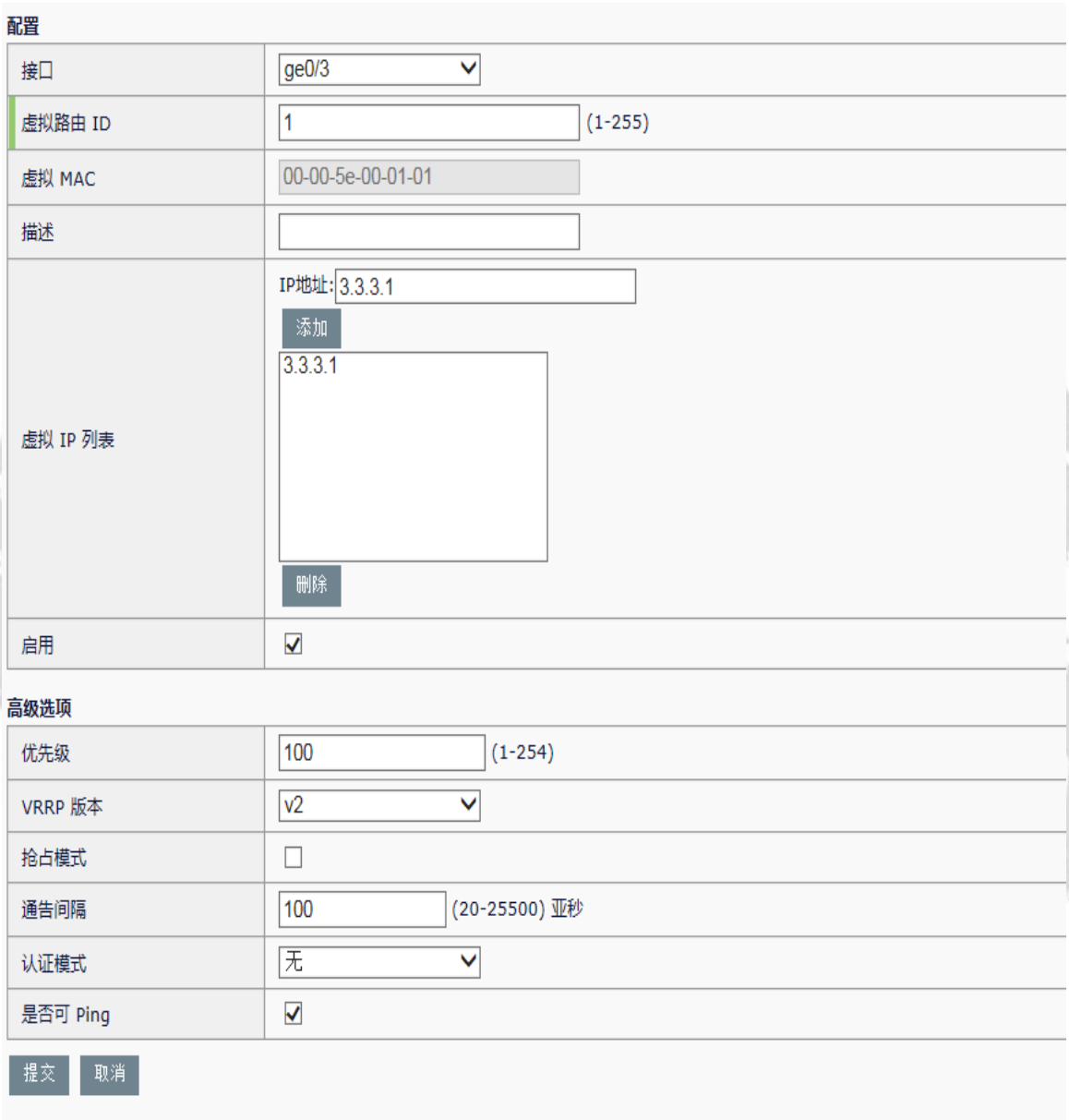
备份组 1：host_A 作为 Master 路由器，host_B 作为 Backup 路由器，虚拟 IP 为 3.3.3.1。

备份组 2：host_A 作为 Backup 路由器，host_B 作为 Master 路由器，虚拟 IP 为 3.3.3.2。

为了实现业务流量在 host_ A、和 host_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 3.3.3.1 和 3.3.3.2。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。

配置步骤：

1、在 host_A 进入**系统管理>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 3.3.3.1，提交后启用此备份组。

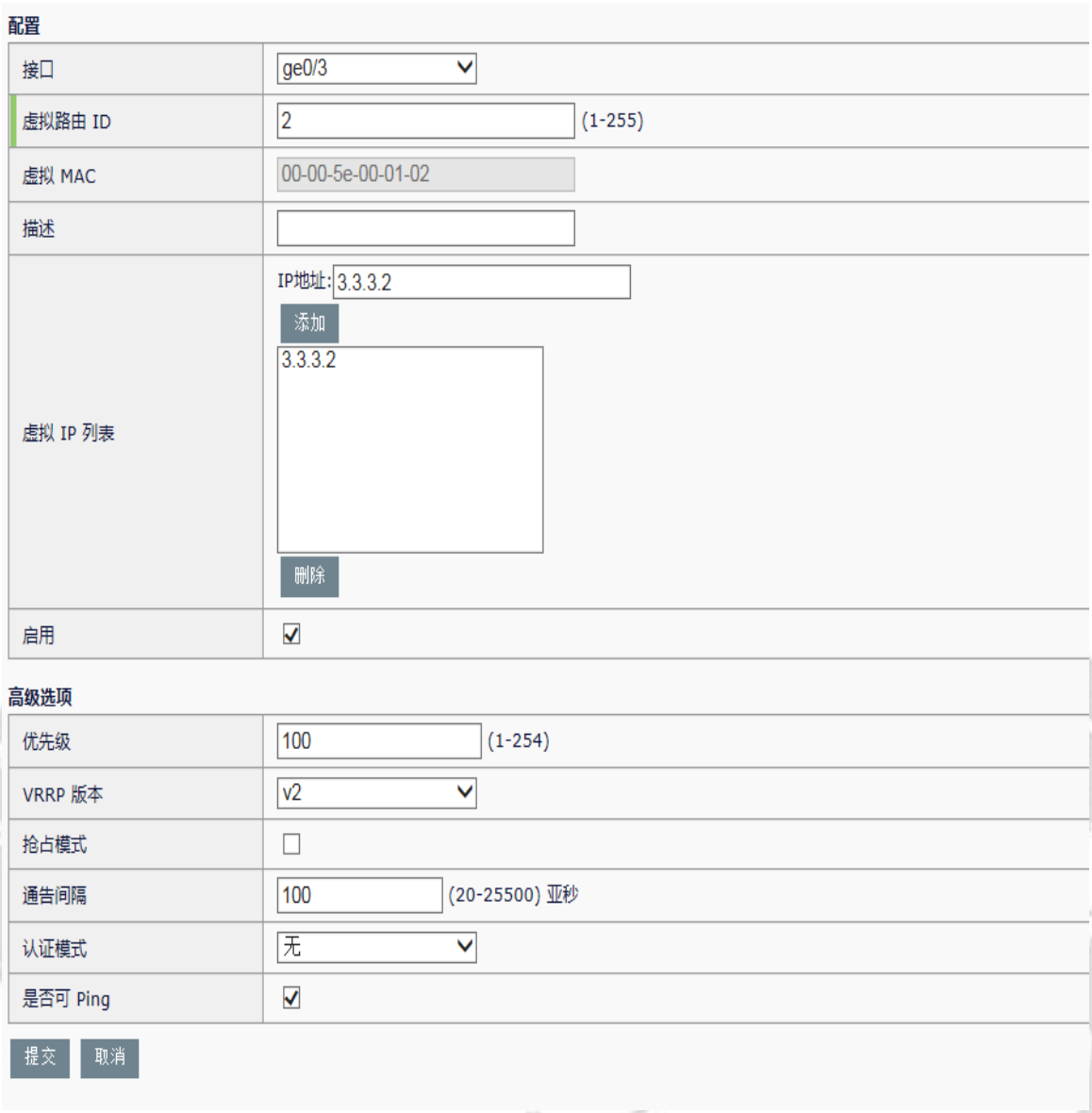
2、在 host_A 进入**系统管理>VRRP**，点击**新建**按钮，如下图配置：

VRID 设置为 2，优先级为 50，虚拟 IP 为 192.168.31.2，提交后启用此备份组。

3、在 host_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，提交后启用此备份组。

4、在 host_B 进入**系统>VRRP**，点击“**新建**”按钮，如下图配置：



VRID 设置为 2，优先级为 100，虚拟 IP 为 192.168.31.2，提交后启用此备份组。

41.4 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	备份组所属接口必须满足： 接口处于 UP 状态 接口网线上能检测到载波信号

接口上至少配置了一个真实 IP 地址

第42章 日志管理

42.1 系统日志概述

系统日志是一种记录设备运行状况的方式。本设备支持标准的 SYSLOG 格式、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。

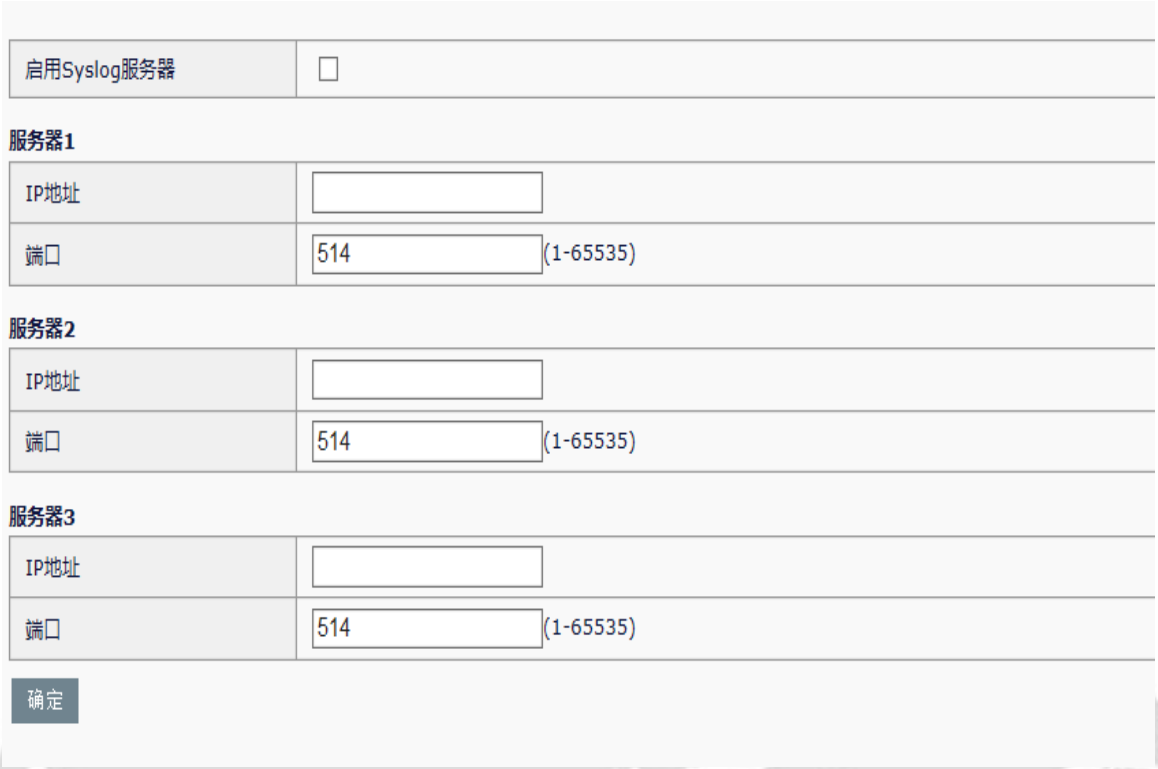
42.2 配置说明

42.2.1 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

42.2.2 配置 SYSLOG 服务器

1、进入**系统>日志设定>日志服务器**，如下图：



启用：选中表示启用，不选表示关闭。

IP 地址：Syslog 服务器地址。

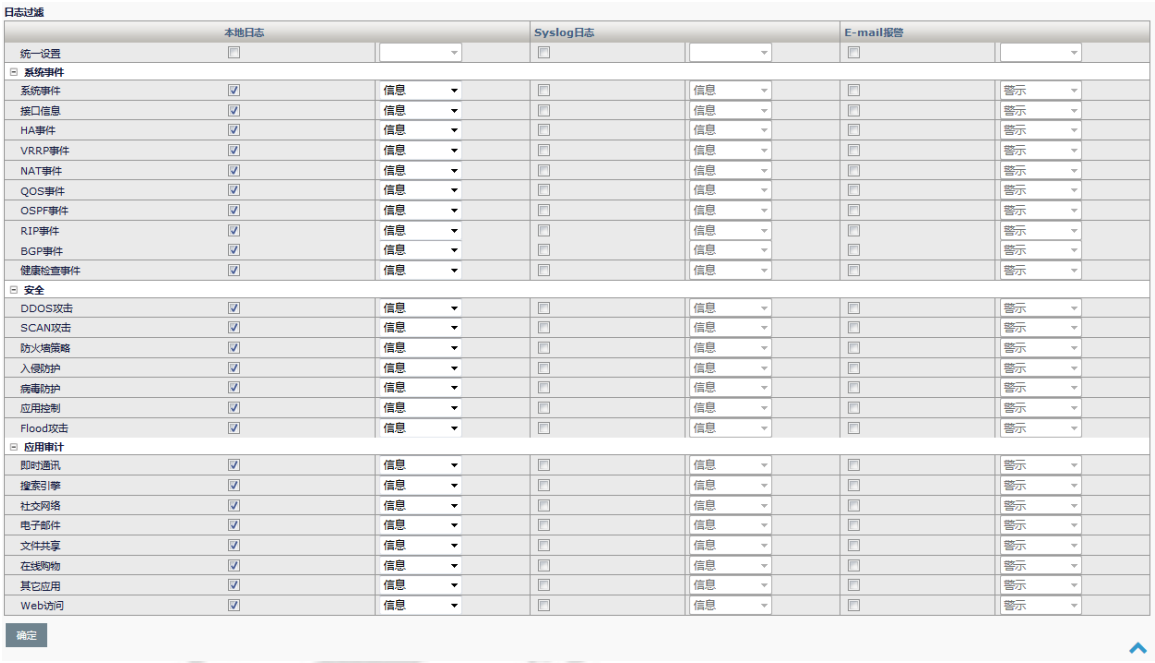
端口：Syslog 服务器端口。

服务器 1、服务器 2、服务器 3 表示可以同时将日志发送到数个不同的 Syslog 服务器，之间互不影响。

2、点击**确定**。

42.3 配置日志过滤

1、进入**系统>日志设定>日志过滤**，如下图：



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。

2、点击**提交**。

提示：

日志过滤中只对大于或等于该级别的日志有效。

日志过滤中涉及到的日志模块只是发送日志模块的的一部分。

42.4 日志记录和查询

42.4.1 日志查看

下一代防火墙设备上的日志展示一共分为七大类，包括系统日志、安全日志、NAT 日志、应用控制日志、入侵防护日志、病毒防火墙日志和操作日志，每种分类同系统>日志设定>日志过滤中所包含功能模块一致。

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“**查询**”功能选择具体的日志模块、日志级别、日志产生时段等进行日志的精确显示。

操作日志的日志内容和日志配置只能在 audit 审计用户下查看和操作

五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**，如下图：

查询 导出日志

	时间	类型	级别	消息
1	2015-05-29 16:31:59	系统事件	通知	Content="The system is up!"
2	2015-05-29 16:31:57	HA事件	警告	Content="Master(NONE) to Master(ALL), ha no neigbour"
3	2015-05-29 16:31:54	HA事件	警告	Content="Init to Master(NONE), ha initialization over"
4	2015-05-29 16:31:54	HA事件	警告	Content="Disable to Init, HA start"
5	2015-05-29 16:31:54	HA事件	通知	Content="Ha started in master-master mode"
6	2015-05-29 16:30:09	系统事件	通知	Content="The system is going down for reboot NOW!"
7	2015-05-29 16:28:42	系统事件	警告	Content="admin upgrade V100R0100B20150529 from web, success."
8	2015-05-24 22:14:24	接口信息	警告	Content="interface ge0/0 link up"
9	2015-05-24 22:14:12	接口信息	警告	Content="interface ge0/0 link down"
10	2015-05-24 04:40:28	HA事件	警告	Content="HA (Master(ALL)) lost neighbour!"
11	2015-05-24 04:40:20	接口信息	警告	Content="interface ge0/3 link down"
12	2015-05-24 04:39:57	HA事件	信息	Content="HA finished to compare system config"
13	2015-05-24 04:38:57	HA事件	信息	Content="HA finished to compare system config"
14	2015-05-24 04:37:57	HA事件	信息	Content="HA finished to compare system config"
15	2015-05-24 04:36:57	HA事件	信息	Content="HA finished to compare system config"
16	2015-05-24 04:35:57	HA事件	信息	Content="HA finished to compare system config"
17	2015-05-24 04:34:56	HA事件	信息	Content="HA finished to compare system config"
18	2015-05-24 04:33:56	HA事件	信息	Content="HA finished to compare system config"
19	2015-05-24 04:32:56	HA事件	信息	Content="HA finished to compare system config"
20	2015-05-24 04:31:56	HA事件	信息	Content="HA finished to compare system config"

20 第 1 共142页 显示1到20,共2829记录

时间：该日志消息的产生时间。

类型：该日志消息的模块类型。

级别：该日志消息的级别。

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。

日志翻页：统计当前类别中所展示出的日志总页数。同时提供日志翻页功能，可以向前一页、向后一页、首页、末页和翻到特定页操作。最新的日志在第一页，默认展示第一页，且每页最多展示 50 条日志。

提示：

审计日志只有 audit 用户可以配置和查看。

42.4.2 日志查询条件设置

在日志显示页面，可以通过**过滤**来显示相应条件的日志。不设置过滤条件时，默认显示所有日志。当配置有条件查询设置，如果需要取消所有条件，点击**重置**。

1、进入**日志>系统日志**点击**查询**，如下图：

模块：选择需要查看的日志模块。

日志级别：选择需要显示的日志级别。默认为空，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 地址：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 地址：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。

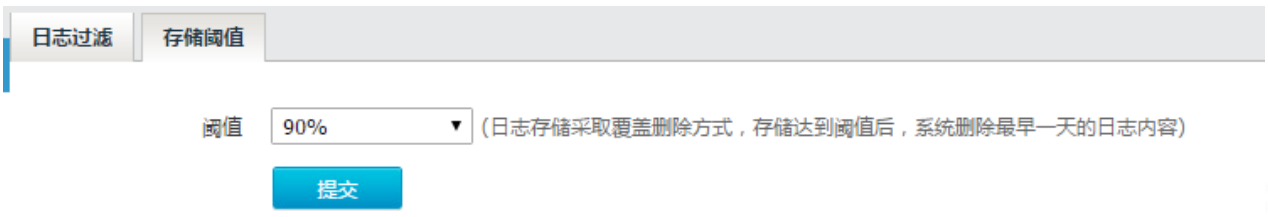
开始时间/结束时间：日志产生的时间段。

2、点击查询。

42.5 硬盘阈值设置

硬盘阈值设置针对带有硬盘的下一代防火墙设备，该配置对设备的硬盘加以限制，若超出该阈值则硬盘从最早一天的日志文件开始删除，直到硬盘的使用空间小于阈值。

1、进入**系统>日志设定>日志过滤，**点击存储阈值，如下图：



42.6 配置案例

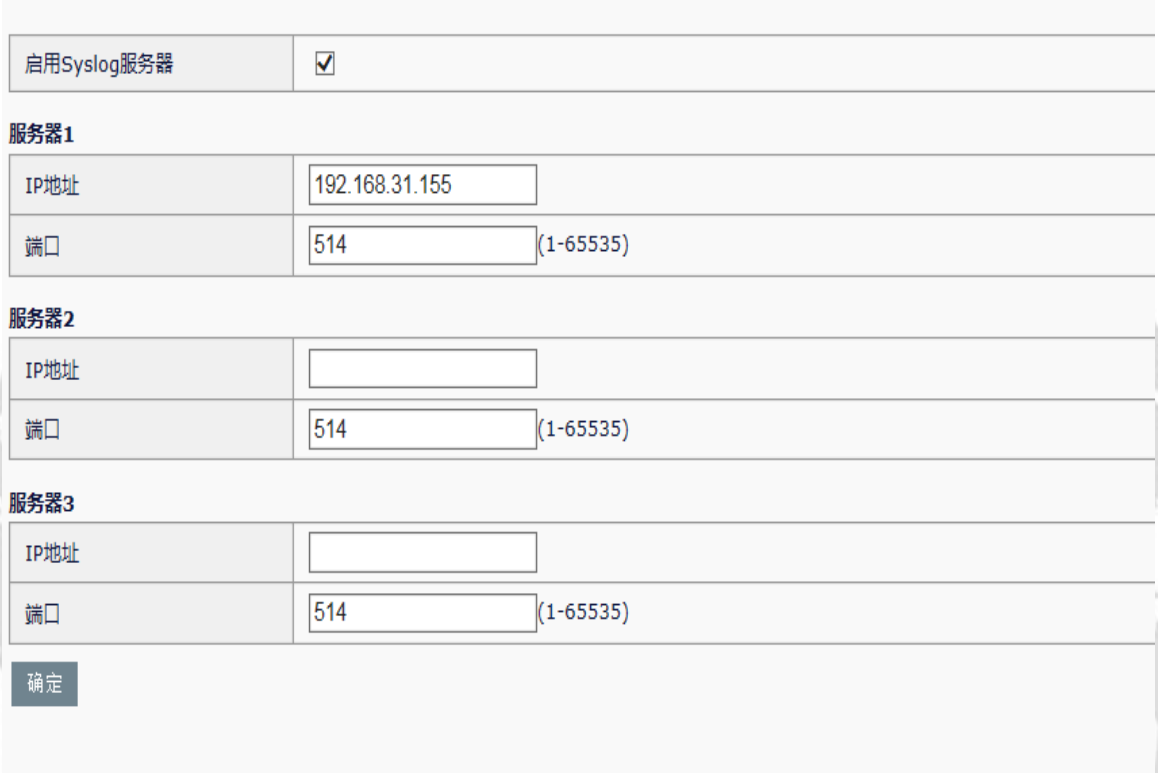
42.6.1 配置案例：配置 HA 模块 SYSLOG 日志

案例描述：

配置 HA 事件模块发送到日志服务器。

配置步骤：

1、进入**系统>日志设定>日志服务器：**



2、设置配置参数

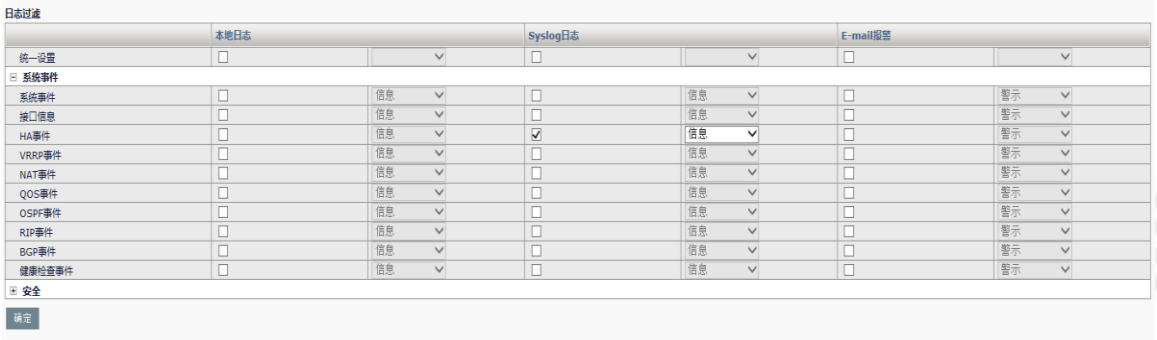
IP 地址：Syslog 服务器地址为”192.168.31.155”。

端口：Syslog 服务器端口默认为 514。

启用：选中表示启用

3、点击提交完成设置。

4、进入**系统>日志设定>日志过滤：**



5、设置参数。

6、点击确定完成设置。

提示：

进行 HA 模块相关操作后，在 Syslog 服务器上能够看到 HA 模块产生的日志信息。

42.7 常见故障分析

42.7.1 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	是否正确配置 SYLOG 服务器的地址和端口号 是否指定模块的日志类别和等级到 SYSLOG Server
解决	正确配置 SYSLOG 服务器的地址和端口号 指定模块的日志类别和等级到 SYSLOG Server

42.7.2 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	是否正确配置告警邮件配置参数 是否启用对应模块发送 E-mail 日志 所产生的日志级别是否满足发送 email 告警要求（警示及以上级别）
解决	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 启用对应模块发送 E-mail 日志 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。

第43章 网络诊断

43.1 诊断工具概述

为了方便用户进行配置排错，下一代防火墙中提供了诊断工具功能。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。

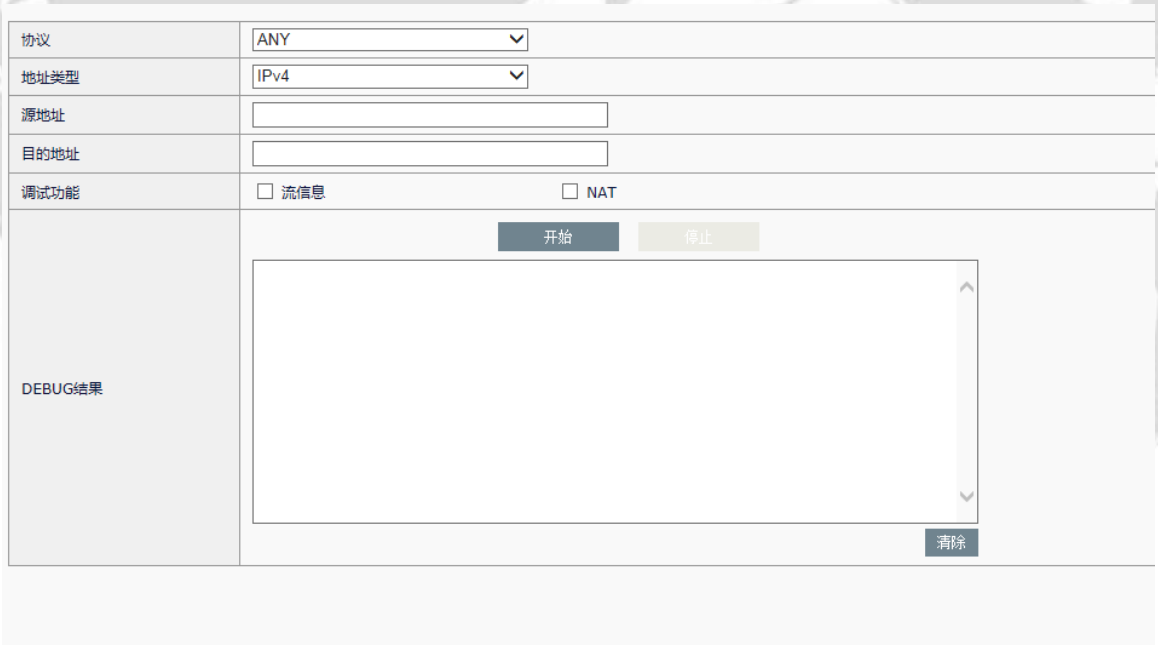
43.2 配置诊断工具

43.2.1 配置诊断工具的基本要素

诊断工具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**系统>系统维护>诊断工具**，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。

IP 类型：数据包的 IP 类型，下拉框中可以选择 IPv4、IPv6。

源 IP：数据包的源地址，输入只支持主机地址格式。

目的 IP：数据包的目的地址，输入只支持主机地址格式。

调试功能：指定查看的功能模块处理结果，可选择流信息、NAT。

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。

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。

注意：

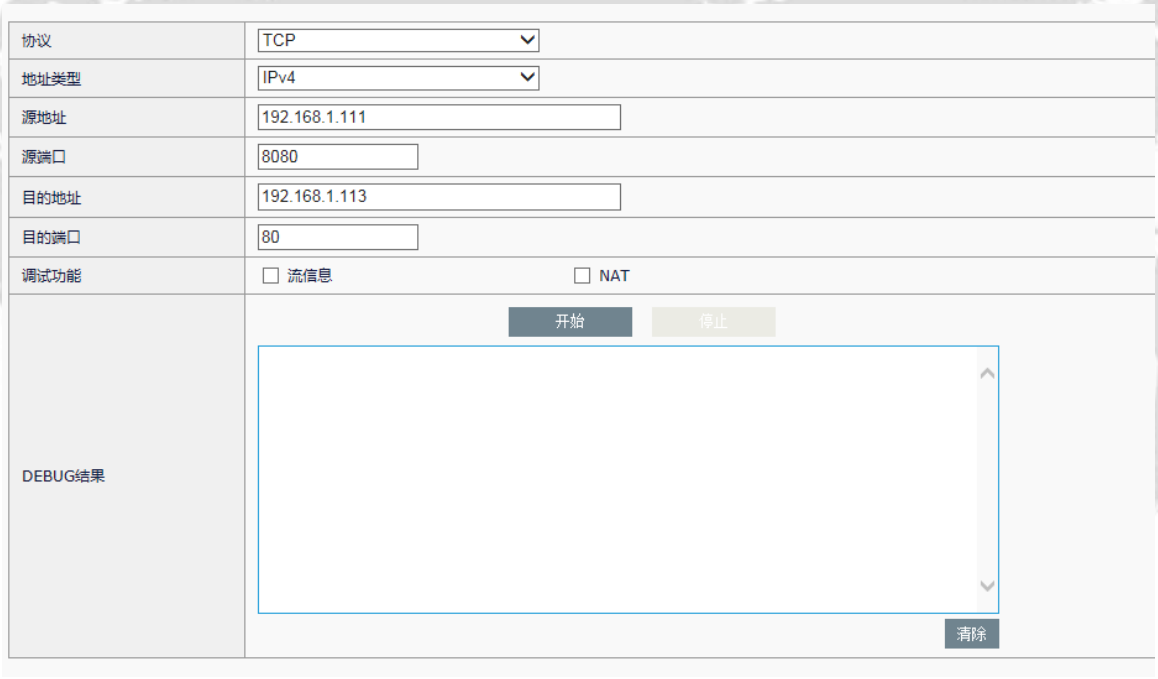
在调试过程中不能更改参数，需停止后方可更改。

43.2.2 配置协议为 TCP(UDP)的诊断工具

协议为 TCP(UDP)的诊断工具需要填写源端口、目的端口参数。

配置步骤：

1、进入**网络配置>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。

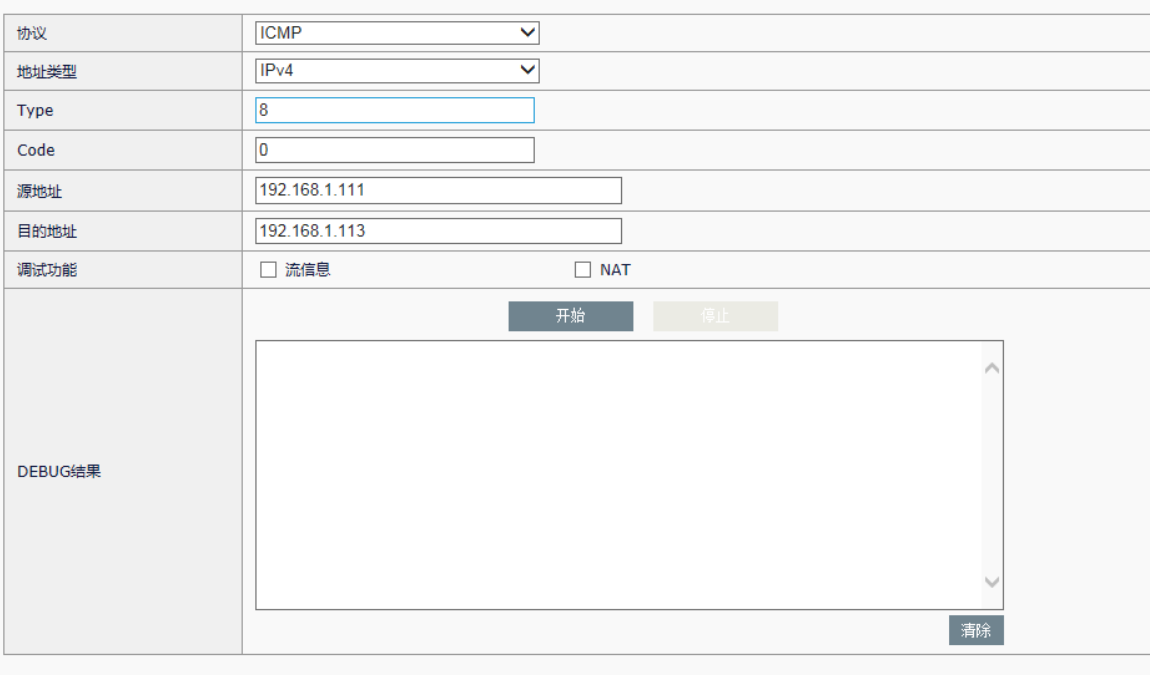
目的端口：数据包的目的端口。

43.2.3 配置协议为 ICMP 的诊断工具

协议为 ICMP 的诊断工具需要填写 Code、Type 参数。

配置步骤：

1、进入**系统>系统维护>诊断工具**，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。

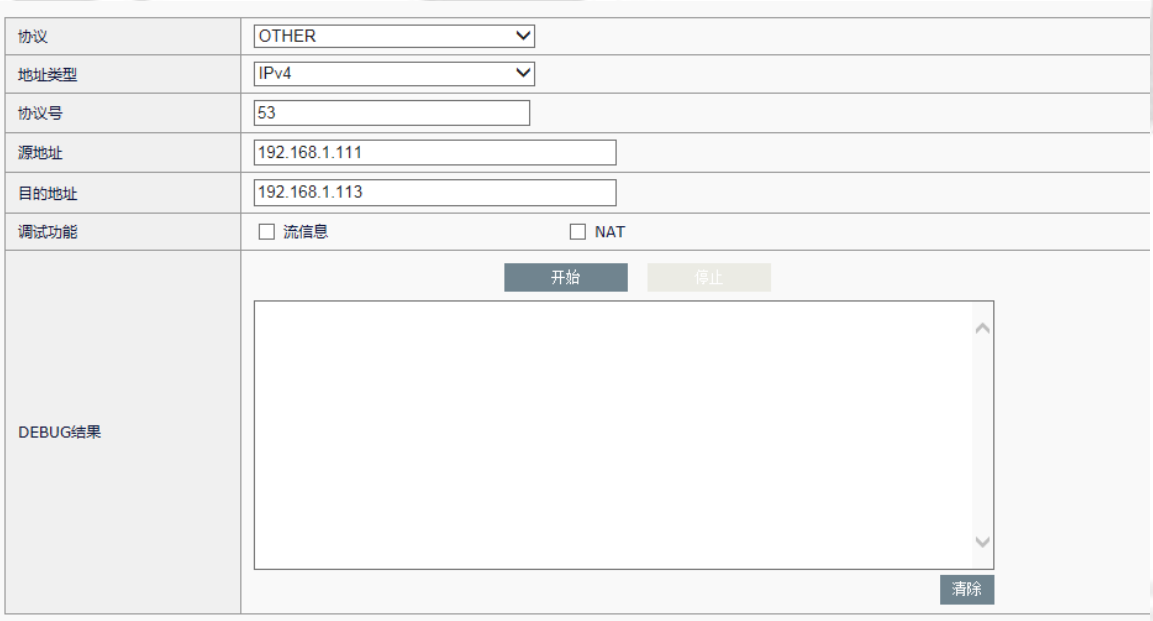
Code：ICMP 报文携带的的代码字段，取值区间 0~255。

43.2.4 配置协议为 OTHER 的诊断工具

协议为 OTHER 的诊断工具需要填写四层协议号参数。

配置步骤：

1、进入**系统>系统维护>诊断工具**，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。

43.3 配置案例

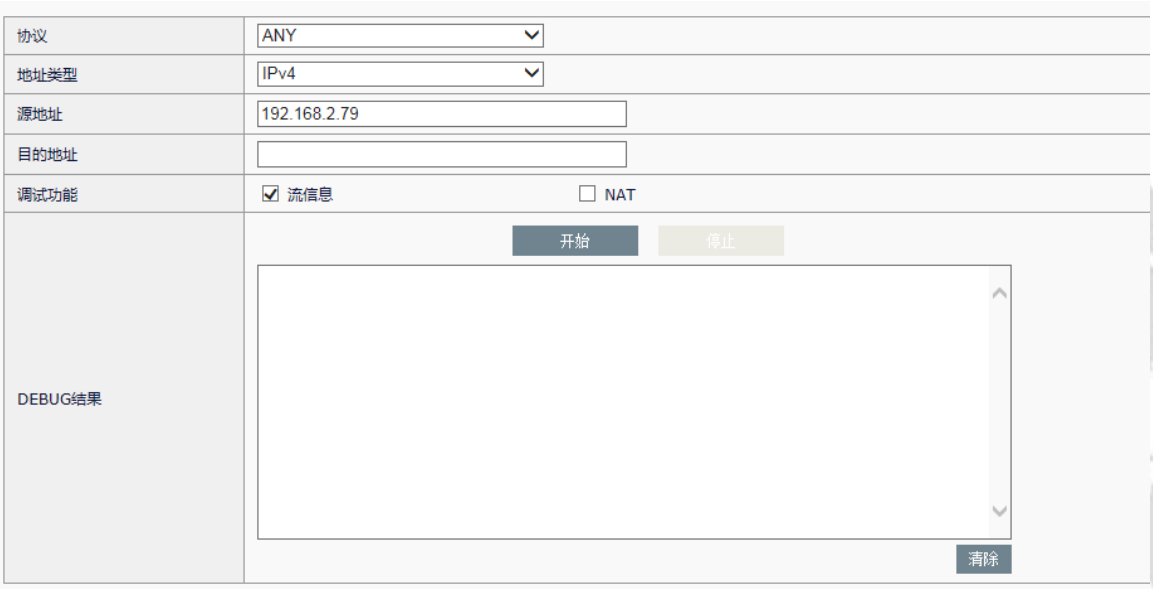
43.3.1 案例 1：使用 IPv4 的诊断工具功能

案例描述

观察主机 192.168.2.23 与任意主机之间交互的数据包的流信息

配置步骤：

1、进入**系统>系统维护>诊断工具**，协议下拉框中选择 ANY，IP 类型下拉框中选择 IPv4，调试功能复选框中选择流信息，如下图：



2、点击**开始**，如下图：

第44章 抓包工具

44.1 概述

使用抓包工具功能，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。

44.2 抓包工具配置

进入**系统>系统维护>抓包工具**，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

注意：

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，最多保存 10 个抓包文件，抓满 10 个文件后会自动停止抓取，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。

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。

源地址和目的地址始终为连接的初始源地址和目的地址。

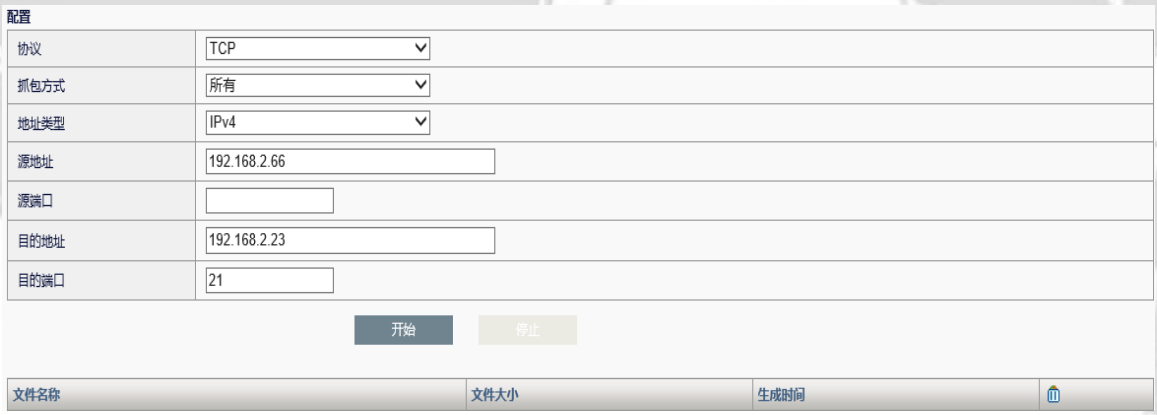
44.3 配置案例

案例描述

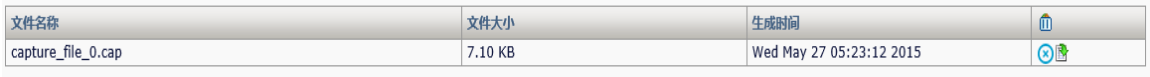
地址为 192.168.2.23，提供 FTP 服务，客户端地址为 192.168.2.66，要求配置过滤条件，抓取这次 FTP 访问的报文。

配置步骤：

1、进入**系统>系统维护>抓包工具**，进行过滤条件的设置：



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:



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。

第45章 授权

45.1 概述

防火墙中的部分功能需要经过授权激活之后才能使用，激活网址：license.sec-inside.com

45.2 在线激活

配置 DNS 和到公网路由，确保设备可以上网。然后在设备管理页面点击在线激活，输入激活码后点击确定，完成激活。

注意！功能授权需要重启才能生效

模块名	授权状态	剩余时间	授权点数
下一代防火墙	已授权	-	-
应用控制	已授权	-	-
入侵防护	已授权	-	-
病毒防护	已授权	-	-
URL分类控制	已授权	-	-
虚拟专用网(VPN) - IPSEC	已授权	-	-
高级可持续攻击(APT)防护	未授权	-	-
应用特征库升级服务	已授权	5 天	-
入侵防御升级服务	已授权	33 天	-
病毒防护升级服务	未授权	-	-
URL分类特征库升级服务	已授权	5 天	-
虚拟专用网(VPN) - IPSEC客户端数	已授权	-	5

在线激活 离线激活

45.3 离线激活

访问 icense.sec-inside.com，输入激活码，设备序列号，验证码，点击提交。

然后输入公司和联系人信息，提交后得到**授权码**。

进入**系统>授权**，点击**离线激活**，输入**授权码**，点击**确定**。

注意！功能授权需要重启才能生效

模块名	授权状态	剩余时间	授权点数
下一代防火墙	已授权	-	-
应用控制	已授权	-	-
入侵防护	已授权	-	-
病毒防护	已授权	-	-
URL分类控制	已授权	-	-
虚拟专用网(VPN) - IPSEC	已授权	-	-
高级可持续攻击(APT)防护	未授权	-	-
应用特征库升级服务	已授权	5 天	-
入侵防御升级服务	已授权	33 天	-
病毒防护升级服务	未授权	-	-
URL分类特征库升级服务	已授权	5 天	-
虚拟专用网(VPN) - IPSEC客户端数	已授权	-	5

在线激活 离线激活

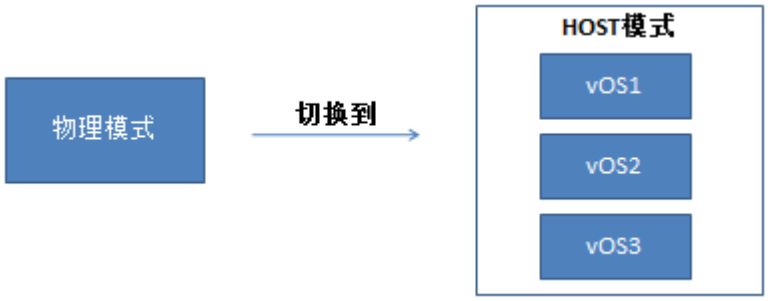
输入授权码

提交 取消

第46章 虚拟防火墙

46.1 概述

系统支持完全虚拟化，包含 CPU、内存、IO 等硬件资源虚拟化。在硬件支持的基础上，系统可以配置并运行多个虚拟系统，同时进行工作。



虚拟化术语约定：

1） BOS 模式（物理模式）

指系统处于普通的单机模式。

2）HOST 模式

指系统切换到宿主机模式，可以通过宿主机的管理页面（虚拟机管理系统），创建虚拟机。宿主机也可称为物理机。

3）虚拟 OS/虚拟机

指运行在 HOST 上的虚拟系统。

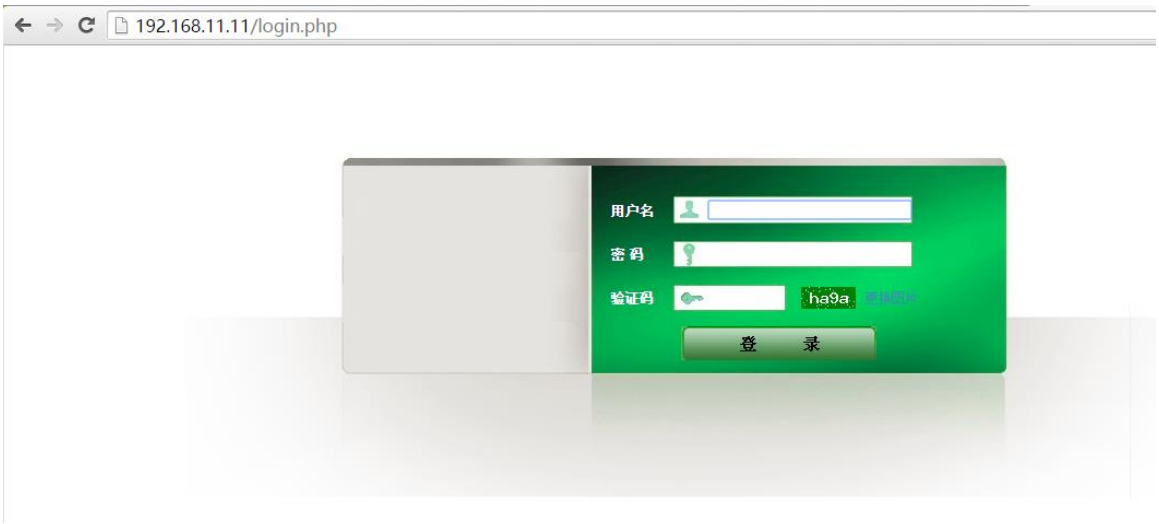
注：支持虚拟化的设备型号咨询，请联系相关人员。

46.2 启动HOST系统

系统启动时， GRUB 启动菜单中可选择进入 BOS 模式（物理模式）或者 HOST 模式。选择 HOST 后系统将进入 HOST 模式。

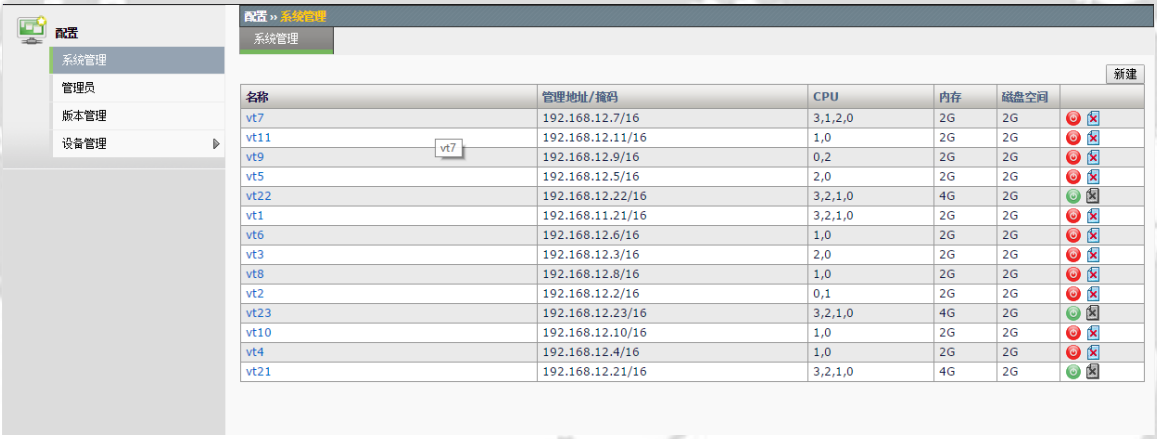
46.3 登录管理系统

HOST 模式启动完毕后，可通过页面登录虚拟机管理系统，进行配置和监控虚拟机。也可通过命令行控制台登录管理系统，通过标准的 linux virsh（list/console 等）系列命令对虚拟机进行控制。

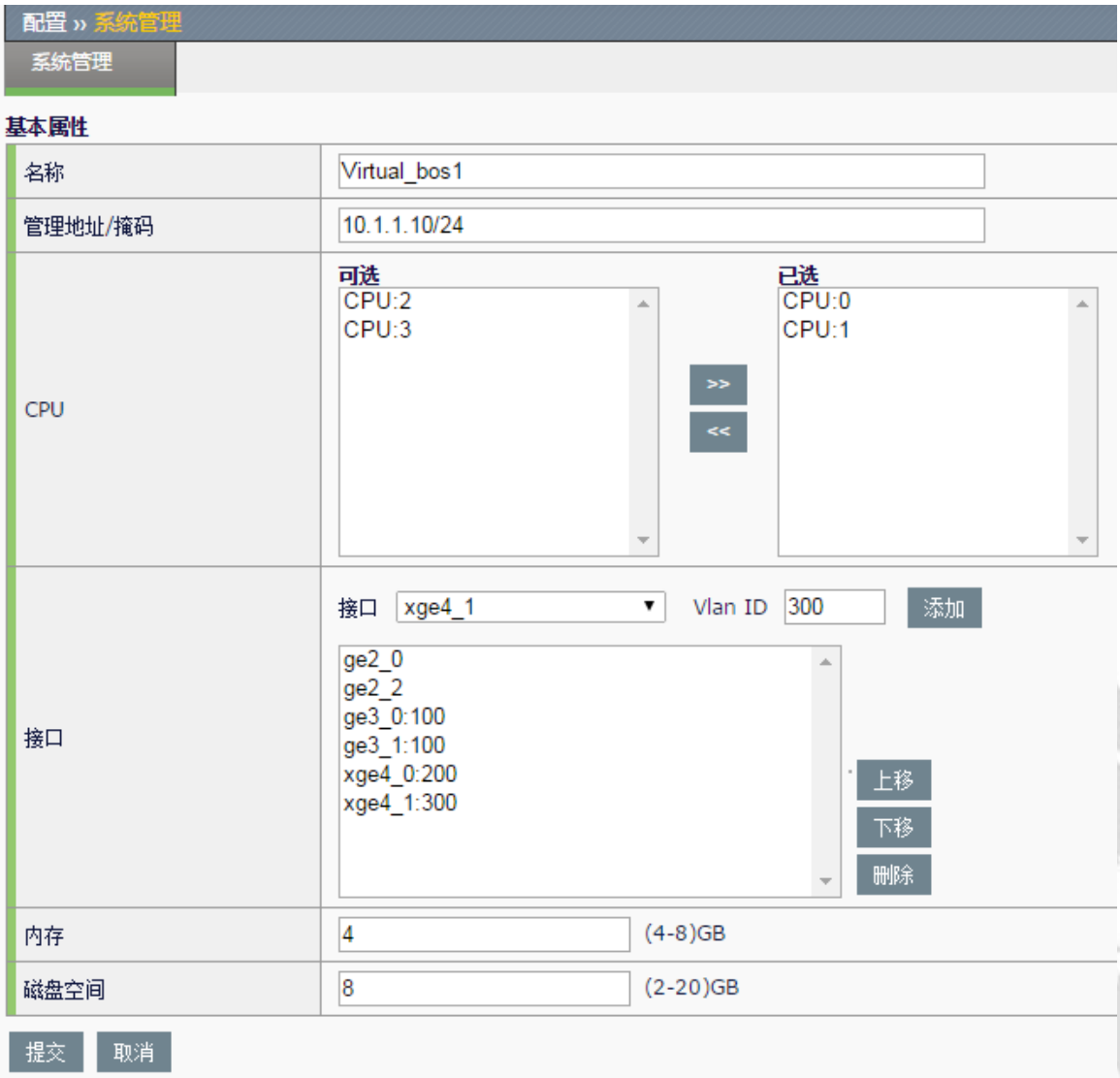


46.4 创建虚拟机

进入**配置>系统管理**，可看到如下界面。



点击**“新建”**按钮，创建新的虚拟机；点击**虚拟机名称**，可编辑已存在的虚拟机：



名称：虚拟机名称。（名称不能冲突）

管理地址/掩码：虚拟机的管理地址/掩码。配置的管理 IP 会直接下发到虚拟机的 mgt 口。

CPU：当前系统的 CPU 资源。CPU 可以多个虚拟机复用。

接口：当前系统的接口资源。

物理接口可以同时划入多个虚拟机，在不同虚拟机中 tag-ID 不能相同。

同一物理接口 tag-id 相同的两台虚拟机不能同时运行；

如果配置接口不带 tag-ID，最好此物理口为本虚拟机独占。

虚拟机接口和物理接口的映射关系:

1）虚拟机的虚拟接口和物理接口+TAG，为一一映射关系。

例如:　Virtual-BOS1　ge0/0　----------　HOST ge0/0 vlan-tag 10

Virtual-BOS2　ge0/0　----------　HOST ge0/0 vlan-tag 11

Virtual-BOS3　ge0/1　----------　HOST ge0/1

如上，业务流量进入物理接口 ge0/0，携带 vlan-tag 10 的流量发送到 Virtual-BOS1；

携带 vlan-tag 11 的流量发送到 Virtual-BOS2。不带 tag 的业务流量进入物理接口 ge0/1 会发送到 virtual-BOS3 的 ge0/1。

2）VLAN tag 的处理在物理接口上进行。

所有从物理口转交到虚拟机的流量都脱掉了 VLAN tag；

从虚拟机中发出的流量，在 HOST 中打上对应的 VLAN tag 后，才从物理接口发出去。

内存：当前系统的内存资源。

内存资源不能复用。多个同时运行的虚拟机内存总和要小于 HOST 内存大小。

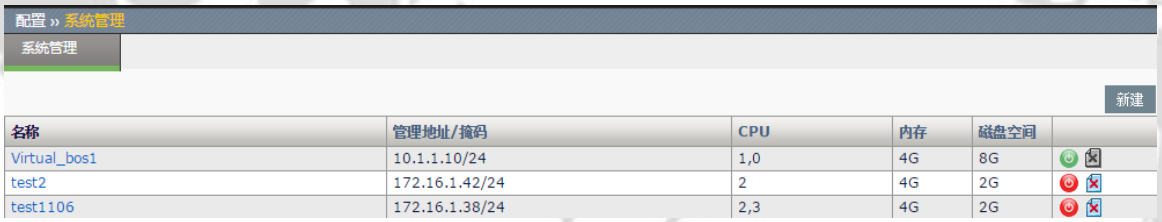
硬盘：当前系统的硬盘资源。

硬盘资源不能复用。多个同时运行的虚拟机硬盘总和要小于 HOST 硬盘大小

46.5 启动或停止虚拟机

进入**配置>系统管理**，点击虚拟机的开关按钮 ：

启动后，按钮变绿 ：



46.6 登录虚拟机

虚拟机启动 OK 后，可通过 HTTPS/Telnet 登录虚拟机。

因为是完整的虚拟化，所以启动后的虚拟机和真实机在软件上没有差异，配置页面和命令相同。

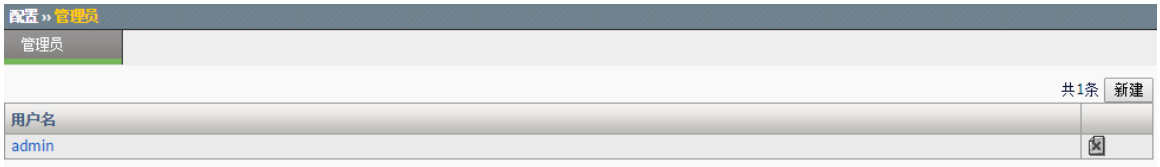
46.7 升级虚拟机

进入**配置>版本管理**，对虚拟机版本，进行系统升级。

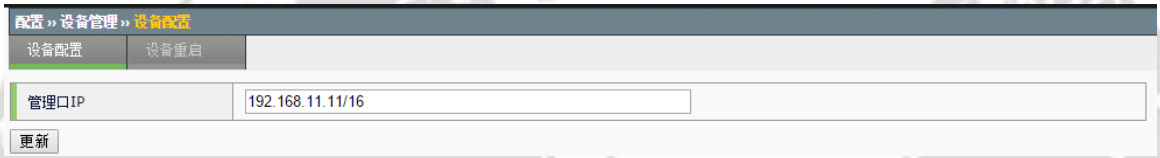
升级后的版本文件，只对之后新创建的虚拟机有效。已创建好的虚拟机，可以进入其中直接进行版本升级即可。

46.8 配置管理系统

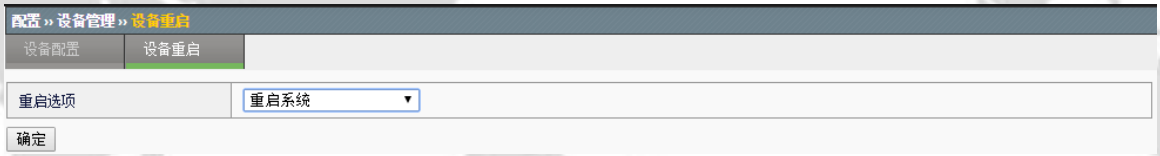
进入**配置>管理员**，可添加和编辑管理员。



进入**配置>设备管理>设备配置**，可编辑管理系统的管理 IP。



进入**配置>设备管理>设备重启**，可编辑管理系统的管理 IP。



第47章 云平台

47.1 概述

大规模网络、应用业务的巨幅增长，企业用户面临的安全威胁也与日俱增，威胁种类呈现出多样化的趋势。在企业网络安全建设方面，往往通过部署多台、多种类的安全设备，实现对信息网络的分级保护。传统的网管平台虽然可以集中式的进行安全检测和控制，但是管理性能低下，且接收数据存在各种性能瓶颈。在此背景下，我们推出了下一代数据驱动安全管理云中心（独立产品售卖），他不仅支持以往的硬件性能扩展，还支持基于软件的水平扩展，来满足大批量网络安全设备上报的数据元信息，通过大数据分析算法，安全资产管理，云计算等手段，以安全数据为核心，来驱动整个网络的安全能力的提升，是新一代的云安全界的顶尖产品。通过运行浏览器对云平台进行配置和管理。云平台安装之后默认开启了 web 服务。

47.2 云平台代理配置

1、进入**系统>云平台>云平台代理配置**，如下图：

云平台地址：云平台 IP 地址
云平台端口：云平台端口
状态上报间隔：设备向云平台发送心跳报文的时间间隔
绑定码：用户绑定码

2、点击**系统>云平台>云平台代理监控**，查看云平台登录状态。

云平台代理监控

启用/禁用	☑
代理版本	2
云平台地址	172.17.50.150
云平台IP	172.17.50.150
云平台端口	9070
绑定码	aed995e7ce694c4287d9cd512e3d3229
运行状态	云平台正常通信

刷新

第48章 SSL VPN

48.1 SSL VPN概述

Secure Socket Layer-安全套接层，俗称 SSL。于 1990 年开发的 SSL 通过提供私密性，信息完整性，身份认证以及私有性来保障 Word Wide Web 通讯的安全。SSL 是一个不依赖于平台和运用程序的协议，是天然的安全远程接入，在方案上，特别是权限控制、应用粒度上有独到之处，成为远程接入领域颇受青睐的选择，目前已经超越了技术范畴，而成为一个安全网络服务框架。

我们的设备使用 IP 方式建立 SSL VPN 远程连接，所有客户端都从服务器获得一个 VPN IP 来访问内部服务器，需要专用 SSL VPN 客户端软件来帮助建立连接。通信过程中使用 UDP 封装 SSLVPN 协议，协商使用 1194 端口，端口映射和 NAT 都可以轻松支持。拥有独立的用户中心页面，访问设备的 8443 端口可以轻松获取客户端安装文件，并有简明易懂的帮助文档辅助用户安装配置客户端。在使用客户端过程中用户还可以通过客户端的“修改密码”按钮跳转至此用户中心，也可以直接登录至此修改密码，增强了安全性。

48.2 配置SSL VPN

48.2.1 SSL VPN 设置

进入**网络>SSL VPN>SSL VPN 配置；**

基本设置：

启用：启用 SSL VPN 功能

用户中心：启用用户中心，可自定义端口号进行连接

多点登录：启用多点登录，单个用户可以多个终端进行登录

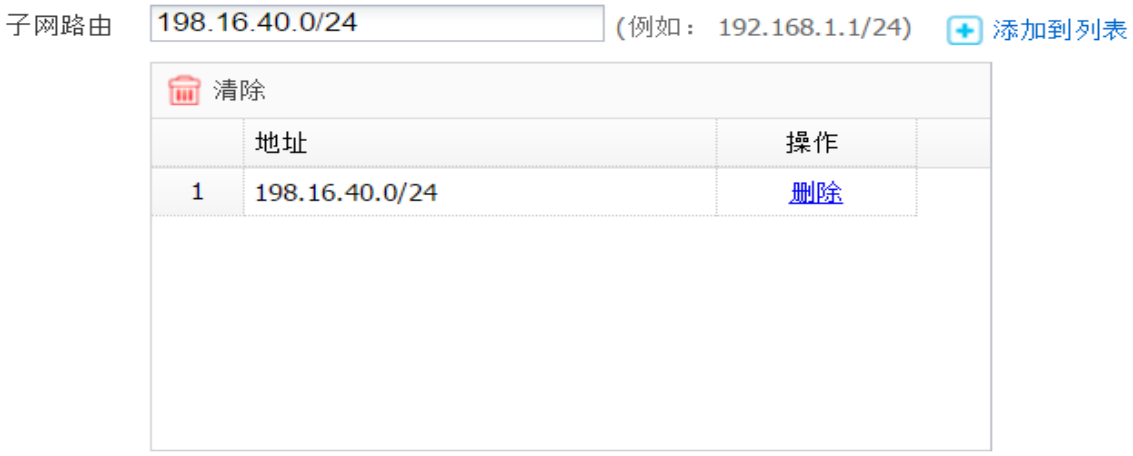
隧道地址：SSLVPN 隧道地址，将作为 VPN 用户网关地址

地址池：地址池内地址将分配给连接的 VPN 用户

DNS1&DNS2：首选&备选 DNS，将下发给拨入的 VPN 用户

WINS1 &WINS2:首选&备选 WINS，同上

子网路由：作为下发给客户端的路由的目的网段，路由下一跳为隧道地址



点击**‘添加到列表’**添加子网；点击 删除 删除已添加的子网。

高级选项：

此处配置 SSL VPN 帮助中心页面的客户端下载链接，格式需为 http://或 https://开头域名类 URL，添加的 URL 对应帮助中心客户端下载图标映射链接。

48.2.2 SSL VPN 用户中心

用户中心地址：https://<设备 IP 地址>:8443，用户中心拥有三大功能，可使用本地用户或远程用户账户登录，不可使用管理员账户登录。

密码修改：

客户端下载：（需要在 web 页面 SSL VPN 高级功能处配置）

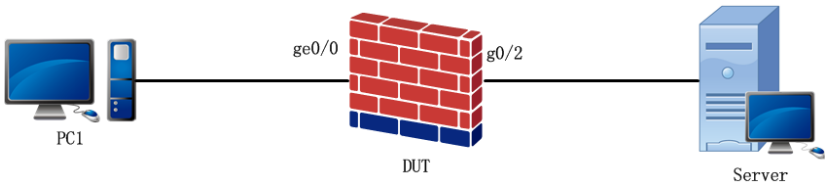
帮助文档

48.2.3 SSL VPN 监控

点击**网络>SSL VPN>SSL VPN 监控,**监控拨入的 SSL VPN 用户

48.3 配置案例

案例拓扑：

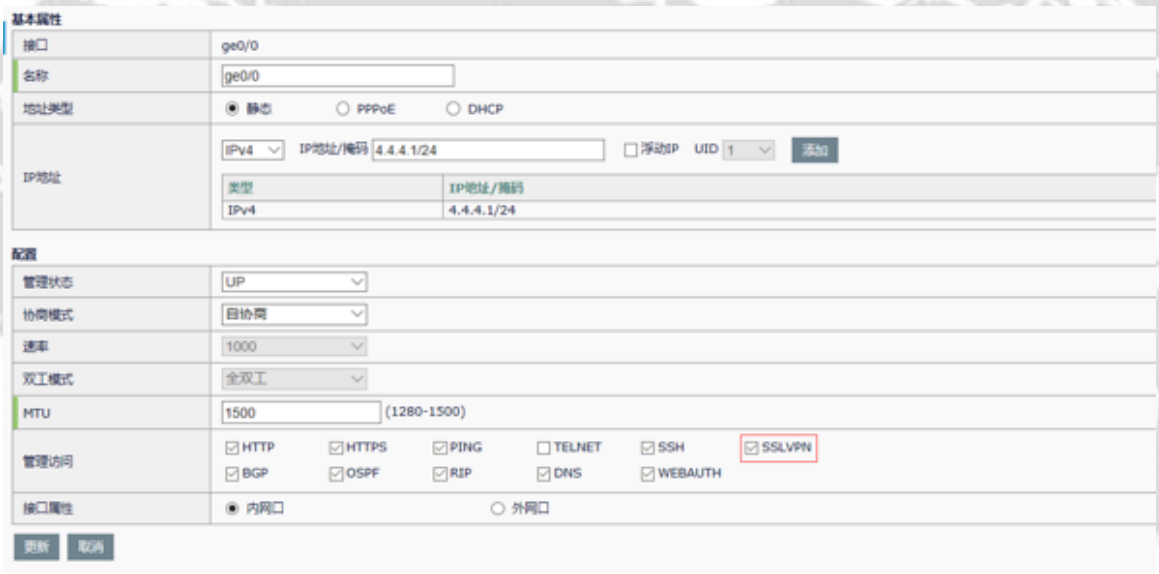


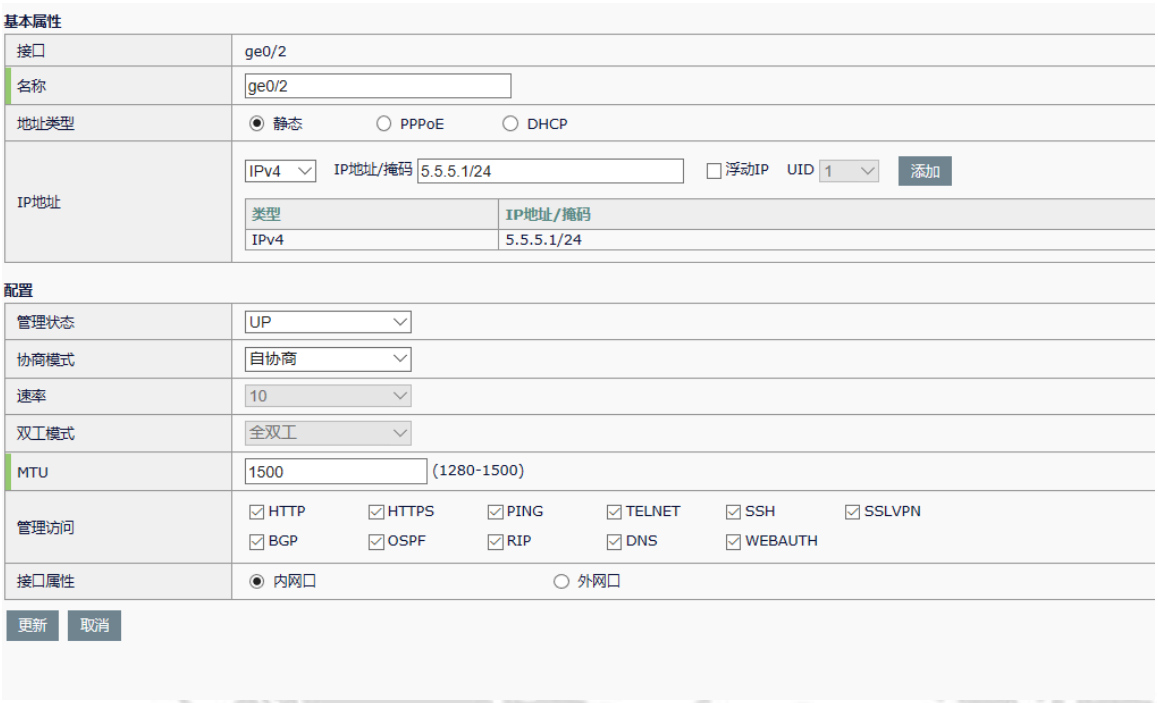
DUTge0/0 地址：4.4.4.1/24，ge0/2 地址：5.5.5.1/24

Client IP 地址：4.4.4.4/24

ServerIP 地址：5.5.5.5/24,默认网关为 5.5.5.1

(1) DUT：进入**网络>接口配置>物理接口**配置接口，ge0/0的IP地址配置为4.4.4.1/24， ge0/2的IP地址配置为5.5.5.1/24，





(2) 进入对象>用户>用户，点击新建，名称：test密码为123456。

(3) DUT：配置SSL VPN，进入网络>SSL VPN>SSL VPN配置，输入隧道地址10.1.1.1/24,地址池10.1.1.0/24，DNS1输入114.114.114.114，DNS2输入8.8.8.8，子网路由输入5.5.5.0/24和6.5.5.0/24，高级选项输入相应的客户端连接。

(4) PC:在PC上安装客户端

(5) PC:打开客户端，填写服务器地址4.4.4.1，输入用户名：test密码：123456，点击登录。

(6) 登录成功,在监控页面查看登录信息

(7) 通过 client 端 ping server 端 IP 地址，可以正常通信

第49章 VRF

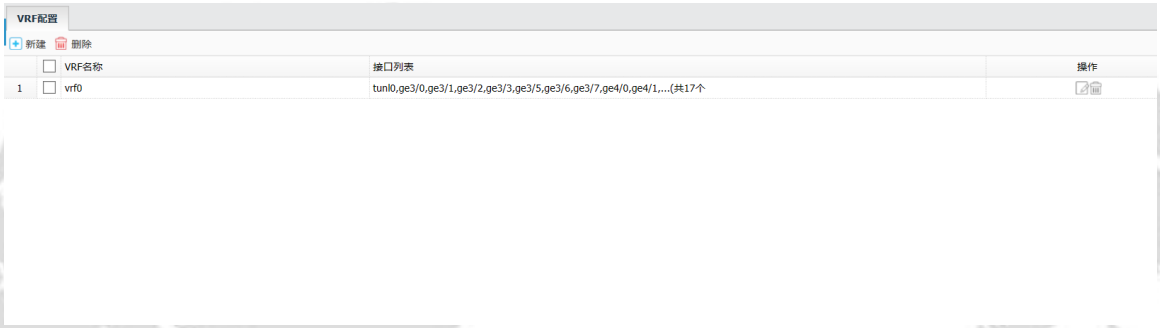
49.1 概述

一个系统通常仅限于一个设施使用，VRF 技术能够从一台设备划分出多个虚拟系统，每个虚拟系统可视为一台独立的转发设备

49.2 VRF配置

49.2.1 VRF 配置

1、进入**系统>VRF>VRF 配置**，如下图：



参数说明：

新建：新增一个 VRF 系统配置

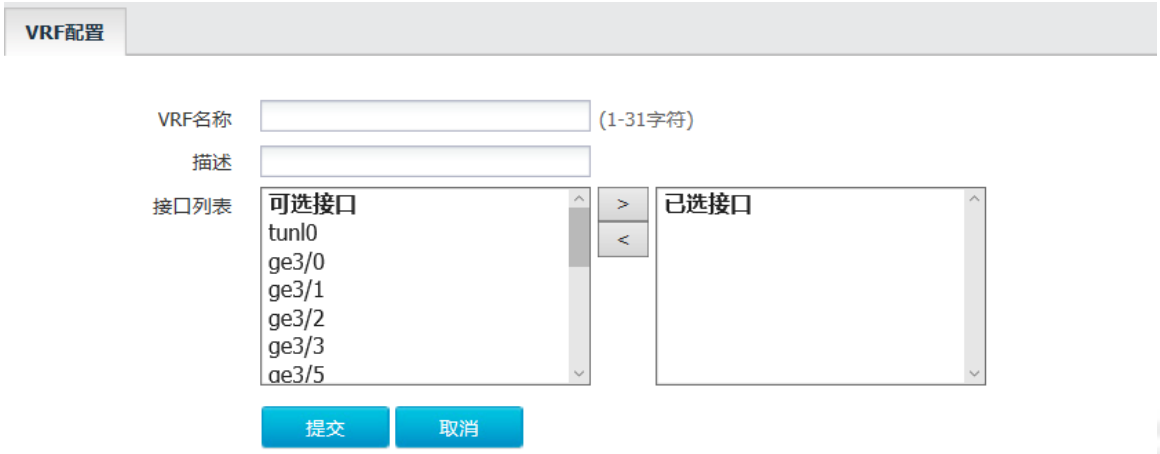
删除：删除选中 VRF 系统配置

源 IP：数据包的源地址，输入只支持主机地址格式。

接口列表：当前 VRF 系统中包含的接口

操作：修改或删除 VRF 系统

2、进入**系统>VRF>VRF 配置>新建**，如下图：



参数说明：

VRF 名称： VRF 系统的名称

描述：VRF 系统描述

可选接口：可被 VRF 系统选中的接口

已选接口：已被 VRF 系统选中的接口

提交：提交后已被选中接口加入 VRF 系统中

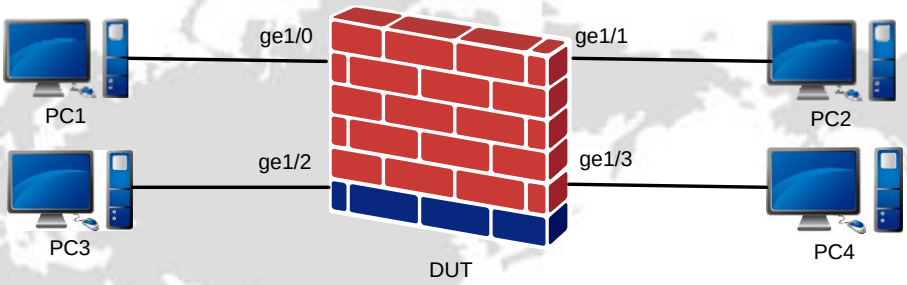
取消：取消当前的操作

注意：

接口加入 VRF 系统后才能对接口 ip 等属性进行配置

49.3 配置案例

49.3.1 多个 VRF 转发

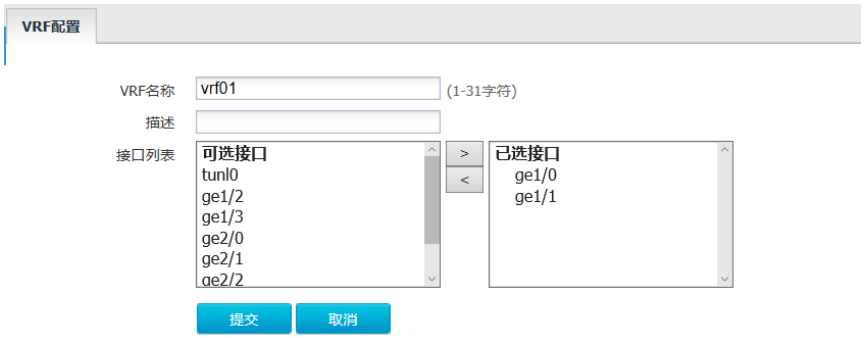


通过 console/telnet/web 访问配置 DUT

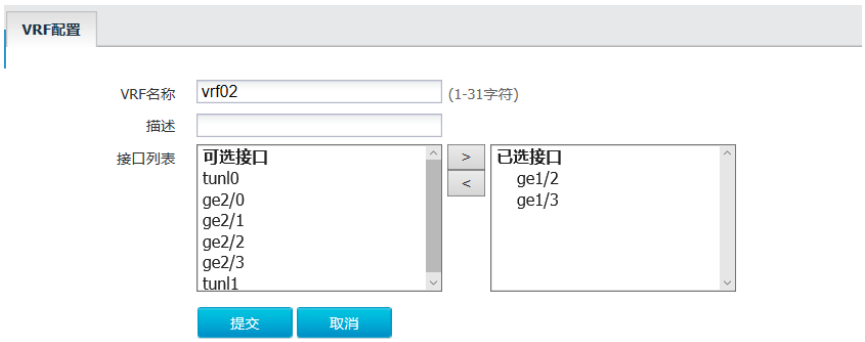
VRF01 ge1/0: 15.0.0.1/24　ge1/1: 31.0.0.1/24　PC1:15.0.0.10 网关 15.0.0.1 PC2:31.0.0.10/24 网关 31.0.0.1

VRF02 ge1/2: 15.0.0.1/24　ge1/3: 31.0.0.1/24　PC3:15.0.0.10 网关 15.0.0.1 PC4:31.0.0.10/24 网关 31.0.0.1

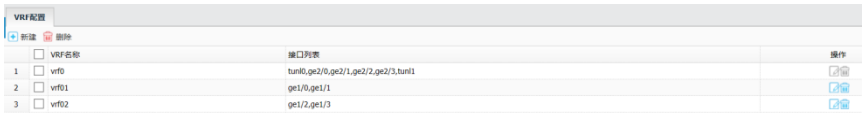
1、配置 VRF 子系统 VRF01：进入系统>VRF>VRF 配置，新建子系统 VRF01,将 ge1/0,ge1/1 加入到 VRF01



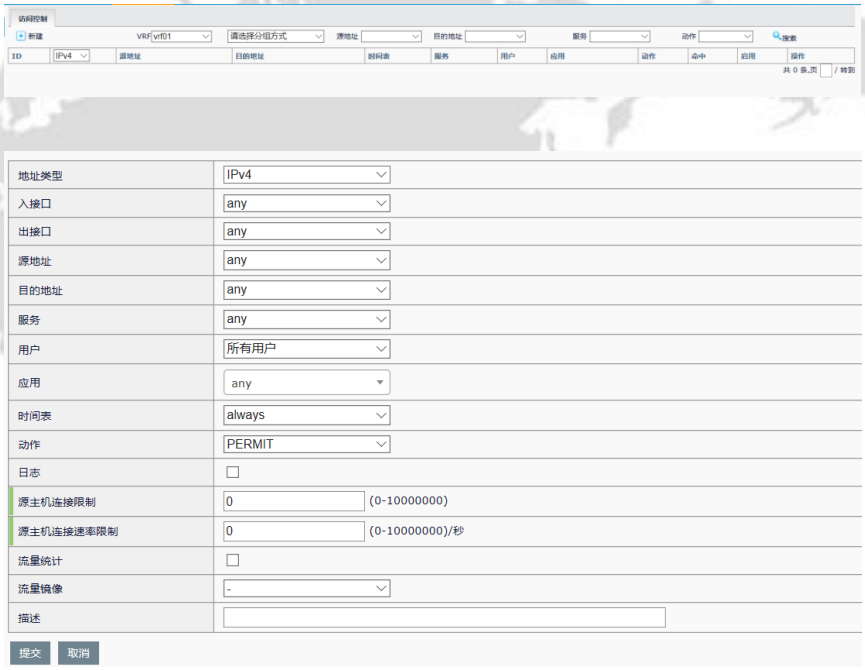
2、配置 VRF 子系统 VRF02：进入系统>VRF>VRF 配置，新建子系统 VRF02,将 ge1/2,ge1/3 加入到 VRF02



3、查看 VRF 配置，对应接口成功加入到相应 VRF

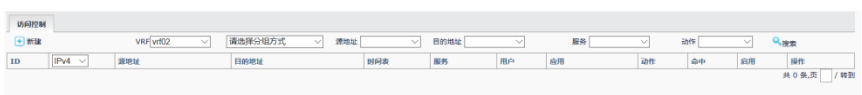


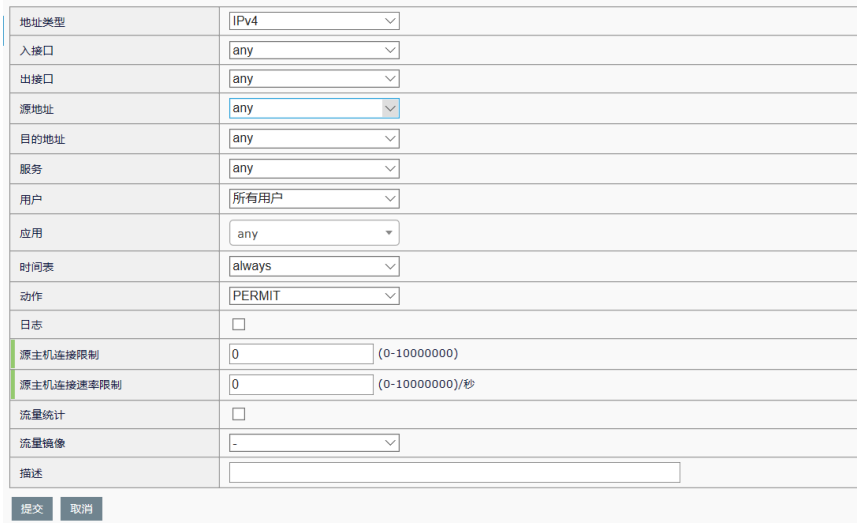
4、配置 VRF01 防火墙策略，进入策略>访问控制选择 VRF01 新建防火墙策略，配置全通策略



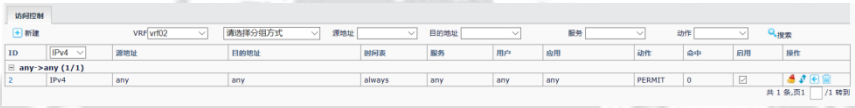
查看 VRF01 已配置的防火墙策略

5、配置 VRF02 防火墙策略，进入策略>访问控制选择 VRF02 新建防火墙策略，配置全通策略

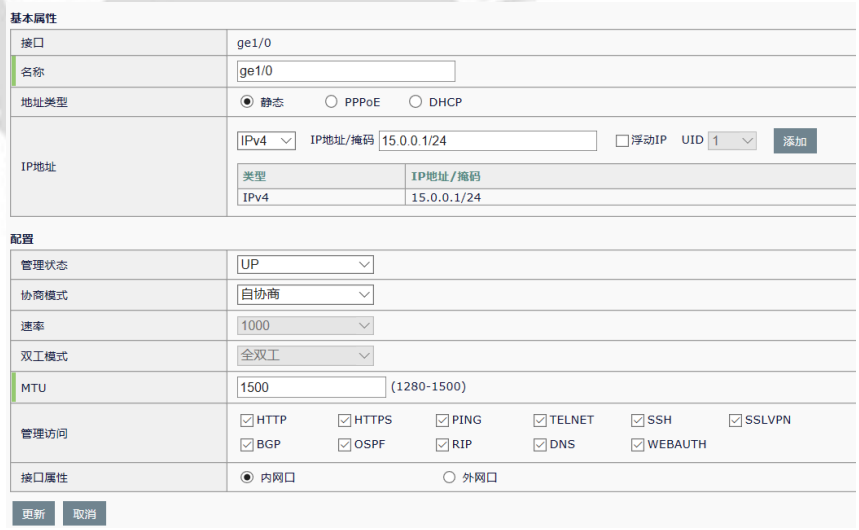


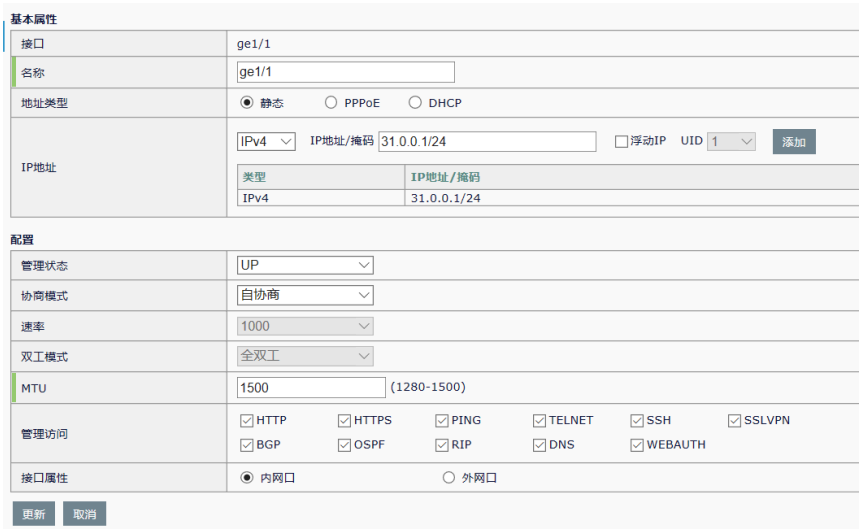


查看 VRF02 已配置的防火墙策略

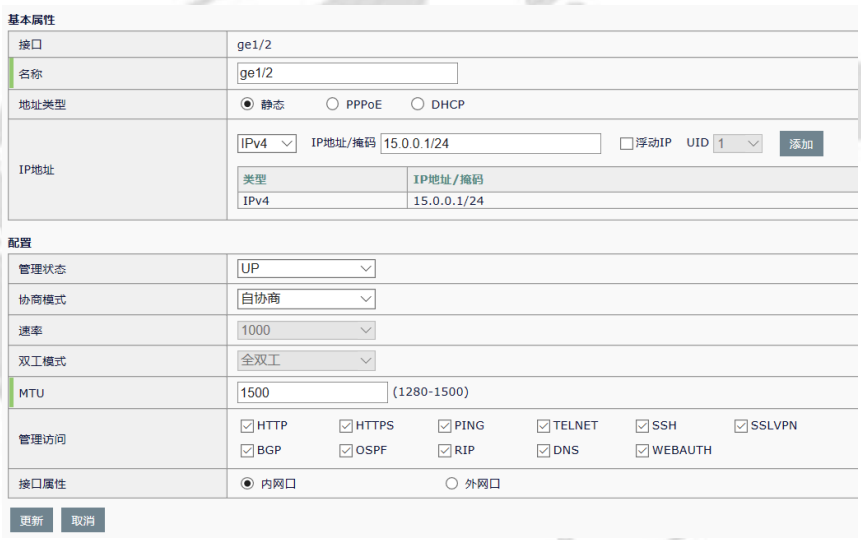


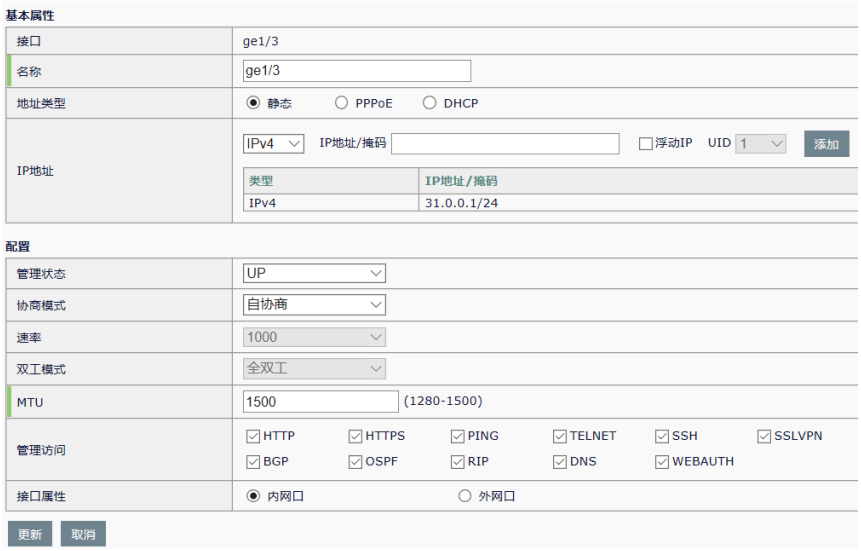
6、配置 VRF01 系统 ge1/0、ge1/1 的接口地址，进入网络>物理接口选择 ge1/0 配置接口地址 15.0.0.1/24，选择 ge1/1 配置接口地址 31.0.0.1/24



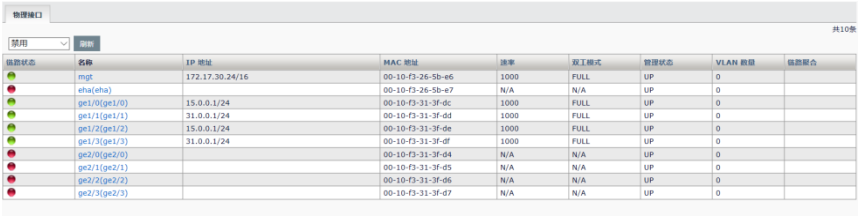


7、配置 VRF02 系统 ge1/2、ge1/3 的接口地址，进入网络>物理接口 选择 ge1/2 配置接口地址 15.0.0.1/24，选择 ge1/3 配置接口地址 31.0.0.1/24





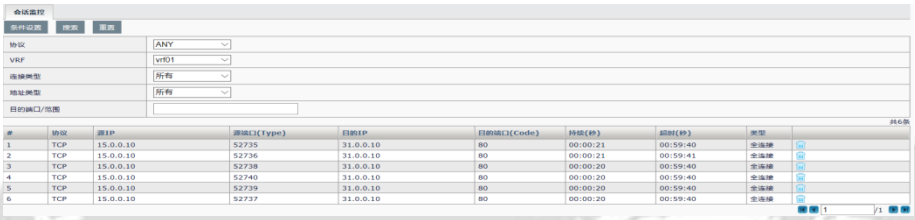
8、查看接口配置



9、业务访问

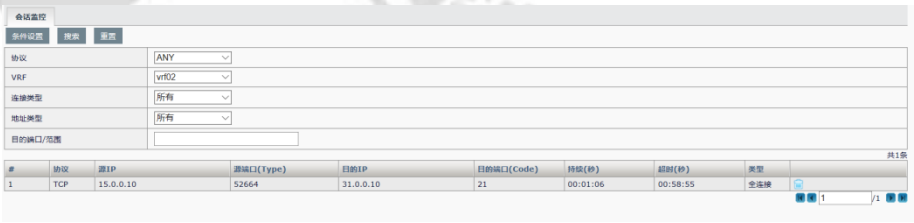
PC1，PC2 间互 ping 能通，PC1 可访问 PC2（开启 HTTP）服务，在**统计>会话监控页面搜索**

VRF01 会话,可观察到 PC1 访问 PC2 的 HTTP 连接

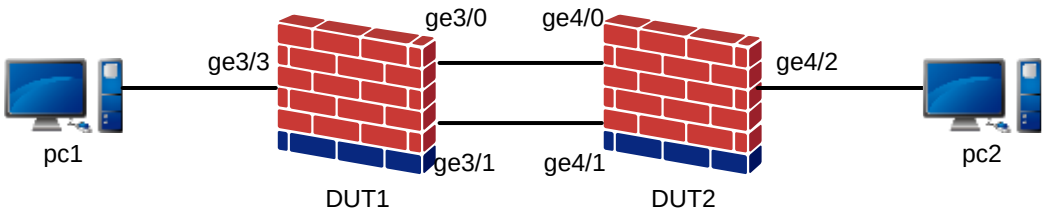


PC3，PC4 间互 ping 能通，PC3 可访问 PC4（开启 FTP）服务，在**统计>会话监控页面搜索**

VRF02 会话,可观察到 PC3 访问 PC4 的 ftp 连接



49.3.2 VRF 下支持防火墙策略



通过 console/telnet/web 访问配置 DUT

DUT1: ge3/3: 15.0.0.1/24 ge3/0: 20.0.0.1/24 ge3/1: 21.0.0.1/24 三个接口都属于 VRF01

静态路由 31.0.0.0/24 下一跳 20.0.0.2

PC1:15.0.0.10/24 网关 15.0.0.1

DUT2: ge4/2: 31.0.0.1/24 ge4/0: 20.0.0.2/24 ge4/1:21.0.0.2/24 不加入 VRF 系统

静态路由 15.0.0.0/24 下一跳 20.0.0.1

PC2:31.0.0.10/24 网关 31.0.0.1

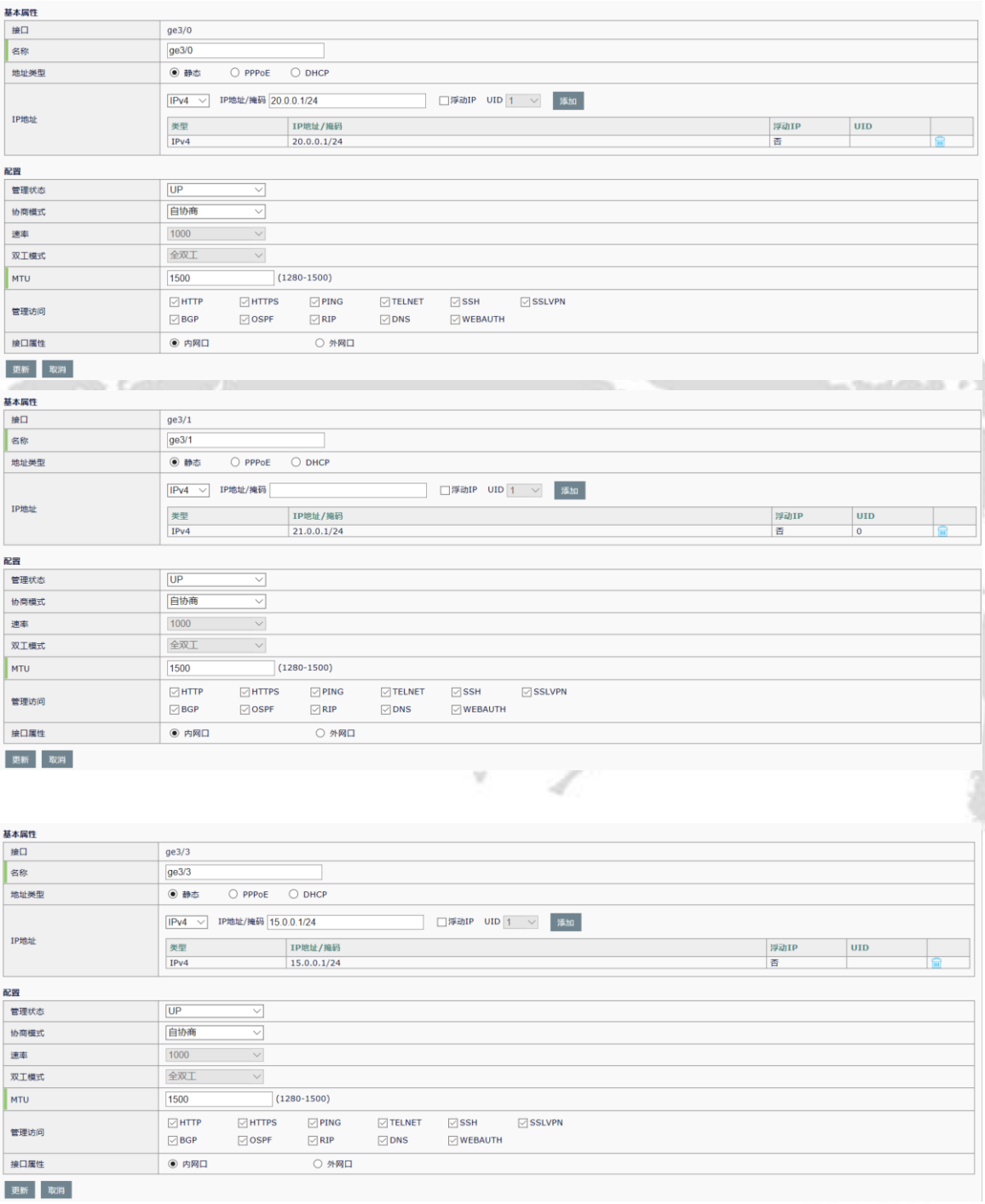
1、配置 VRF 子系统 VRF01：进入系统>VRF>VRF 配置，新建子系统 VRF01,将 ge3/0、ge3/1、ge3/3 加入到 VRF01

VRF配置

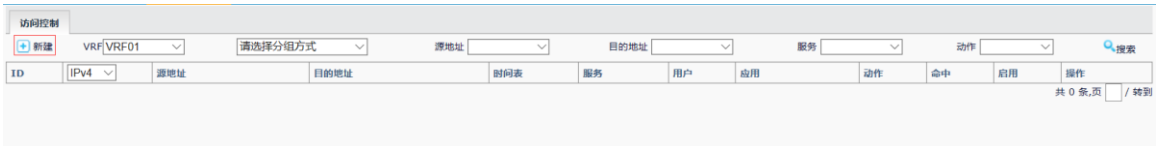
新建 删除

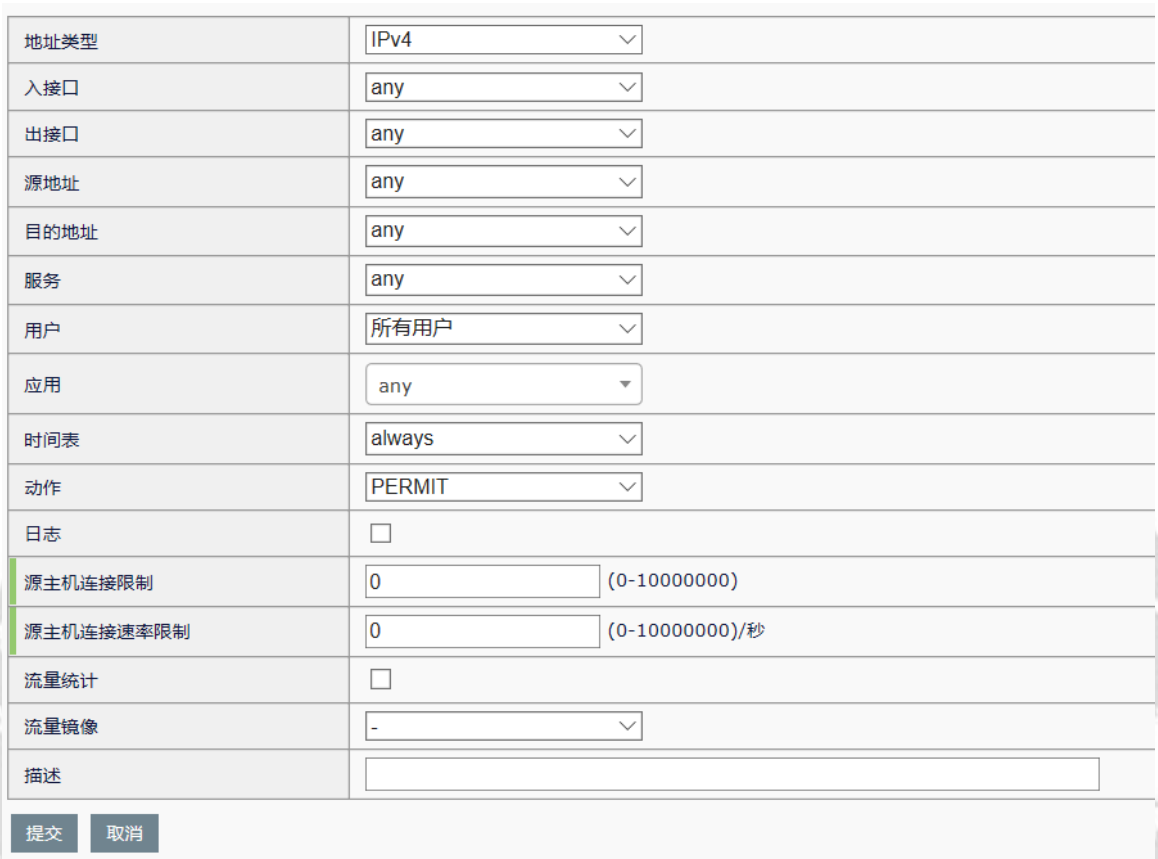
		VRF名称	接口列表
1	☐	vrf0	tunl0,ge3/2,ge3/4,ge3/5,ge3/6,ge3/7,ge4/0,ge4/1,ge4/2,ge4/3,...(共13个
2	☐	VRF01	ge3/0,ge3/1,ge3/3

2、配置 VRF 子系统 VRF01 接口地址：进入网络>接口，配置 ge3/0、ge3/1、ge3/3 接口地址



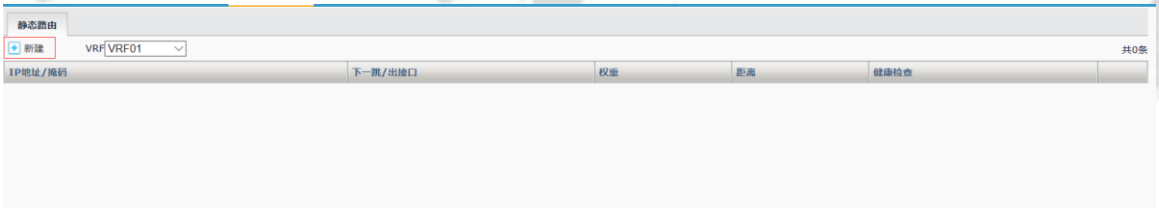
3、配置 VRF01 防火墙策略,配置全通策略

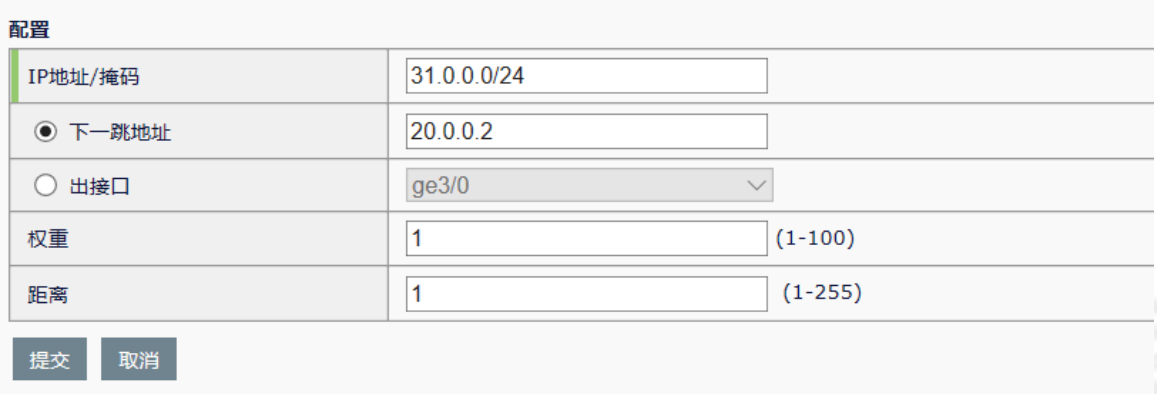




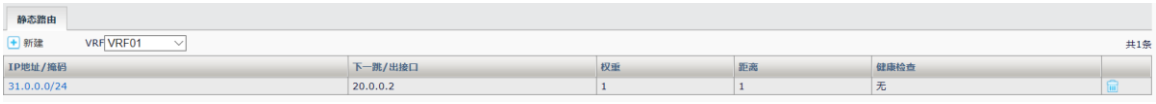
4、配置 DUT2 接口地址，配置对应策略，确保 DUT1，DUT2 直连互通。

5、DUT1 VRF01 配置静态路由





6、DUT1 VRF01 配置静态路由

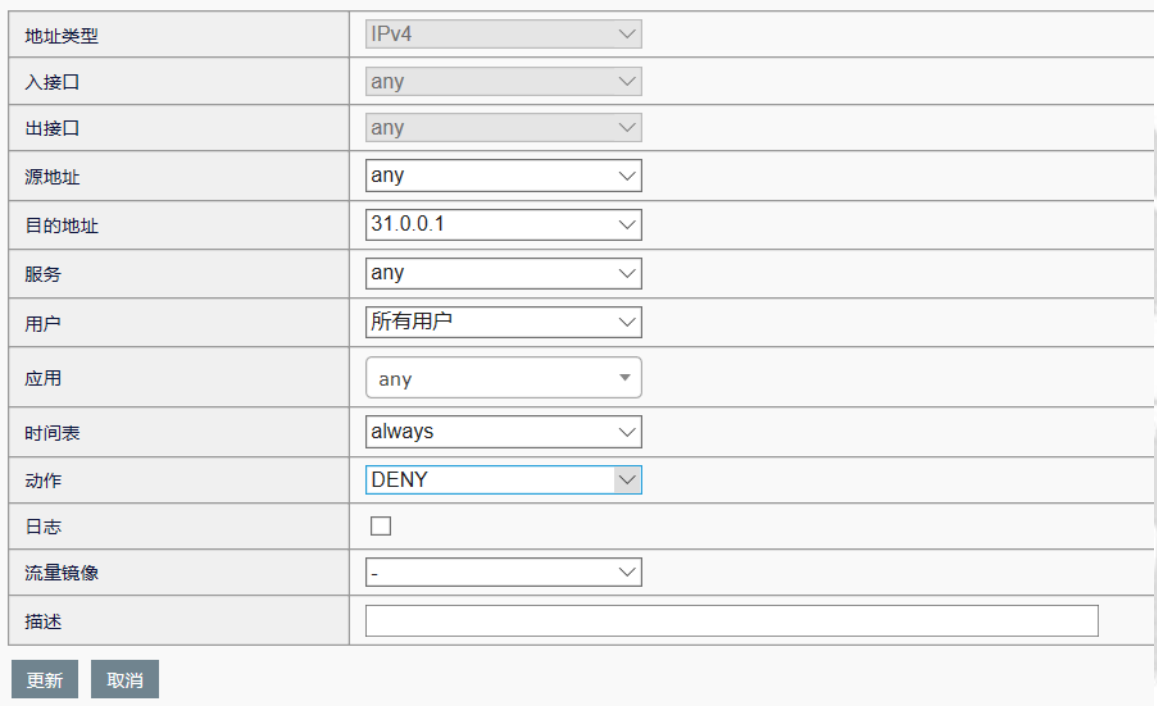


7、PC1 长 ping 目标地址 31.0.0.1

DUT2 上 debug ip packet receive 可观察到从 ge4/0 口收到的报文

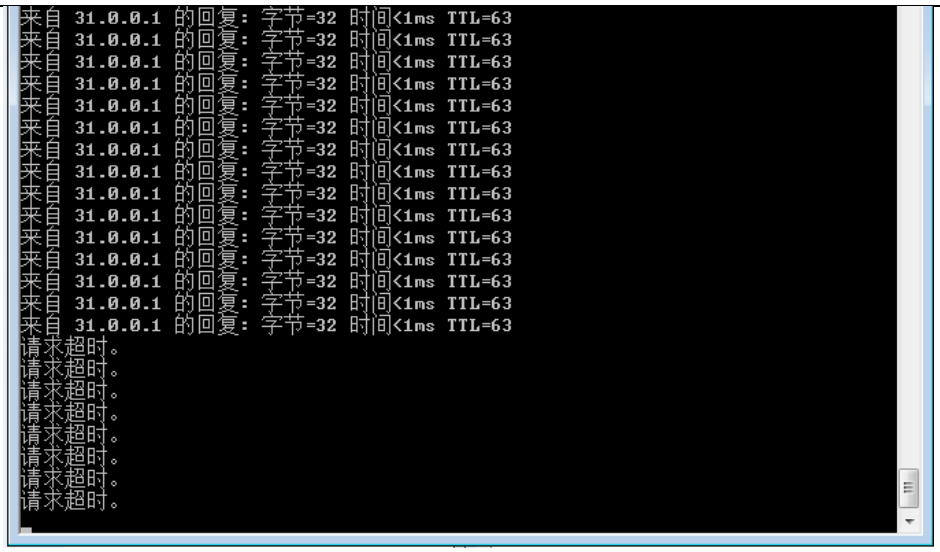
```
      flags 0 frag_offset = 0 ttl = 127 protocol = 1 checksum = 47290,
      src = 15.0.0.101 dest = 31.0.0.1 if = ge4/0 ,
      recv ,  type 0
```

8、修改防火墙策略 deny 目的地址为 31.0.0.1 的报文

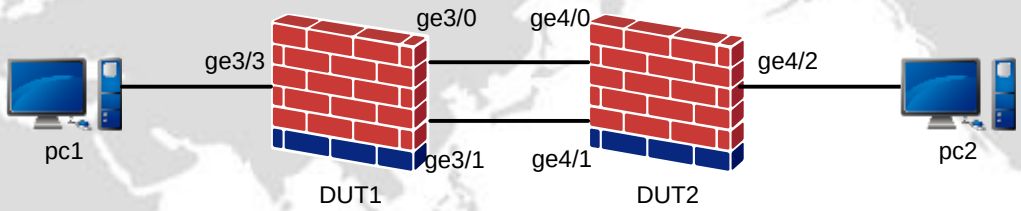


9、观察到 pc1 发起的 ping 包不通，DUT1 上 debug ip packet detail

```
[Core 1][VRF1][4842968026] DROP for policy mode is deny
[Core 1][VRF1][4842968026] ++++++++++++++++++++DEBUG DROP PACKET++++++++++++++++++++
[Core 1][VRF1][4842968026] ipv4 drop, tb_packet_handle_loop flow_main.c:254
[Core 1][VRF1][4842968026] ipv4 drop, policy_handle_by_mode tb_policy.c:3758
[Core 1][VRF1][4842968026] IPv4:  version = 4 hdrlen = 5 tos = 0 total len = 60 ID = 22210 ,
      flags 0 frag_offset = 0 ttl = 127 protocol = 1 checksum = 46745,
      src = 15.0.0.101 dest = 31.0.0.1 if = ge3/3 ,
      drop ,  type 0
```



49.3.3 VRF 下支持静态路由和策略路由



通过 console/telnet/web 访问配置 DUT

DUT1: ge3/3: 15.0.0.1/24 ge3/0: 20.0.0.1/24 ge3/1: 21.0.0.1/24 三个接口都属于 VRF01

静态路由 31.0.0.0/24 下一跳 20.0.0.2

PC1:15.0.0.10/24 网关 15.0.0.1

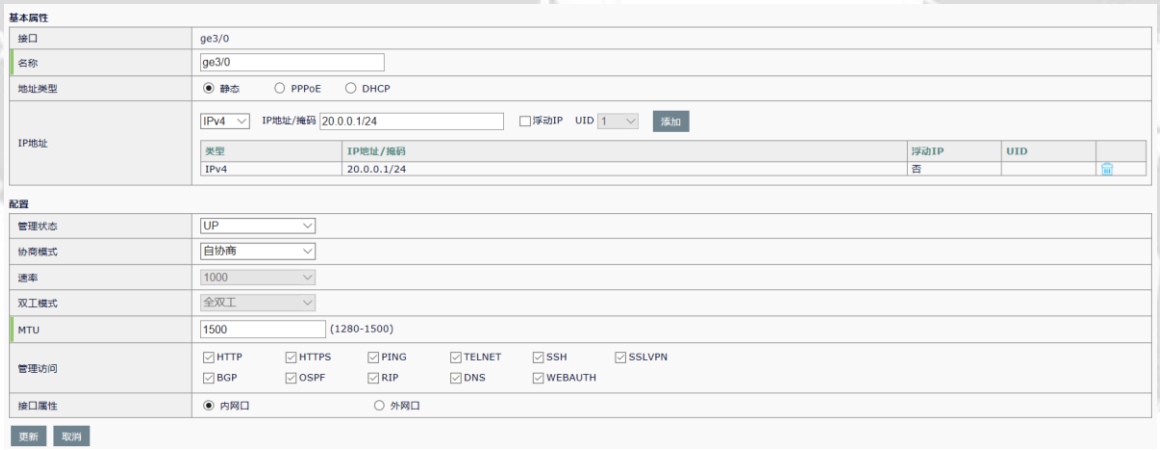
DUT2: ge4/2: 31.0.0.1/24 ge4/0: 20.0.0.2/24 ge4/1:21.0.0.2/24 不加入 VRF 系统

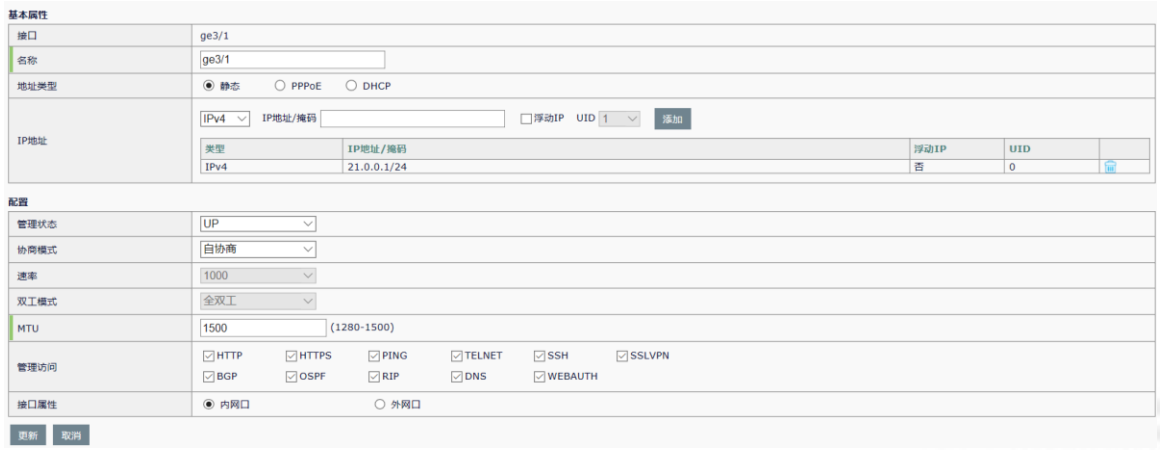
静态路由 15.0.0.0/24 下一跳 20.0.0.1

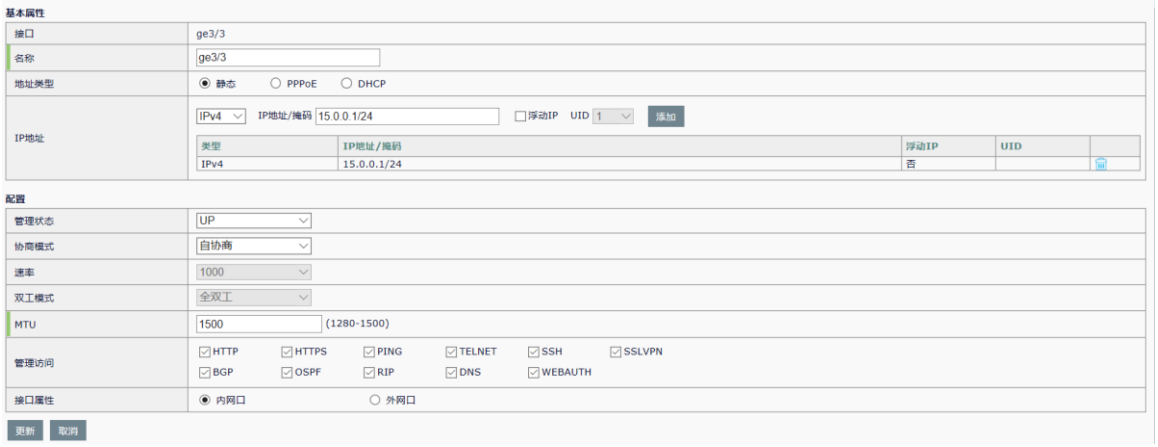
PC2:31.0.0.10/24 网关 31.0.0.1

1、配置 VRF 子系统 VRF01：进入系统>VRF>VRF 配置，新建子系统 VRF01,将 ge3/0、ge3/1、ge3/3 加入到 VRF01

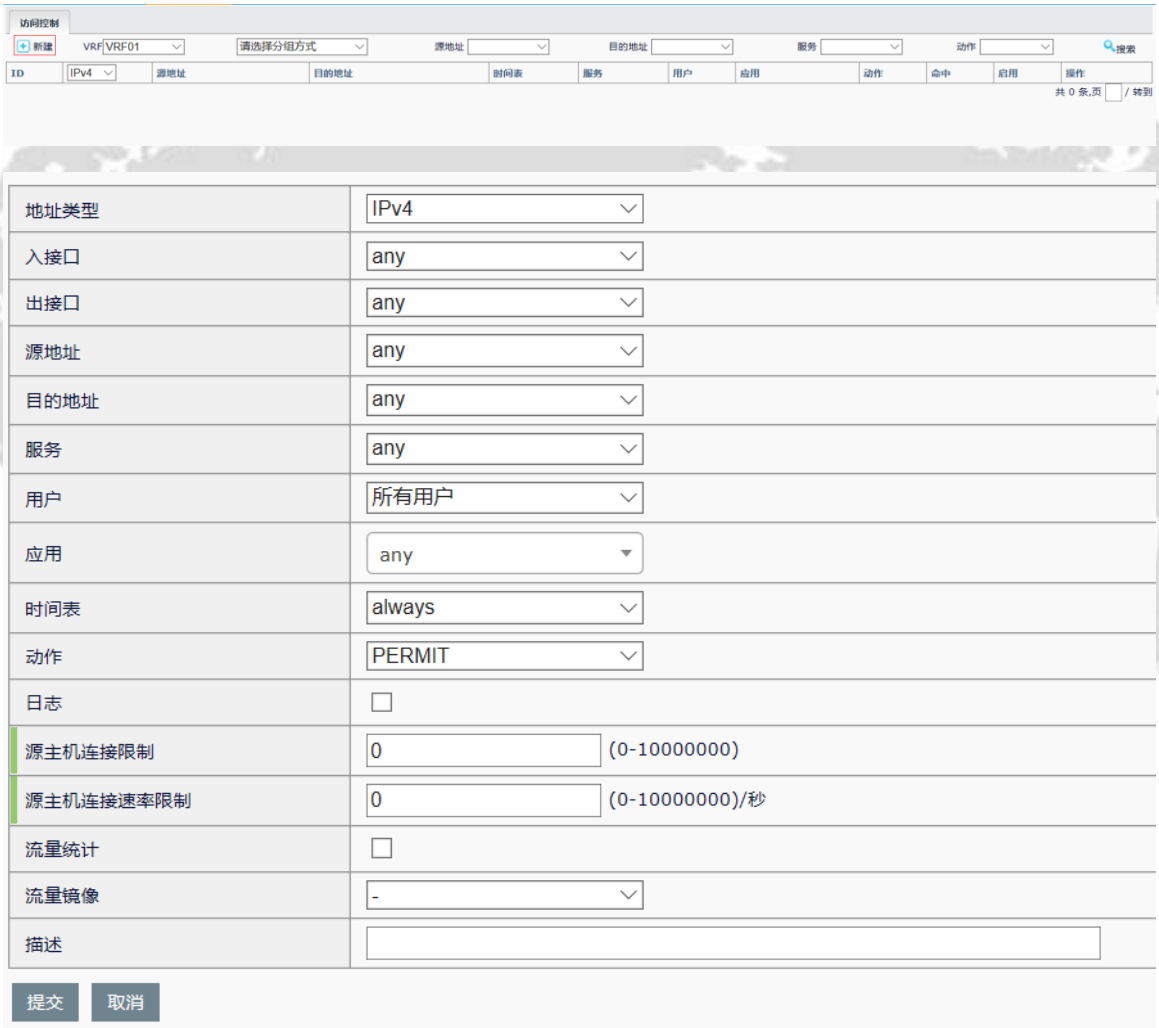
2、配置 VRF 子系统 VRF01 接口地址：进入网络>接口，配置 ge3/0、ge3/1、ge3/3 接口地址





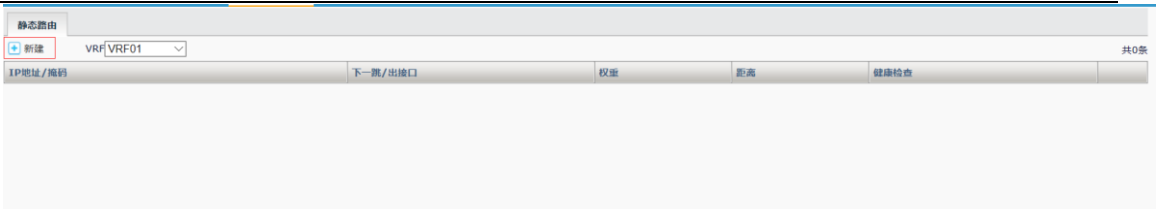


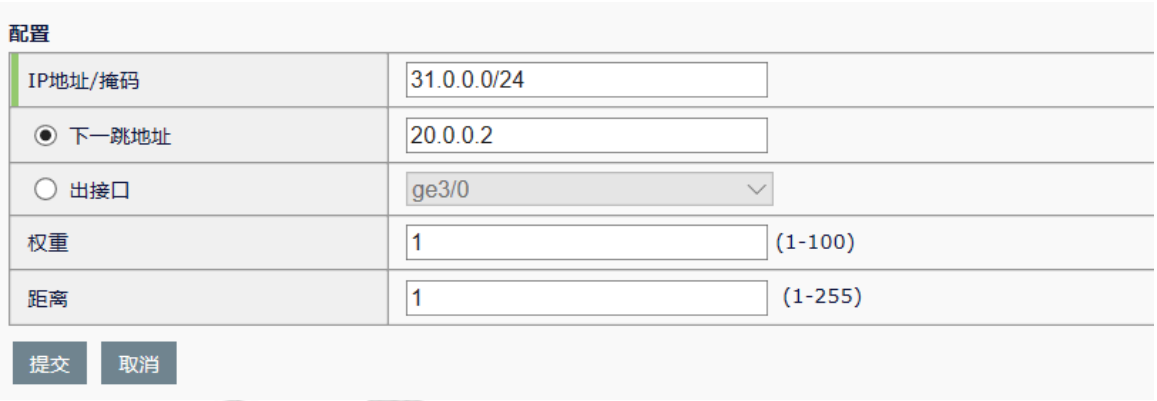
3、配置 VRF01 防火墙策略,配置全通策略



4、配置 DUT2 接口地址，配置对应策略，确保 DUT1，DUT2 直连互通。

5、DUT1 VRF01 配置静态路由





6、DUT1 VRF01 配置静态路由

7、PC1 长 ping 目标地址 31.0.0.1

DUT2 上 debug ip packet receive 可观察到从 ge4/0 口收到的报文

```
        flags 0 frag_offset = 0 ttl = 127 protocol = 1 checksum = 47290,
        src = 15.0.0.101 dest = 31.0.0.1 if = ge4/0 ,
        recv ,  type 0
```

8、DUT1 配置策略路由，目的地址 31.0.0.0/32 的网段下一跳指向 21.0.0.2，新建地址对象 31.0.0.0/24

新建地址对象

名称	31.0.0.0/24
描述	
类型	IPV4 IPV6
成员	主机 子网 31.0.0.0/24 范围 - ISP地址库 ISP_CERNET.dat(教育网) 添加 31.0.0.0/24 删除

提交 取消

配置策略路由

策略路由

状态 ☑
入接口 ge3/3
源地址 any
目的地址 31.0.0.0/24
用户 所有用户
服务 any
应用 any
时间 always
下一跳信息

网关 21.0.0.2 权重 1 添加到列表

	类型	网关	出接口	健康检查	权重	命中次数	操作
1	网关	21.0.0.2	-	-	1	0	删除

多路径选择 根据源IP

提交 取消

9、DUT2 开启 debug ip packet receive 观察到报文走策略路由从 ge4/1 收到请求报文

```
[Core 1][VRF0][4295711619] IPV4:  version = 4 hdrlen = 5 tos = 0 total len = 60 ID = 23148 ,
      flags 0 frag_offset = 0 ttl = 127 protocol = 1 checksum = 45807,
      src = 15.0.0.101 dest = 31.0.0.1 if = ge4/1 ,
      recv ,  type 0
```