# 浪潮 ADC-3000 系列应用交付产品

# 配置管理手册

| | |
|---|---|
| 手册版本 | V1.0 |
| 产品版本 | V4.0 |
| 资料状态 | 发行 |



## 免责声明

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

# 目录

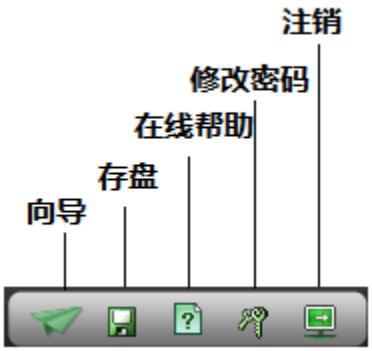
# 1 第1章 Web 管理介绍

## 1.1 WEB管理概述

通过运行Internet浏览器的任何计算机使用HTTP或一个安全的HTTPS连接，便能够配置并管理应用交付控制设备。在进行Web管理前，必须配置应用交付控制设备使其能够接受来自指定接口的HTTP或HTTPS管理。

推荐使用IE8.0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 工具条




### 1.2.1 向导

使用**配置向导**，可以快速的配置网络、服务器负载及链路负载，使得用户能够迅速的完成设备的初步部署

### 1.2.2 存盘

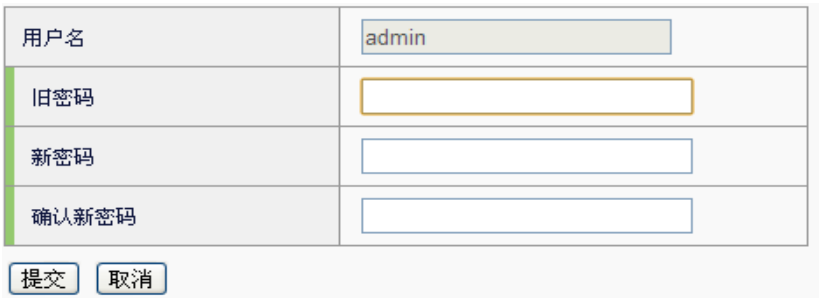
**存盘**按钮永久保存配置更改。应用交付控制设备默认不永久保存配置更改，如果进行配置更改后，不点击**存盘**按钮，则设备下一次启动后会丢失上次所做的配置。

### 1.2.3 在线帮助

**在线帮助**按钮在新窗口中打开帮助页面，帮助页面包括应用交付控制设备各功能介绍和相关配置项说明。用户可以根据需要查看相关帮助信息。

### 1.2.4 修改密码

**修改密码**按钮在新窗口中打开修改密码页面。




**参数说明：**

**用户名：**管理员名称。

**旧密码：**管理员的旧密码。

**新密码：**设置的新密码。

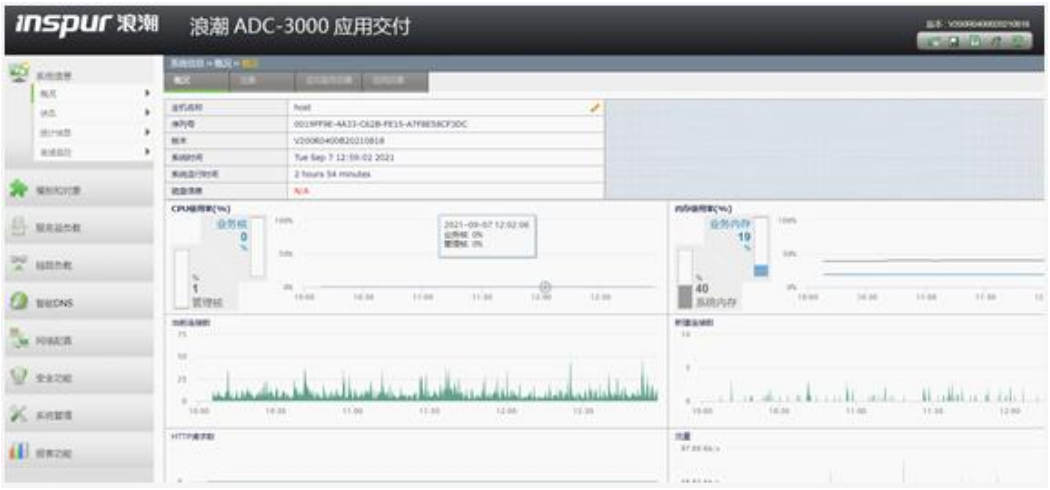
**确认新密码：**确认设置的新密码。

### 1.2.5 注销

**注销**按钮立即注销当前登录用户。下一次进行 Web 管理时会要求输入用户名和密码。

## 1.3 Web管理

Web管理界面由菜单、工具条、信息栏和主内容区页面组成，每个菜单有相应的一个或多个子菜单，最多可能有四级菜单。当点击一个菜单项目，如系统信息，系统菜单会扩展为：概况、状态、统计、会话监控四个子菜单，同时默认第一个二级菜单关联的三级菜单会在页面右侧主内容区上部分区域以“页签”的方式显示，相关联的页面会在主内容区中显示。右侧主内容区域的页面默认显示第一个子菜单内容。




### 1.3.1 菜单

菜单提供了应用交付控制设备的主要配置选项。

**系统信息**：系统相关的一些关键信息展示。包括概况、状态、统计信息、会话监控。

**模板和对象**：一些系统通用的配置项，可以供其他模块引用。包括对象管理、健康检查、tRule。

**服务器负载**：服务器负载相关配置。包括虚拟服务、模板、服务池、服务器节点、SSL 证书。

**链路负载**：链路负载相关配置。包括虚拟链路（出站）、智能 DNS（入站）。

**智能 DNS**：智能 DNS 相关配置。包括 DNS 服务器，本地负载全局负载，以及公共对象。

**网络配置**：网络相关配置。包括接口、路由、设备 IP、ARP、NAT、协议管理。

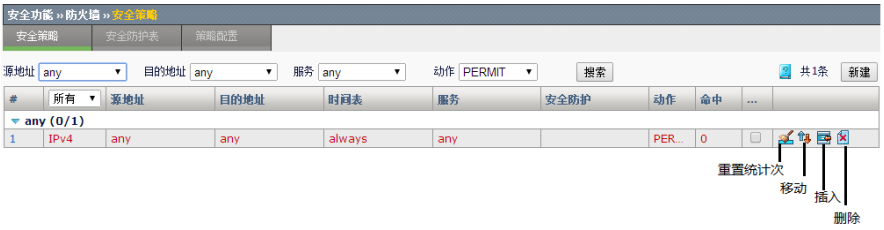
**安全功能**：安全相关配置。包括防火墙、防攻击、HTTP 防护。

**系统管理**：系统相关的配置。包括配置、管理员、版本管理、许可管理、服务管理、高可用性、VRRP、SNMP、日志管理。

**报表功能**：报表相关的配置以及查看、下载生成的报表。

### 1.3.2 列表

很多管理配置页面是列表的形式，例如管理员、接口、安全策略等。下图为应用交付控制设备列表图。




列表中的条目显示项信息。列表中最右面的列一般为图标按钮列，可对该条目进行一些操作，例如**重置统计次数、移动、插入、删除**等。点击列表中的名称列或者 ID 等关键字类型的列时，进入到编辑该条目的页面，这样的列文字一般显示为蓝色。例如这里的#列，即 ID 列。

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

### 1.3.3 图标

页面中有很多图标帮助进行配置管理操作。当鼠标停留到图标上时，会出现提示信息，以帮助理解图标的含义。下表对页面中的图标进行说明。

| 图标 | 名称 | 说明 |
|---|---|---|
| | 展开 | 展开当前条目 |
| | 上移 | 将当前条目向上移动一个位置 |
| | 下移 | 将当前条目向下移动一个位置 |
| | 移动 | 移动当前条目到指定位置 |
| | 插入 | 在当前条目前面插入一个新条目 |
| | 删除 | 删除一个条目 |

## 1.4 设备默认配置

出厂的 ADC 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 ADC 进行管理、配置。

### 1.4.1 管理接口的默认配置

管理接口（MGT）的默认地址配置为 192.168.1.250/24。允许对该接口进行 PING 和 HTTPS 操作。

### 1.4.2 默认管理员用户

系统默认的管理员用户为 admin，密码为 adc.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。

# 2 第2章 配置向导

## 2.1 配置向导概述

使用配置向导，可以快速的配置网络、服务器负载及链路负载，使得用户能够迅速的完成设备的初步部署。

## 2.2 网络配置向导

通过网络配置向导，可以一站式快速完成网络基础配置，包括选择接入外网的物理接口、选择接入内网的物理接口，在物理接口上配置名称、IP 地址并根据 IP 地址进行运营商自动识别、静态路由配置。

**配置步骤：**

进入**配置向导>网络配置向导**，如下图：


点击**网络配置向导**，进入**内外网接口配置**，如下图：


**外网接口配置：**选择连接外网的接口进行配置

**外网接口：**接入到外网的接口

**名称：**接入到外网的接口的名称，最多 63 字符

**IP 地址：**接入到外网的接口的 IP 地址，格式为 IP 地址/掩码长度

**运营商：**根据 IP 地址识别出运营商

点击**添加配置**添加到外网配置列表

**内网接口配置：**选择连接内网的接口进行配置

**内网接口：**接入到内网的接口

**名称：**接入到内网的接口的名称，最多 63 字符

**IP 地址：**接入到内网的接口的 IP 地址，格式为 IP 地址/掩码长度

点击**添加配置**添加到内网配置列表

点击 删除一条网络配置

点击**下一步**，继续进行**路由配置**，如下图：


**IP 地址/掩码：**路由的目的 IP 地址与掩码长度

**下一跳地址：**路由下一跳 IP

**出接口：**路由的出接口

**权重：**路由权重，范围 1-100

**距离：**路由优先级，范围<1-255>

点击**添加配置**，添加到路由配置列表

点击**上一步**，可以返回上一步配置界面

点击**下一步**，进入到**网络配置预览**，如下图


**外网接口配置**：连接到外网的接口配置信息预览

**内网接口配置**：连接到内网的接口配置信息预览

**路由配置**：路由配置信息预览

点击**上一步**，可以返回上一步配置页面

**点击确定**，完成本次网络配置向导，给出“配置已经下发！”的提示信息，如下图：

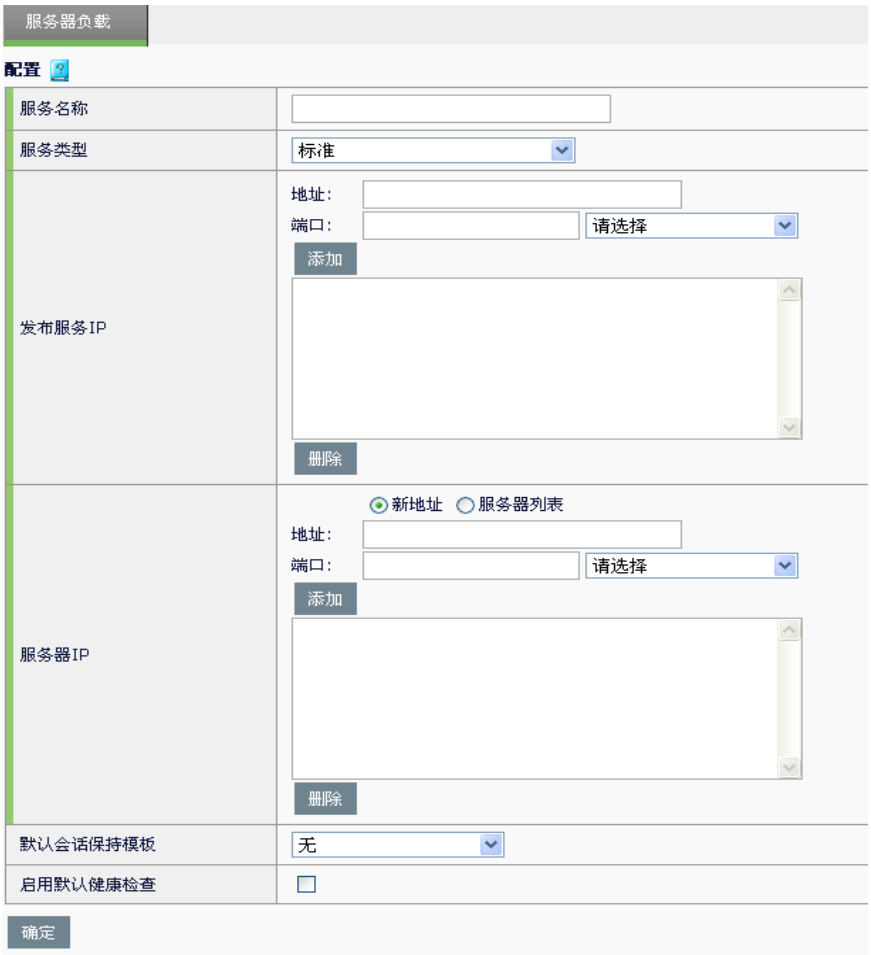

## 2.3 配置服务器负载

服务器负载向导是配置虚拟服务及相关服务池与服务器节点的向导。

**配置步骤：**

1. 点击**服务器负载**，如下图所示：


出现服务器负载向导配置界面，如下图所示：




**服务器负载配置参数说明：**

**名称**：虚拟服务的识别名，最多可输入 63 个有效字符。

**服务类型**：是指虚拟服务的工作类型。

**发布服务 IP**： 虚拟服务 IP 地址、端口号。

**地址**：虚拟服务提供服务的地址，客户端可向该目标地址发送请求。

**端口**：虚拟服务提供的服务协议类型的端口号，客户端可向该端口发送对应的请求。配置范围为 0 至 65535，配置为 0 时表示所有端口。

点击**添加**添加一个虚拟服务。

点击**删除**删除一个虚拟服务。

**服务器 IP**：真实服务器 IP 地址与端口号。

**地址**：指定服务池中服务成员的 IP 地址，可以新建也可以从服务器列表中选取。

**端口**：指定服务池中服务成员的端口。可以自己手动定义。

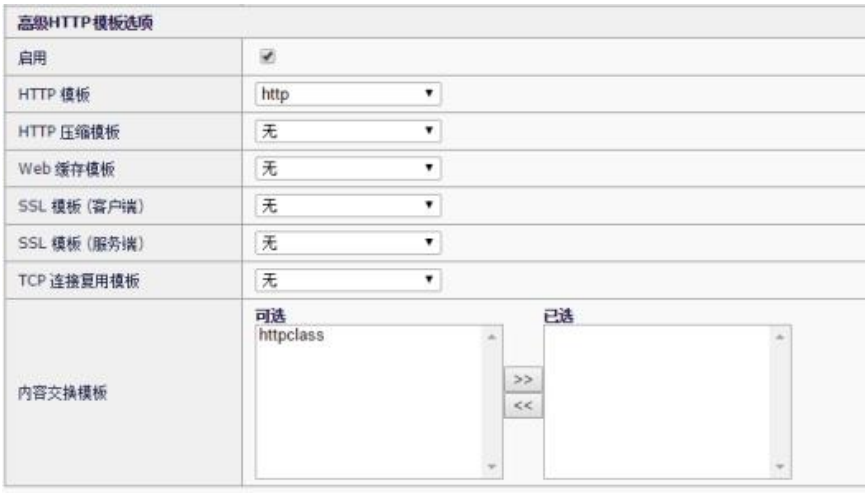
点击**添加**添加一个真实服务器。

点击**删除**删除一个真实服务器。

**默认会话保持模板**：可选择在该虚拟服务中生效的会话保持模板。

**启用默认健康检查**：为该虚拟服务进行默认健康检查。

当选择**服务类型**为 **HTTP** 时，还会出现**高级 HTTP 模板选项**，选择**启用**后，将会出现如下图所示的选项：




**HTTP 模板**：可选择预制或自定义的 HTTP 服务处理的模板，具体配置见相关章节。

**HTTP 压缩模板**：可选择预制或自定义的 HTTP 压缩处理的模板，具体配置见相关章节。

**Web 缓存模板**：可选择预制或自定义的 Web 缓存处理的模板，具体配置见相关章节。

**SSL 模板（客户端）**：针对客户端 SSL 流量进行处理的模板，具体配置见相关章节。

**SSL 模板（服务端）**：针对服务端 SSL 流量进行处理的模板，具体配置见相关章节。

**TCP 连接复用模板**：可选择预制或自定义的 TCP 连接复用的模板，具体配置见相关章节。

**内容交换模板**： HTTP 协议进行内容交换处理的模板，具体配置见相关章节。

## 2.4 配置链路负载

链路负载向导是配置虚拟链路及相关链路池与链路节点的向导。

**配置步骤：**

点击**链路负载**，如下图所示：


出现链路负载向导配置页面，如下图所示：


点击**下一步**开始配置。


**外网端口：**外网接入的接口。

**下一跳地址：**运营商提供的外网接入的下一跳地址。

**运营商：**选择网络服务的运营商。

**上行带宽：**配置该条链路的上行总带宽。

**下行带宽：**配置该条链路的下行总带宽。

点击**下一步**，配置**源 NAT 地址组**：


**起始地址：**源 NAT 地址池的开始地址。

**结束地址：**源 NAT 地址池的结束地址。

点击**下一步**，配置**链路出站策略：**


系统会根据链路配置情况，智能生成链路出站策略，用户可根据自己的实际情况进行选择。

点击**下一步**，配置**特定用户上网策略：**


**用户 IP：**特殊用户的 IP 地址。

**出站链路：**特殊用户的流量出站链路。

**可选应用：**对指定应用执行此策略。

点击**下一步**，配置**链路常用域名服务器：**


**服务器 1**：出站链路首选的 DNS 服务器。

**服务器 2**：出站链路备选的 DNS 服务器。

# 3 第3章 系统信息

## 3.1 系统信息概述

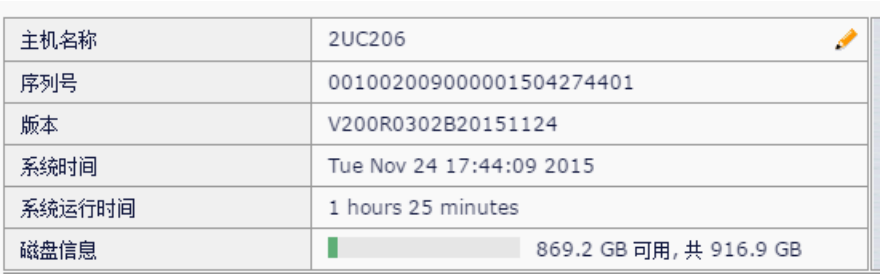
通过 Web 登录设备后默认进入系统信息页面，该页面显示系统当前运行状态和高级别日志信息。本章介绍该页面中各个部分。

## 3.2 概况

进入**系统信息>概况**，可以查看系统概况。

### 3.2.1 查看主机信息

进入**系统信息>概况**，可以看到主机信息。



| | |
|---|---|
| 主机名称 | 2UC206 |
| 序列号 | 00100200900000150427440l |
| 版本 | V200R0302B20151124 |
| 系统时间 | Tue Nov 24 17:44:09 2015 |
| 系统运行时间 | 1 hours 25 minutes |
| 磁盘信息 | 869.2 GB 可用, 共 916.9 GB |

**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。

**设备序列号：**ADC 应用交付控制系统的唯一标识，是设备出厂时设定好的。

**版本：**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。

**系统运行时间：**表示系统从上次启动已经运行的时间。

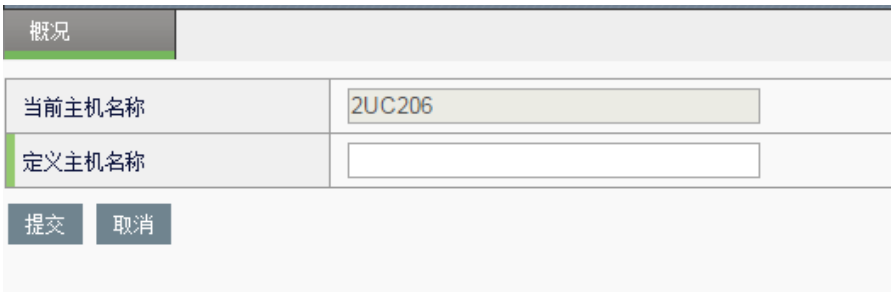
**磁盘信息：**表示设备上存储磁盘的容量信息。

### 3.2.1 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：**

**系统信息>概况**，在主机名称一栏中点击**图标** 




**当前主机名：** ADC 目前主机名。

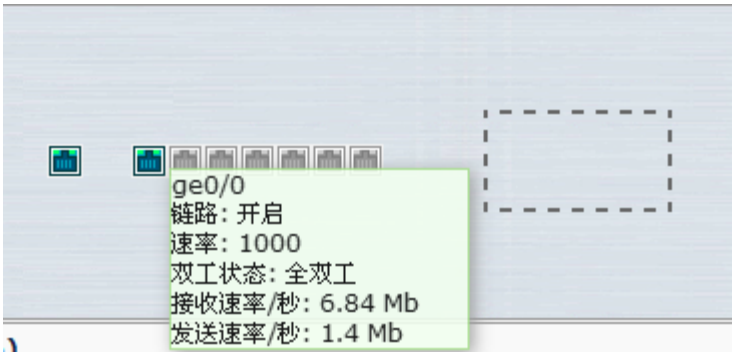
**定义主机名：** ADC 修改后的主机名。

在定义主机名中输入新定义的主机名称

点击**提交**按钮。

### 3.2.2 查看接口信息

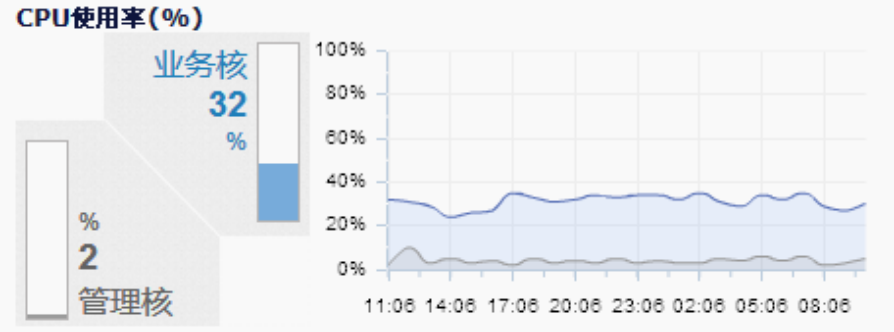
进入**系统信息>概况**，可以查看当前 ADC 应用交付控制的产品接口示意图。




图中，设备的物理接口示意图，当前在线的接口显示为蓝绿色，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。

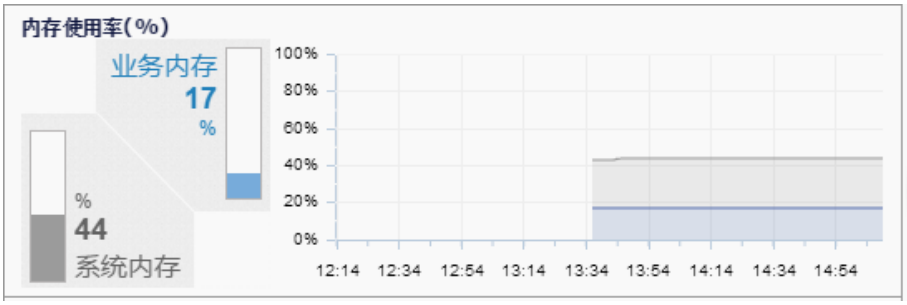
### 3.2.3 查看CPU使用情况

进入**系统信息>概况**，可以查看当前管理核 CPU 和业务核 CPU 的使用情况及 CPU 历史使用情况。



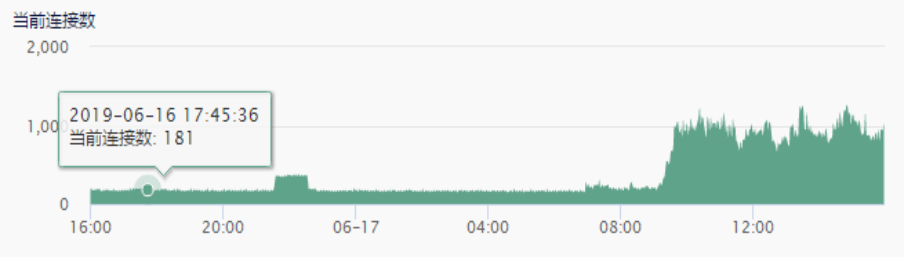

### 3.2.4 查看内存使用情况

进入**系统信息>概况**，可以查看当前系统内存和业务内存的使用情况及历史使用情况。



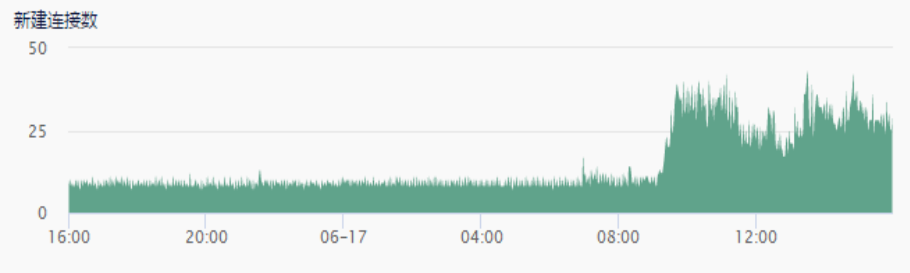

### 3.2.5 查看当前连接数

显示连接数随时间的变化曲线。



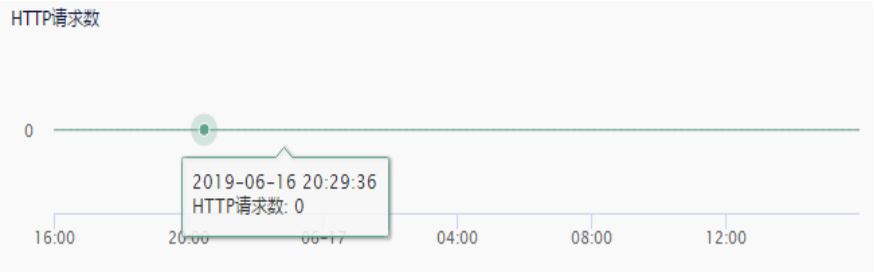

### 3.2.6 查看新建连接数

显示每秒新建连接数随时间的变化曲线。



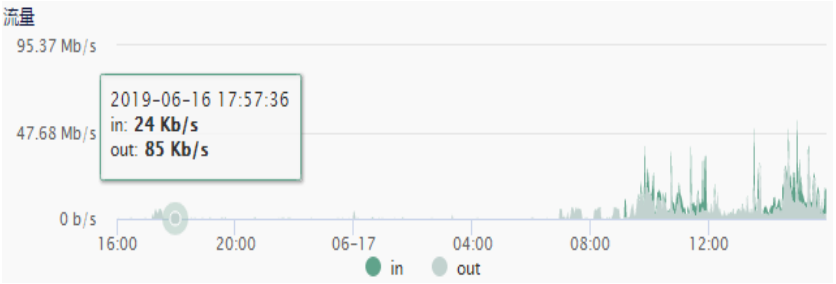

### 3.2.7 查看HTTP请求速率

显示每秒 HTTP 请求数随时间的变化曲线（虚拟服务启用 HTTP 模板时有效）。




### 3.2.8 查看流量

显示设备数据流量随时间变化的曲线。




### 3.2.9 查看高级别日志

高级别的日志。点击**更多**可进入日志查询页面查看详细情况。

最新高级别日志 更多

| 时间 | 类型 | 级别 | 消息 |
|---|---|---|---|
| 2019-06-21 15:44:19 | 健康检查事件 | 警示 | Content="member ip 3.3.3.1 port 0 pool v_pool2 template icmp down" |
| 2019-06-21 15:44:12 | 健康检查事件 | 警示 | Content="member ip 3.3.3.1 port 0 pool pool2 template icmp down" |
| 2019-06-21 15:42:27 | 接口信息 | 警示 | Content="interface vlan100 link up" |
| 2019-06-21 15:42:27 | 接口信息 | 警示 | Content="interface ge0/3 link up" |
| 2019-06-21 15:42:24 | 接口信息 | 警示 | Content="interface vlan100 link down" |
| 2019-06-21 15:42:23 | 接口信息 | 警示 | Content="interface ge0/3 link down" |
| 2019-06-21 15:42:20 | 健康检查事件 | 警示 | Content="member ip 152.1.1.2 port 0 pool 152 template icmp down" |
| 2019-06-21 15:42:19 | 健康检查事件 | 警示 | Content="member ip 152.1.1.5 port 0 pool 152 template icmp down" |
| 2019-06-21 15:42:19 | 健康检查事件 | 警示 | Content="member ip 152.1.1.2 port 443 pool 443 template icmp down" |
| 2019-06-21 15:42:17 | 接口信息 | 警示 | Content="interface ge0/4 link up" |

# 3.1 流量

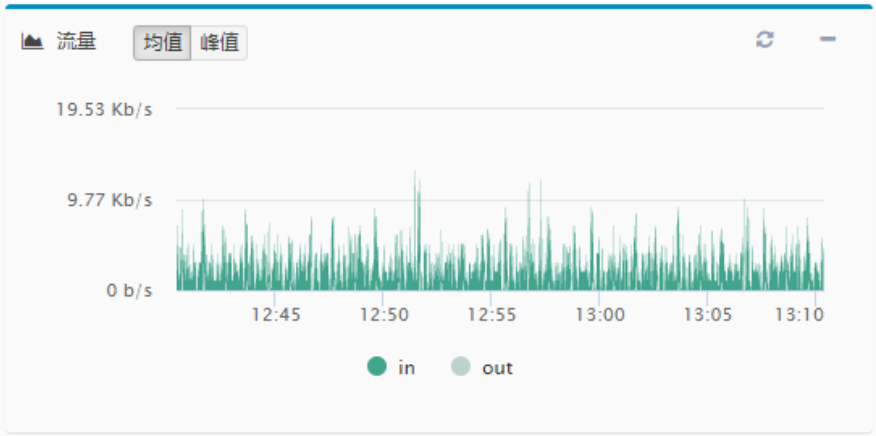
进入系统信息>概况>流量，可以查看系统的流量、连接数、接口统计、应用流量的信息，可以选择统计时间间隔，其中包括最近半小时、最近 3 小时、最近 24 小时、最近 7 天、最近 30 天。

## 3.1.1 流量时间

通过选择最近半小时、最近 3 小时、最近 24 小时、最近 7 天、最近 30 天，显示选择时间的流量、连接数、接口统计、应用流量的统计信息。


## 3.1.2 流量

显示指定时间段内设备流量的均值和峰值随时间变化的曲线。

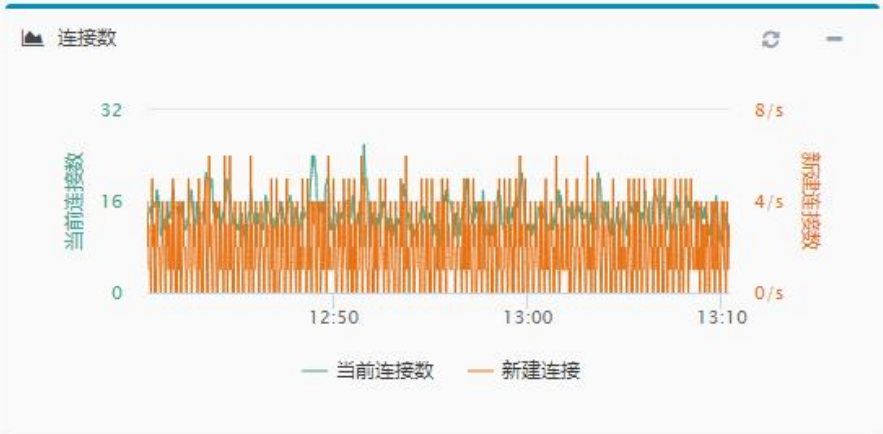



**均值：**指定时间段内收发流量的平均值，单位 b/s

**峰值：**指定时间段内收发流量的最大值，单位 b/s

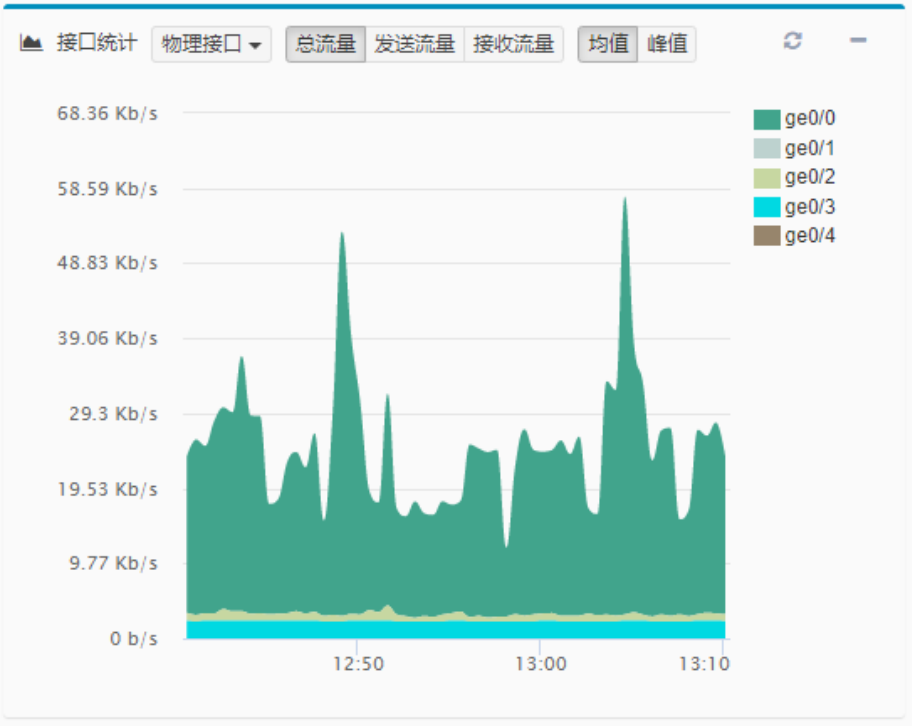
## 3.1.3 连接数

显示指定时间段内设备当前连接数随时间变化的曲线。



### 3.1.4 接口统计

显示指定时间段内设备接口流量速率统计随时间变化的曲线。




**物理接口：**设备的物理实体接口

**总流量：**设备的整体流量统计

**发送流量：**设备整体发出的流量统计

**接收流量：**设备整体接收的流量统计

**均值：**设备整体流量的平均值

**峰值：**设备整体流量的最大值

### 3.1.5 应用流量

显示设备整体的应用流量分类。


## 3.2 虚拟服务质量

进入**系统信息>概况>虚拟服务质量**，可以根据虚拟服务名称进行过滤，查看某一个虚拟服务的一些关键配置信息、服务质量评分、服务成员状态和流量统计情况等。

### 3.2.1 查看虚拟服务信息


**虚拟服务配置信息包括：**虚拟服务名称、虚拟服务类型、地址端口

**接收速率/秒：**虚拟服务正向流量（客户端到虚拟服务流量），单位 bit/s

**发送速率/秒：**虚拟服务反向流量（虚拟服务到客户端流量），单位 bit/s

**新建连接数：**每秒钟新建连接数

**并发连接数：**当前并发数

**最大连接数：**达到过的最大并发数

**http/秒：**http 请求速度，请求数/秒

**ssl(客户端)：**客户端 ssl 交易数速率

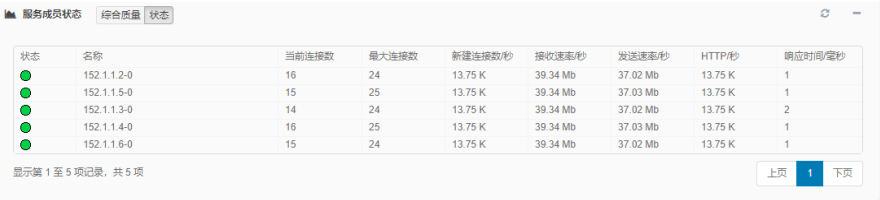
**ssl(服务端)：**服务器端 ssl 交易数速率

**综合评分：**虚拟服务评分，是虚拟服务中所有服务成员评分的平均值

### 3.2.2 查看服务成员状态

默认显示服务成员综合质量历史统计，服务成员按照发送速率递减排序。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 24 小时、最近 7 天、最近 30 天。


点击**状态**，查看服务成员状态实时统计信息，按照发送速率递减排序




**状态：**服务成员的状态

**名称：**服务成员地址与端口

**当前连接数：**当前并发数

**最大连接数：**达到过的最大并发数

**新建连接：**每秒钟新建连接数

**接收速率/秒：**服务成员正向流量（客户端到虚拟服务流量），单位 bit/s

**发送速率/秒：**服务成员反向流量（虚拟服务到客户端流量），单位 bit/s

**http/秒：**http 请求速度，请求数/秒

**响应时间/毫秒：**服务器响应时间


提示

同一个服务池不要被多个虚拟服务同时引用，会导致评分相互干扰。

### 3.2.3 评分阈值设置

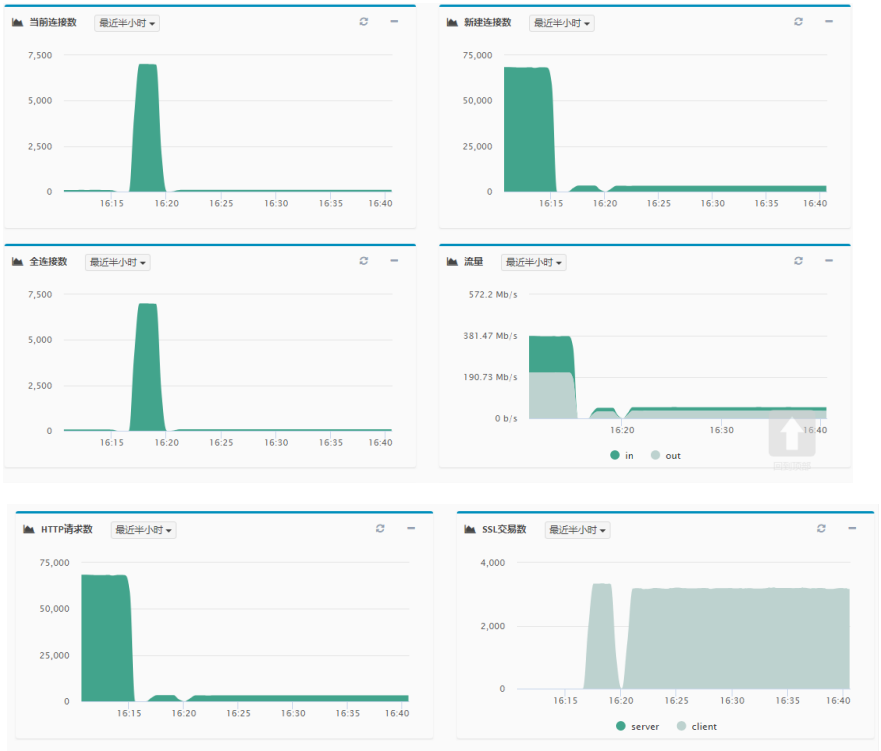
点击**评分阈值设置**，修改评分阈值信息，作为服务成员打分和服务成员综合质量评定的参考项


提示

每个虚拟服务都可以独立配置一套阈值标准，作用于虚拟服务中的所有服务成员，用于服务成员的综合质量评分。

### 3.2.4 查看虚拟服务统计信息

可以查看虚拟服务的当前连接数、新建连接数、全连接数、流量、http 请求数和 ssl 交易数随时间的变化曲线。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 24 小时、最近 7 天、最近 30 天。




## 3.3 链路质量

进入**系统信息>概况>链路质量**，可以根据虚拟链路名称进行过滤，查看某一个虚拟链路的一些关键配置信息、打分情况、链路节点状态和流量统计

情况等。

### 3.3.1 查看虚拟链路信息


**虚拟链路配置信息包括：**虚拟链路名称、地址

**接收速率/秒：**虚拟链路接收流量，单位 bit/s

**发送速率/秒：**虚拟链路发送流量，单位 bit/s

**新建连接数：**每秒钟新建连接数

**并发连接数：**当前并发数

**综合评分：**虚拟链路评分，是虚拟链路中所有链路节点评分的平均值

### 3.3.2 评分阈值设置

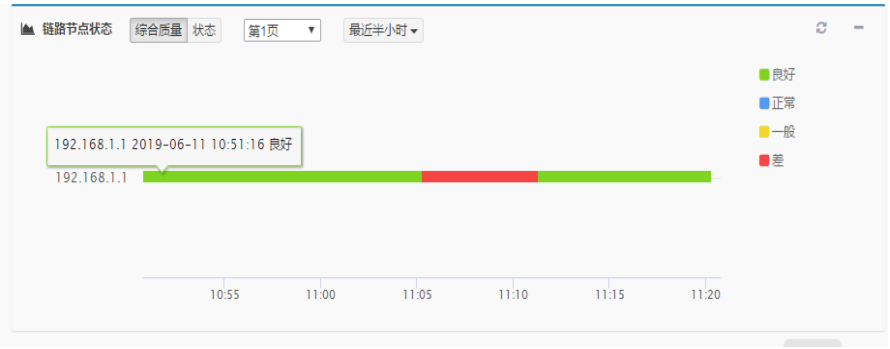
点击**评分阈值设置，**修改评分阈值信息，作为链路节点打分和链路节点综合质量评定的参考项


提示

虚拟链路的评分阈值标准作用于整机的所有虚拟链路。

### 3.3.3 查看链路节点状态

默认显示链路节点综合质量历史统计，链路节点按照发送速率递减排序。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 24 小时、最近 7 天、最近 30 天。




点击**状态**，查看链路节点实时统计信息，各个链路节点按照发送速率递减排序，如下图所示


**状态：**链路节点的状态

**名称：**链路节点地址

**别名：**链路节点的别名

**抖动：**链路节点抖动值（需要引用 icmp 类型的链路质量健康检查模板）

**延时：**链路节点延时值（需要引用 icmp 类型的链路质量健康检查模板）

**丢包率：**链路节点丢包率（需要引用 icmp 类型的链路质量健康检查模板）

**当前连接数：**当前并发数

**最大连接数：**达到过的最大并发数

**新建连接：**每秒钟新建连接数

**接收速率/秒：**链路节点接收流量，单位 bit/s

**发送速率/秒：**链路节点发送流量，单位 bit/s

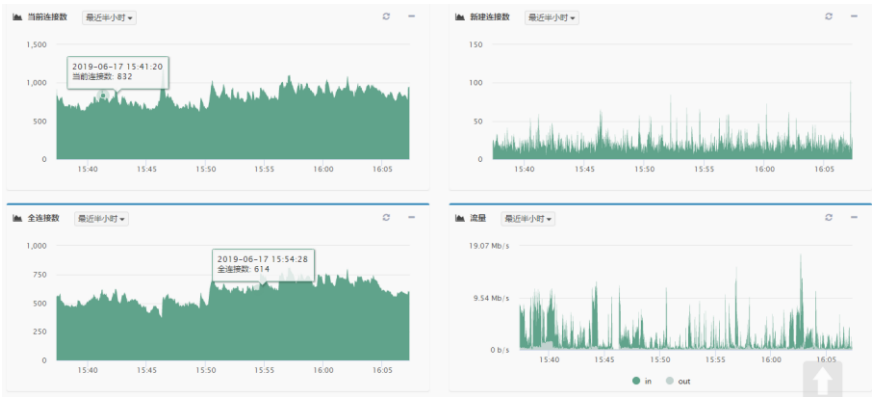
**综合质量：**链路节点根据丢包、延时和抖动情况参考阈值权重配置计算出来的综合评分

提示

链路节点的综合评分需要引用 icmp 类型的链路质量健康检查模板才有意义

### 3.3.4 查看虚拟链路统计信息

可以查看虚拟链路的当前连接数、新建连接数、全连接数、流量随时间的变化曲线。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 24 小时、最近 7 天、最近 30 天。



# 4 第4章 状态

## 4.1 概述

通过状态页面，可以查看虚拟服务、虚拟链路、全局负载均衡、接口的连接数和流量等实时状态，通过这些信息可以判断其工作状况是否正常，给排查问题提供必要的信息。

## 4.2 虚拟服务状态

进入**系统信息>状态>虚拟服务状态**，查看虚拟服务、虚拟地址、服务池和服务器节点状态信息。

### 4.2.1 虚拟服务


**状态：**虚拟服务的状态

**名称：**虚拟服务的名称

**总连接数：**当前并发数

**最大连接数：**达到过的最大并发数

**新建连接：**每秒钟新建连接数

**接收速率/秒：**虚拟服务正向流量（客户端到虚拟服务流量），单位 bit/s

**发送速率/秒：**虚拟服务反向流量（虚拟服务到客户端流量），单位 bit/s

**http/秒：**http 请求速度，请求数/秒

**ssl(客户端)：**客户端 ssl 交易数速率

**ssl(服务端)：**服务器端 ssl 交易数速率

**自动刷新：**自动刷新统计信息，默认禁用自动刷新，可配置自动刷新时间间隔分别为 10 秒、30 秒、300 秒

### 4.2.2 虚拟地址


**状态：**虚拟地址的状态

**IP 地址：**虚拟地址的 IP 地址

**总连接数：**当前并发数

**最大连接数：**达到过的最大并发数

**新建连接：**每秒钟新建连接数

**接收速率/秒：**虚拟服务正向流量（客户端到虚拟服务流量），单位 bit/s

**发送速率/秒：**虚拟服务反向流量（虚拟服务到客户端流量），单位 bit/s

**自动刷新：**自动刷新统计信息，默认禁用自动刷新，可配置自动刷新时间间隔分别为 10 秒、30 秒、300 秒

### 4.2.3 服务池


**状态：**服务池或成员的状态

**名称：**服务池名称或成员地址与端口

**总连接数：**当前并发数

**最大连接数：**达到过的最大并发数

**新建连接：**每秒钟新建连接数

**接收速率/秒：**虚拟服务正向流量（客户端到虚拟服务流量），单位 bit/s

**发送速率/秒：**虚拟服务反向流量（虚拟服务到客户端流量），单位 bit/s

**http/秒：**http 请求速度，请求数/秒

**响应时间/毫秒：**服务器响应时间

**自动刷新：**自动刷新统计信息，默认禁用自动刷新，可配置自动刷新时间间隔分别为 10 秒、30 秒、300 秒

### 4.2.4 服务器节点


**状态：**服务器节点的状态

**IP 地址：**服务器 IP 地址

**总连接数：**当前并发数

**最大连接数：**达到过的最大并发数

**新建连接：**每秒钟新建连接数

**接收速率/秒：**虚拟服务正向流量（客户端到虚拟服务流量），单位 bit/s

**发送速率/秒：**虚拟服务反向流量（虚拟服务到客户端流量），单位 bit/s

**http/秒：**http 请求速度，请求数/秒

**响应时间/毫秒：**服务器响应时间

**自动刷新：**自动刷新统计信息，默认禁用自动刷新，可配置自动刷新时间间隔分别为 10 秒、30 秒、300 秒

## 4.3 虚拟链路状态

进入**系统信息>状态>虚拟链路状态**，查看虚拟链路、链路池和链路节点状态信息。

### 4.3.1 虚拟链路


**状态：**虚拟链路的状态

**名称：**虚拟链路的名称

**总连接数：**当前并发数

**最大连接数：**达到过的最大并发数

**新建连接：**每秒钟新建连接数

**接收速率/秒：**虚拟链路正向流量，单位 bit/s

**发送速率/秒：**虚拟链路反向流量，单位 bit/s

### 4.3.2 链路池


**状态：**虚拟链路或者链路成员的状态

**名称：**虚拟链路或者链路成员的名称

**抖动：**链路池中各个链路节点的抖动值（需要链路池引用 ICMP 类型的链路质量探测健康检查模板）

**延时：**链路池中各个链路节点的延时值（需要链路池引用 ICMP 类型的链路质量探测健康检查模板）

**丢包率：**链路池中各个链路节点的丢包率（需要链路池引用 ICMP 类型的链路质量探测健康检查模板）

**当前连接数：**当前并发数

**最大连接数：**达到过的最大并发数

**新建连接：**每秒钟新建连接数

**接收速率/秒：**虚拟链路正向流量，单位 bit/s

**发送速率/秒：**虚拟链路反向流量，单位 bit/s

**自动刷新：**自动刷新统计信息，默认禁用自动刷新，可配置自动刷新时间间隔分别为 10 秒、30 秒、300 秒

### 4.3.3 链路节点


**状态：**链路节点的状态

**IP：**链路节点的 IP 地址

**别名：**链路节点的别名

**抖动：**各个链路节点的抖动值（需要链路节点引用 ICMP 类型的链路质量探测健康检查模板）

**延时：**各个链路节点的延时值（需要链路节点引用 ICMP 类型的链路质量探测健康检查模板）

**丢包率：**各个链路节点的丢包率（需要链路节点引用 ICMP 类型的链路质量探测健康检查模板）

**当前连接数：**当前并发数

**最大连接数：**达到过的最大并发数

**新建连接：**每秒钟新建连接数

**接收速率/秒：**虚拟链路正向流量，单位 bit/s

**发送速率/秒：**虚拟链路反向流量，单位 bit/s

**响应时间/毫秒：**链路延迟时间

**自动刷新：**自动刷新统计信息，默认禁用自动刷新，可配置自动刷新时间间隔分别为 10 秒、30 秒、300 秒

## 4.4 全局负载均衡状态

### 4.4.1 数据中心

进入**系统信息>状态>全局负载均衡状态**，查看数据中心，全局地址池状态信息。


**状态：**数据中心的状态

**名称：**数据中心的名称

**类型：**数据中心的类型

**连接数：**当前数据中心的连接数

**最大连接数：**达到过的最大并发数

**新建连接：**每秒钟新建连接数

**连接数限制：**配置的连接数限制

**带宽/秒：**当前的带宽

**带宽限制/秒：**配置的带宽限制

**包速率/秒：**当前的数据包速率

**包速率限制/秒：**配置的数据包速率限制

**自动刷新：**自动刷新统计信息，默认禁用自动刷新，可配置自动刷新时间间隔分别为 10 秒、30 秒、300 秒

### 4.4.2 全局地址池状态


**状态：**全局地址池的状态

**名称：**全局地址池的名称

**类型：**全局地址池的类型

**连接数：**当前全局地址池的连接数

**最大连接数：**达到过的最大并发数

**新建连接：**每秒钟新建连接数

**连接数限制：**配置的连接数限制

**带宽/秒：**当前的带宽

**带宽限制/秒：**配置的带宽限制

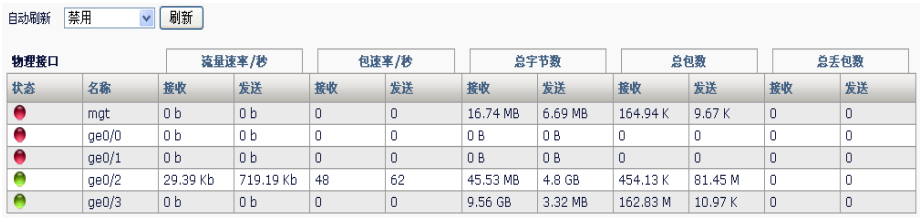
**包速率/秒：**当前的数据包速率

**包速率限制/秒：**配置的数据包速率限制

**自动刷新：**自动刷新统计信息，默认禁用自动刷新，可配置自动刷新时间间隔分别为 10 秒、30 秒、300 秒

## 4.5 查看接口状态

进入**系统信息>状态>接口状态**，如下如所示：




**状态：**表示接口 up/down 状态，红色表示 down，绿色表示 up

**名称：**接口名称

**流量速率：**接口接收/发送数据速率，单位 bit/s

**包速率：**接口接收/发送包速率，单位为个/秒

**总字节数：**接口接收/发送的总字节数，单位为 byte

**总包数：**接口接收/发送总的包个数，单位为个

**总丢包：**接口接收/发送丢弃的总包个数，单位为个

**自动刷新：**自动刷新统计信息，默认禁用自动刷新，可配置自动刷新时间

间隔分别为 10 秒、30 秒、300 秒

# 5 第5章 统计信息

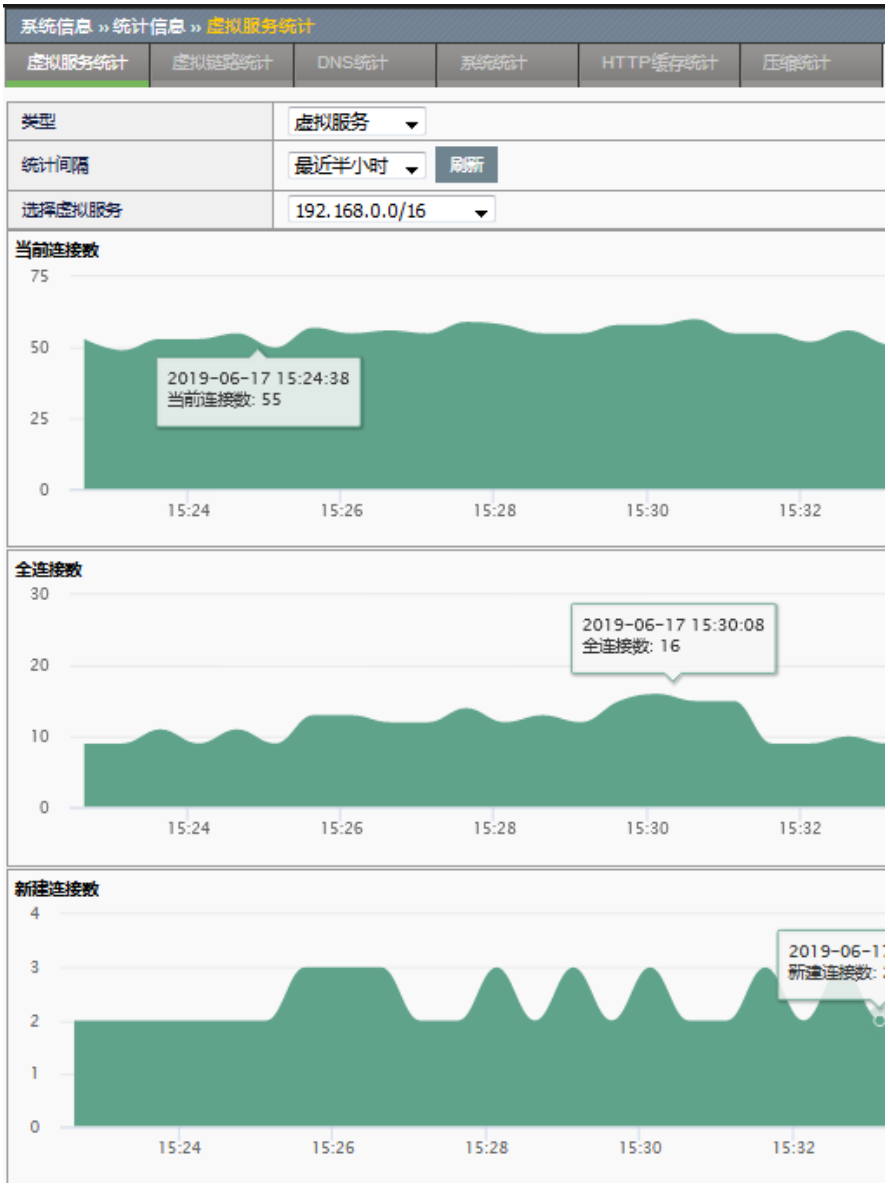
## 5.1 统计信息概述

通过统计信息，可以查看虚拟服务、虚拟链路、DNS 负载、系统以及服务池、服务器节点的当前连接数、全连接数、流量等变化生成的曲线图，也能查看缓存和压缩统计曲线图，通过这些信息可以判断其工作状况是否正常，给排查问题提供必要的信息。

## 5.2 虚拟服务统计

**查看步骤：**

1. 点击**系统信息>统计信息>虚拟服务统计**，进入虚拟服务统计页面，该页面根据下拉菜单中的选项查看系统虚拟服务、服务池和服务成员、服务器节点的当前连接数、全连接数、新建连接数、流量、HTTP 请求数，以及虚拟服务的 SSL 交易数和服务节点的响应时间，可查看最近半小时、最近 3 小时、最近 24 小时、最近 7 天、最近 30 天的统计结果。




2. 选择类型：包括虚拟服务、服务池、服务器节点。


3. 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 24 小时、最近 7 天、最近 30 天。


4. 选择具体服务进行查询。


## 5.3 虚拟链路统计

**查看步骤：**

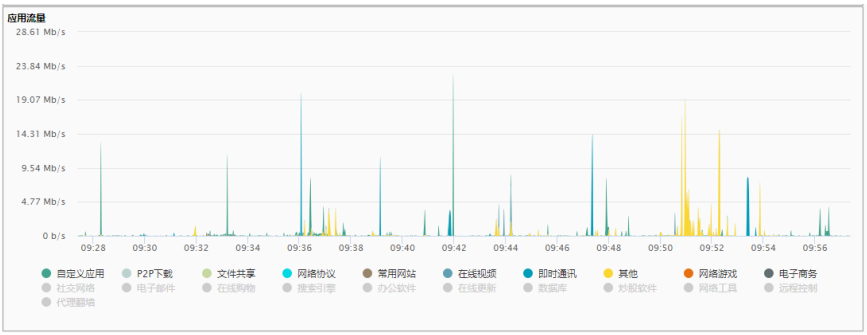
1. 点击**系统信息>统计信息>虚拟链路统计**，进入虚拟链路页面，该页面根据下拉菜单中的选项可查看系统虚拟链路、链路池和链路成员、链路节点的当前连接数、全连接数、新建连接数、流量、应用流量信息，以及链路节点响应时间，链路成员和链路节点的丢包率、延时、抖动信息，可查看最近半小时、最近 3 小时、最近 24 小时、最近 7 天、最近 30 天的统计结果。


2. 选择类型：包括虚拟链路、链路池、链路节点。

3. 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 24 小时、最近 7 天、最近 30 天。


4. 选择具体链路进行查询。


5. 查看链路应用流量信息。




## 5.4 DNS统计

**查看步骤：**

1. 点击**系统信息>统计信息>DNS 统计**，该页面根据下拉菜单中的选项查看本地域名映射、全局域名映射的 DNS 访问次数，可根据域名映射对象，查看最近半小时、最近 3 小时、最近 24 小时、最近 7 天、最近 30 天的统计结果。


2. 选择类型：可选本地域名映射、全局域名映射。


3. 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 24 小时、最近 7 天、最近 30 天。

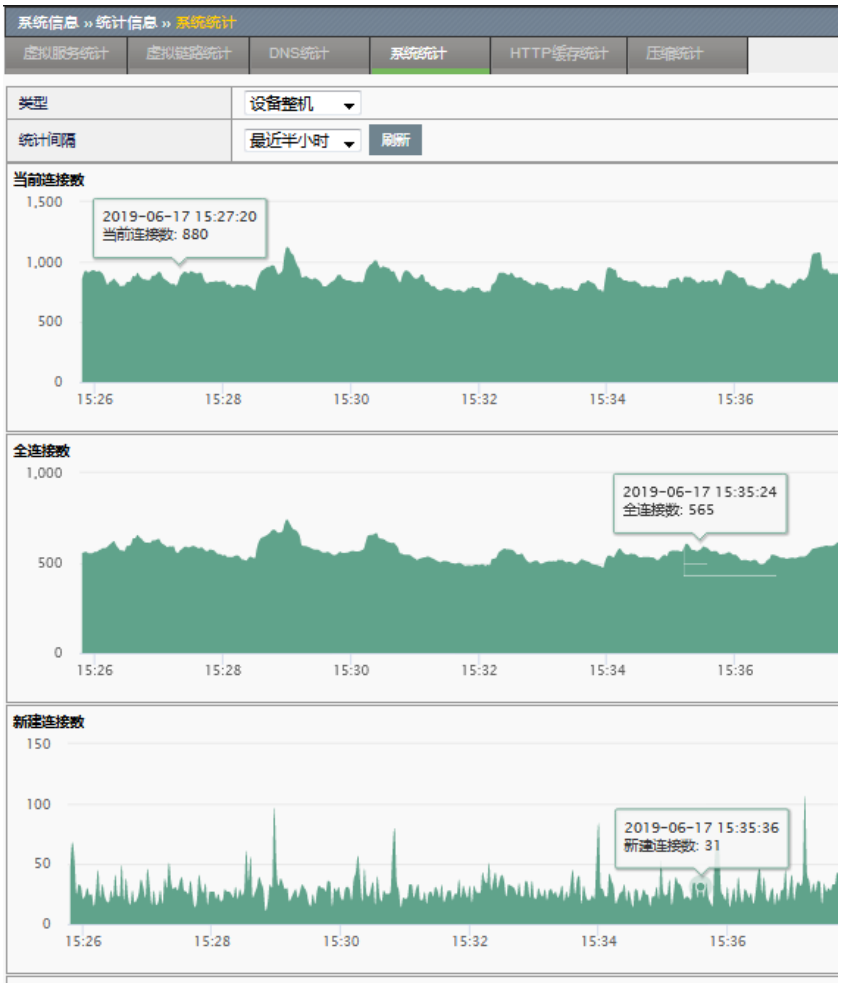

4. 通过配置的域名映射对象进行统计查看：

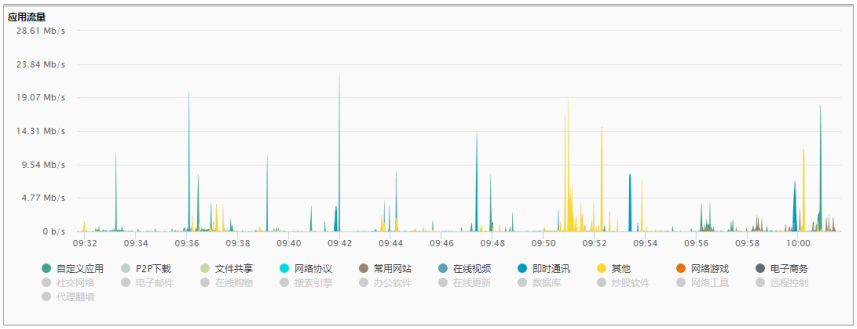

## 5.5 系统统计

**1. 设备整机**

**查看步骤：**

点击**系统信息>统计信息>系统统计**，进入系统统计页面，该页面根据下拉菜单中的选项查看系统设备整机的当前连接数、全连接数、新建连接数、流量、峰值流量、HTTP 请求数、SSL 交易数、应用流量，可查看最近半小时、最近 3 小时、最近 24 小时、最近 7 天、最近 30 天的统计结果。

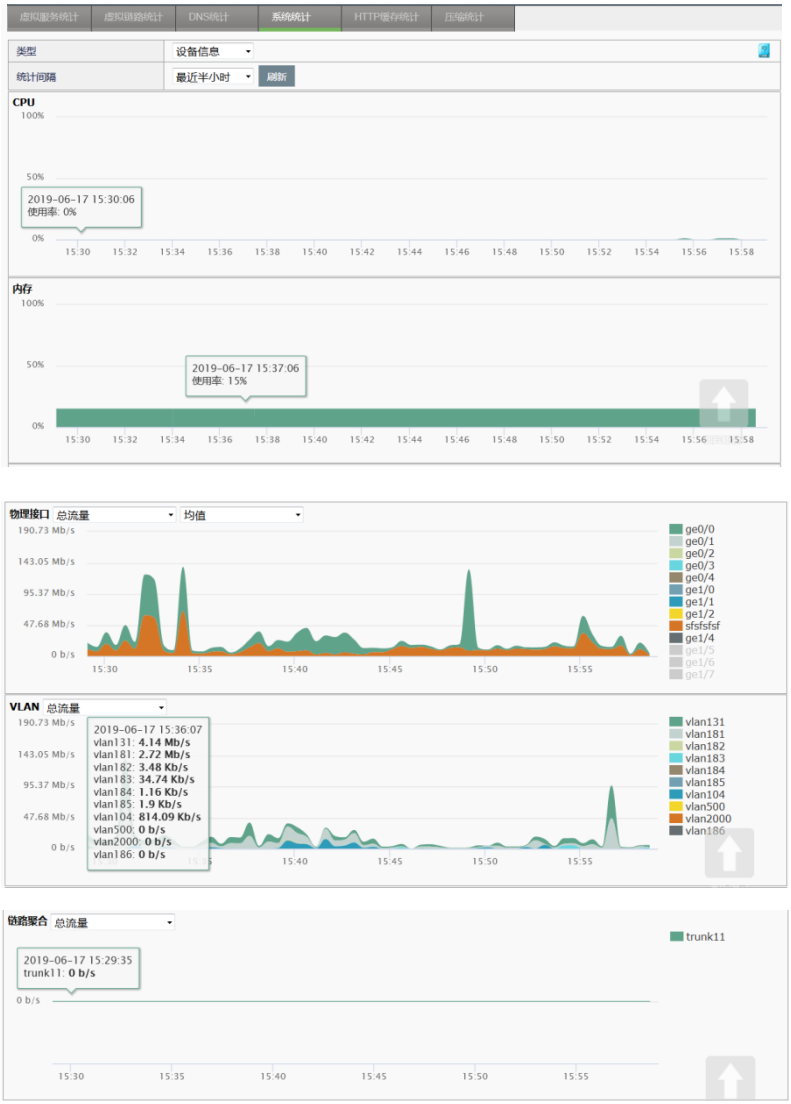



## 2. 设备信息

**查看步骤：**

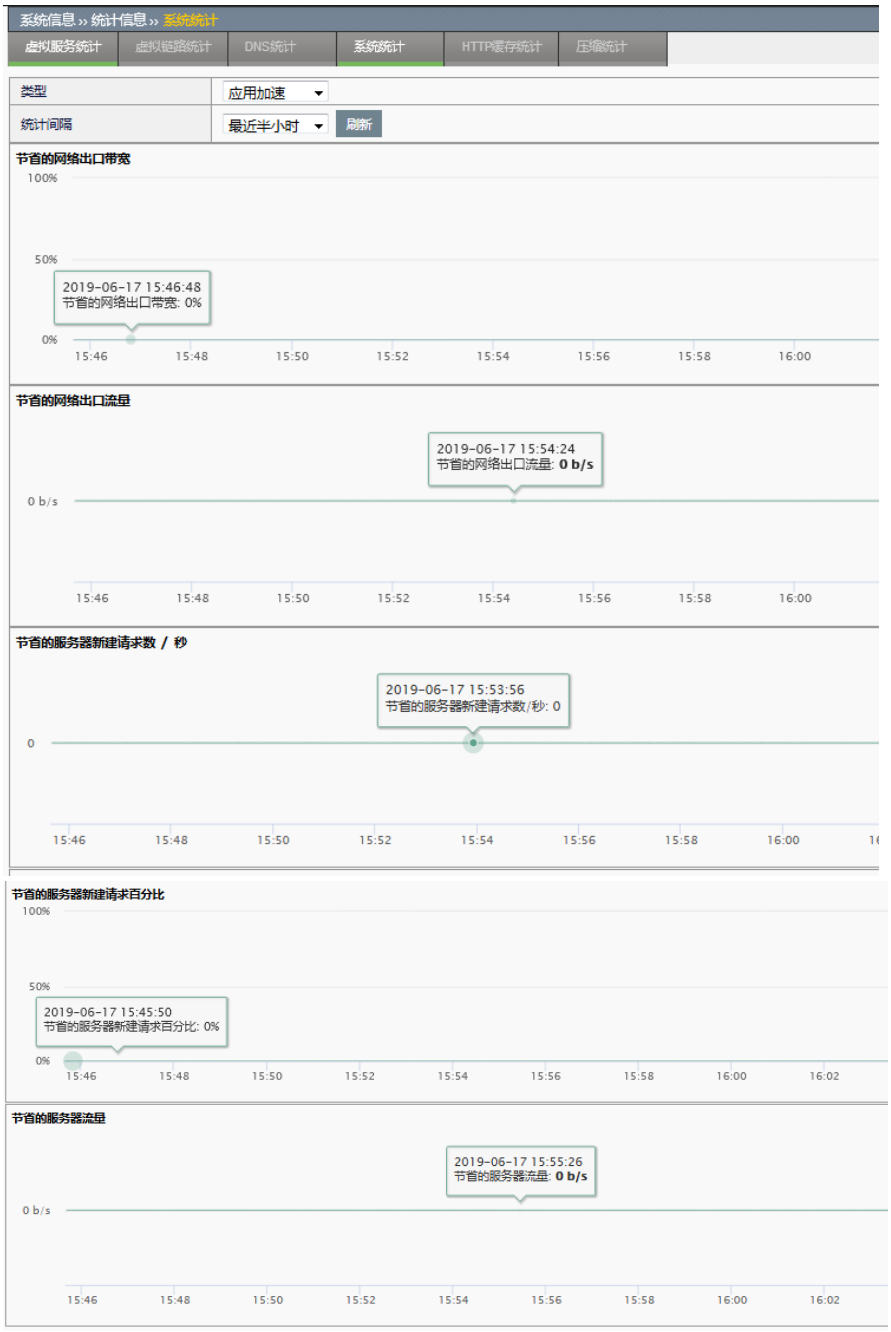
点击**系统信息>统计信息>系统统计，**进入系统统计页面，该页面根据下拉菜单中的选项查看系统设备信息，其中包括 cpu 使用率、内存使用率、物理接口信息，vlan 信息，链路聚合信息。可查看最近半小时、最近 3 小时、最近 24 小时、最近 7 天、最近 30 天的统计结果。




### 3. 应用加速

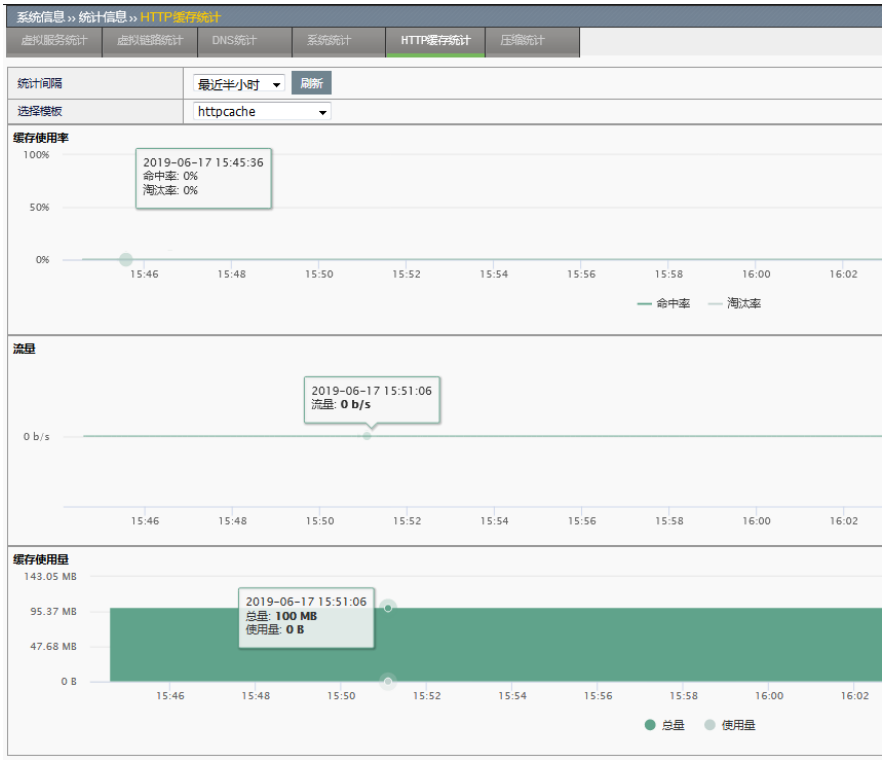
**查看步骤：**

点击**系统信息>统计信息>系统统计**，进入系统统计页面，该页面根据下拉菜单中的选项查看系统的应用加速统计信息，其中包括节省的网络出口带宽、节省的网络出口流量、节省的服务器新建请求数、节省的服务器新建请求百分比、节省的服务器流量信息。可查看最近半小时、最近 3 小时、最近 24 小时、最近 7 天、最近 30 天的统计结果。



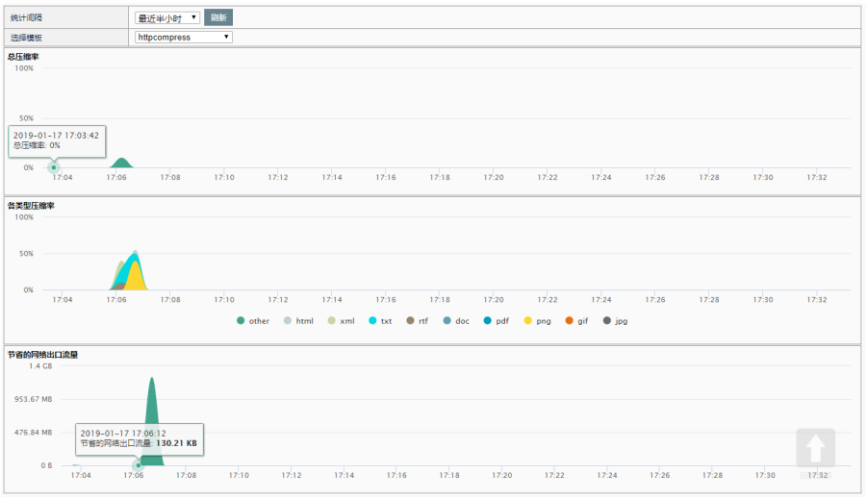

## 5.6 HTTP缓存统计

进入**系统信息->统计信息->HTTP 缓存统计**，可查看到 HTTP 高速缓存最近一段时间的统计图表。如下图：




## 5.7 压缩统计

进入**系统信息>统计信息>压缩统计**，选取**统计间隔**和生效的 HTTP 压缩模版，可以查看实时的压缩统计信息。



# 6 第6章 会话监控

## 6.1 会话监控概述

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

## 6.2 会话统计

**配置步骤：**

1. 点击**系统信息>会话监控>会话统计**，进入会话统计页面，该页面根据下拉菜单中的选项统计系统当前连接数，可根据**源 Ipv4 统计、源 Ipv6 统计、目的 Ipv4 统计、目的 Ipv6 统计、目的端口统计**，还可指定详细条件，统计出的连接数按数量降序排列，最多显示前 50 项。


2. 在类型下拉菜单中选择排序条件：**源 IPv4 统计、源 Ipv6 统计、目的 IPv4 统计、目的 Ipv6 统计、目的端口统计**，默认为按源 IPv4 统计。
3. 在输入框中填写详细的**端口**或 **IP** 匹配条件，可输入 IP 地址/范围/掩码或端口号/范围，如果不输入，默认为全部统计。
4. 点击 搜索 进行统计。
5. 结果显示后，若想查看详细信息，点击 进入标准会话页面查看连接详细信息。

## 6.3 标准会话

**配置步骤：**

1. 点击**系统信息>会话监控>标准会话**，进入**标准会话**页面，该页面根据

输入的类型、名称、协议、源/目的 IP、业务端口、连接状态、地址类型等条件进行组合查询，显示匹配条件的连接。


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

## 6.4 代理会话

**配置步骤：**

1. 点击**系统信息>会话监控>代理会话**，进入**代理会话**页面，可按条件进行搜索，下方会显示代理会话的内容。


2. 点击**条件设置**，可输入虚拟服务名称、源 IP、目的 IP 等条件，默认为所有。
3. 点击 搜索 进行查询。

## 6.5 配置案例

**案例 1：源主机连接数**

**案例描述：**

查看源 ip 的连接数量。

**配置步骤：**

1. 选择类型，源 IPv4 统计。

2. 输入具体 IP 地址。

3. 点击 搜索 ，查看结果。


**案例 2：查看虚拟服务的连接**

**案例描述：**

通过查看虚拟服务标准会话连接情况，了解虚拟服务具体运行情况。

**配置步骤：**

1. 选择类型,选择虚拟服务。
2. 输入具体虚拟服务名称。
3. 选择连接类型，选择全连接。
4. 选择地址类型，选择所有。
5. 点击 搜索 ，查看结果。

| # | 名称 | 成员 | 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 | 不要删-vs | - | TCP | 192.168.31.96 | 9228 | 192.168.31.194 | 80 | 00:01:04 | 01:00:00 | 全连接 |
| 2 | 不要删-vs | - | TCP | 192.168.31.96 | 9227 | 192.168.31.194 | 80 | 00:01:04 | 00:59:33 | 全连接 |
| 3 | 不要删-vs | - | TCP | 192.168.31.192 | 1385 | 192.168.31.194 | 80 | 00:02:56 | 00:59:04 | 全连接 |
| 4 | 不要删-vs | - | TCP | 192.168.31.96 | 9225 | 192.168.31.194 | 80 | 00:01:20 | 00:59:33 | 全连接 |

# 7 第7章 流量统计

## 7.1 基于IP/端口流量统计查询

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

进入**系统信息>会话监控>流量统计**，可看到如下界面。输入检索条件，查询

流量统计结果。


**统计类型：**包括主机和端口

**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，虚拟服务的正向流量，虚拟链路反向流量

**Tcp 出：**TCP 协议流量，虚拟服务的反向流量，虚拟链路正向流量

**UDP 入：**UDP 协议流量，虚拟服务的正向流量，虚拟链路反向流量

**UDP 出：**UDP 协议流量，虚拟服务的反向流量，虚拟链路正向流量

**其他入：**其他协议流量，虚拟服务的正向流量，虚拟链路反向流量

**其他出：**其他协议流量，虚拟服务的反向流量，虚拟链路正向流量

**总流量：**所有协议双方向流量总和

## 7.2 配置案例

**案例描述**

配置过滤条件，查看流量统计。

**配置步骤：**

1. 进入**系统信息>会话监控>流量统计**，进行过滤条件的设置：

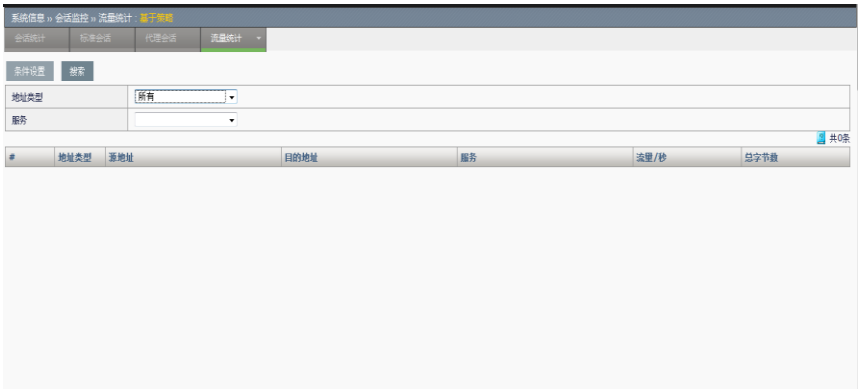

2. 点击搜索，可查看主机的流量统计结果:


## 7.3 基于策略流量统计

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**系统信息>会话监控>流量统计**，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。

**流量/秒：**每秒的流量，单位 B。

**总字节数：**总流量，字节数。

注意

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

## 7.4 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**安全功能>防火墙>安全策略**，开启策略流量统计功能：


注：只有 PERMIT 类型的安全策略可以进行流量统计。

2. 进入**系统信息>会话监控>流量统计**，输入检索条件，查看策略流量统计结果：

# 8 第8章 时间对象

## 8.1 概述

为了方便用户配置和管理，应用交付设备中引入了时间对象概念，时间对象分为绝对时间和周期时间。在其它功能的配置中，可以引用时间对象来定义配置生效的条件。

绝对时间：配置服务在指定的时间内生效。

周期时间：配置服务在指定的时间范围内在指定的周期（星期一 ~ 星期日）执行。

## 8.2 配置时间对象

### 8.2.1 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**模板和对象->对象管理>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**。

### 8.2.2 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**模板和对象->对象管理>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**。

## 8.3 配置案例

### 8.3.1 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**模板和对象->对象管理>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。

### 8.3.2 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**模板和对象->对象管理>时间对象>周期时间**，点击**新建**，如下图：


2. 点击**提交**完成设置。

## 8.4 绝对时间与周期时间监控与维护

### 8.4.1 查看绝对时间

点击**模板和对象->对象管理>时间对象>绝对时间**，如下图：


## 8.5 常见故障分析

### 8.5.1 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。 |

# 9 第9章 服务对象

## 9.1 概述

为了方便用户的配置和管理，应用交付设备中引入了服务对象的概念。在其它功能(如安全策略、NAT 规则、路由策略)的配置中，可以引用服务对象来定义配置生效的条件。

服务对象里包括预定义服务，自定义服务，服务组。

预定义服务：系统预先添加服务，用户不可编辑或删除。

自定义服务：需要用户自行配置添加。

服务组：服务组是服务的集合。

## 9.2 配置服务对象

### 9.2.1 预定义服务

进入**模板和对象->对象管理>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 |

### 9.2.2 配置自定义服务

**配置步骤：**

进入**模板和对象->对象管理>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。

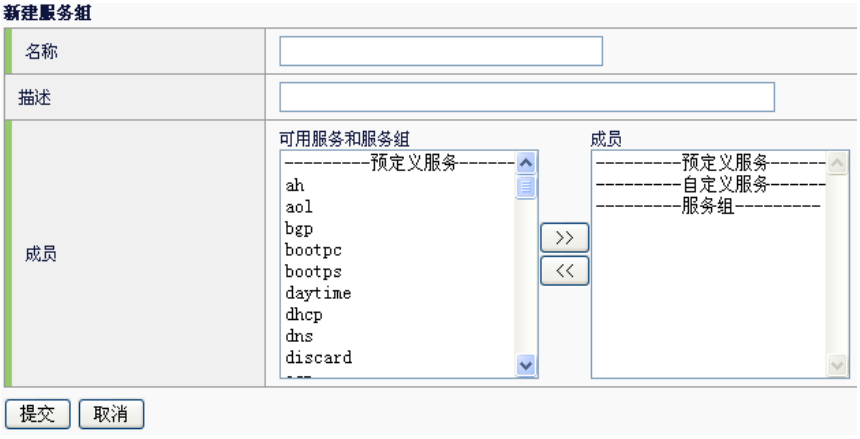
点击**提交**。


如果用户只想对某个协议填写特定端口，则“-”两边填写同样的端口号即可。

### 9.2.3 配置服务组

**配置步骤：**

进入**模板和对象->对象管理>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**。


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。

## 9.3 配置案例

### 9.3.1 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**模板和对象->对象管理->服务对象->自定义服务**，点击**新建**，如下图：


2. 编辑目的端口 8110，点击 >> 添加。
3. 编辑目的端口 8025，点击 >> 添加。
4. 点击**提交**完成设置。

### 9.3.2 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**模板和对象->对象管理>服务对象>服务组**，点击**新建**，如下图：


2. 添加 FTP，SMTP，TFTP 和自定义服务**邮件服务**到开通服务组。

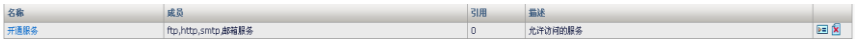
3. 点击 >> 添加。

4. 点击**提交**完成设置。

## 9.4 服务对象监控与维护

### 9.4.1 查看服务组

进入**模板和对象->对象管理>服务对象>服务组**，如下图：




## 9.5 常见故障分析

### 9.5.1 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。 |

# 10 第10章 地址对象

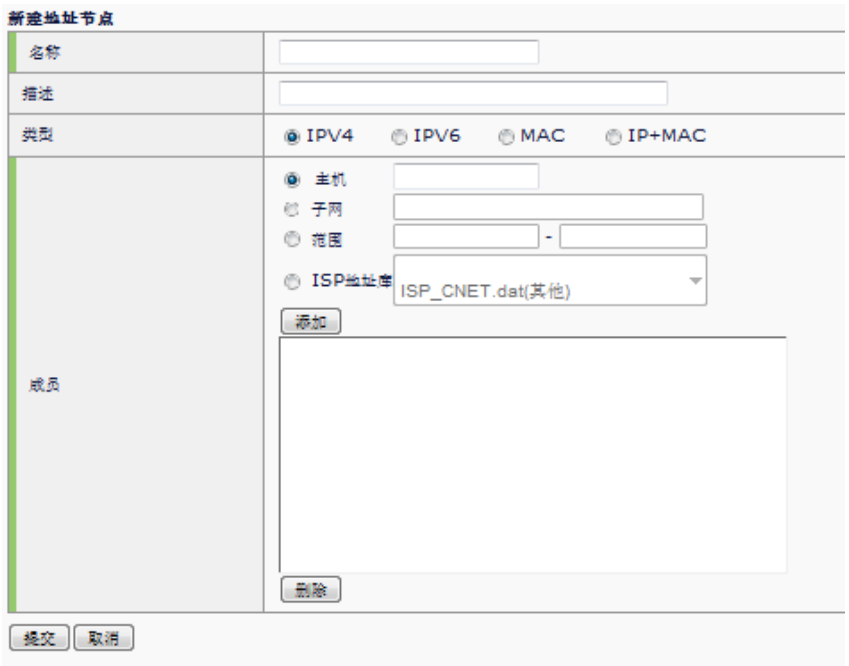
## 10.1 地址对象概述

为了方便用户的配置和管理，应用交付设备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（如安全策略、NAT 规则，路由策略），可以引用地址对象来定义配置生效的条件。

## 10.2 配置地址节点

地址节点分为 IPv4 类型，IPv6 类型，MAC 类型以及 IP+MAC 类型。

1. 进入**模板和对象->对象管理>地址对象>地址节点**，点击**新建**，如下图：




**名称**：为新建地址节点设置名称，不得超过 63 个字符。

**描述**：对新建地址节点做描述，不得超过 127 个字符。

**类型**：地址节点可分为 IPv4 类型，IPv6 类型，MAC 类型以及 IP+MAC 类型。

**地址节点**：IPv4 类型地址节点的内容包含：

- 主机：主机 IPv4 地址。
- 子网： IPv4 网段地址。

- 范围： IPv4 地址池范围。
- IPv4 的 ISP 地址库。

IPv6 类型地址节点的内容包括：

- 主机：主机 IPv6 地址。
- 子网：IPv6 网络地址。
- 范围：IPv6 地址范围。

MAC 类型的地址节点内容是 MAC 地址；

IP+MAC 类型的地址节点内容是 IPv4 地址和 MAC 地址的组合。

2. 点击**提交**。

## 10.3 配置地址组

地址组是地址节点的集合，可以使用地址组方便的管理和地址相关的规则。

**配置步骤：**

**进入模板和对象->对象管理>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**：已经定义好的地址节点和地址组信息。

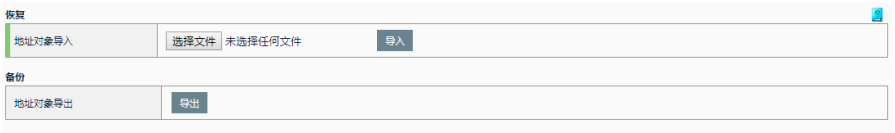
**成员**：地址组成员。

点击**提交**。

## 10.4 配置备份恢复

备份恢复可以备份 IPv4 类型、IPv6 类型、MAC 类型、IP+MAC 类型、地址组地址对象。

**点击模板和对象->对象管理>地址对象>备份恢复**




**选择文件：**选择要导入的地址对象文件

**导入：**导入已选择的地址对象文件

**导出：**导出已配置的地址对象

## 10.5 配置案例

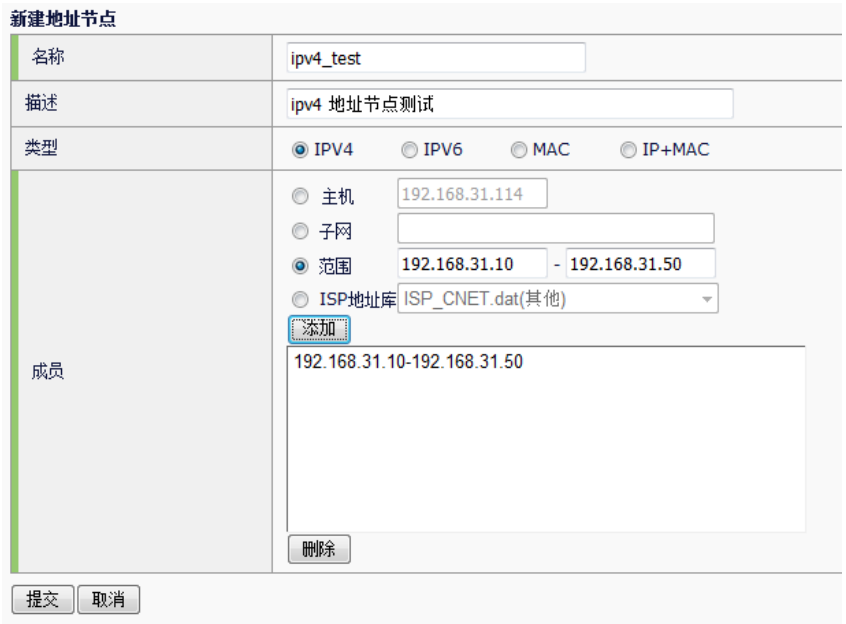
### 10.5.1 配置案例1：增加IPv4地址节点

**案例描述**

增加一个 IPv4 的地址对象，包含内网的某些网段。

**配置步骤：**

1. 进入模板和对象->对象管理>地址对象>地址节点，点击新建，如下图：




2. 输入参数。
3. 点击**提交**完成设置。

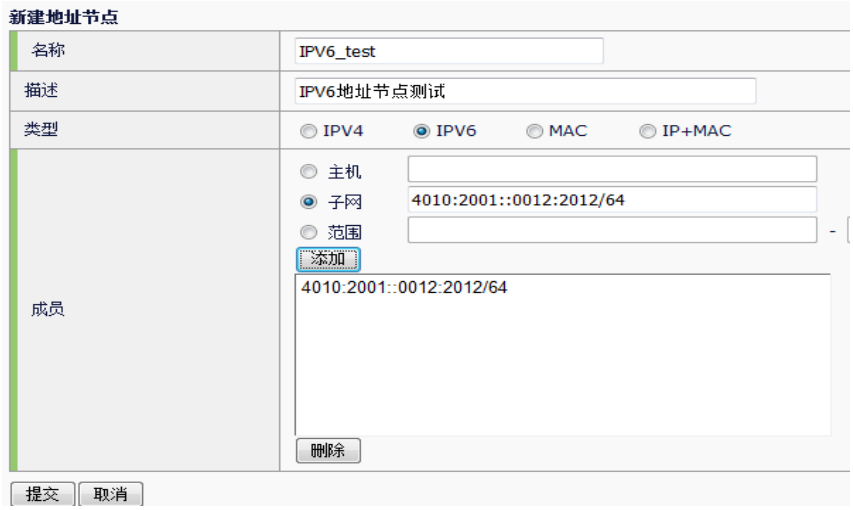
### 10.5.2 配置案例2：增加IPv6地址节点

**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**模板和对象->对象管理>地址对象>地址节点**，点击**新建**，如下图：




2．输入参数。

3．点击**提交**完成设置。

## 10.5.3 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**模板和对象->对象管理>地址对象>地址组**，点击**新建**，如下图：

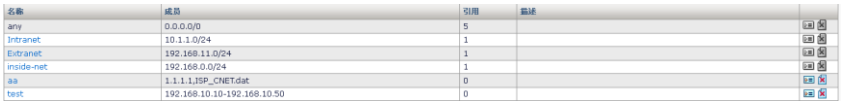

2. 选择**可用地址和地址组**中的地址节点，点击 >> 添加到**成员**中。

3. 点击**提交**完成设置。

## 10.6 地址对象监控与维护

### 10.6.1 查看地址节点

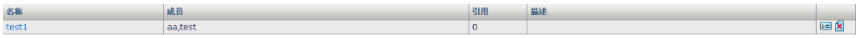
点击**模板和对象->对象管理>地址对象>地址节点**，如下图：



| 名称 | 成员 | 引用 | 描述 | |
|---|---|---|---|---|
| any | 0.0.0.0/0 | 5 | | |
| Intranet | 10.1.1.0/24 | 1 | | |
| Extranet | 192.168.11.0/24 | 1 | | |
| inside-net | 192.168.0.0/24 | 1 | | |
| aa | 1.1.1.1,ISP_CNET.dat | 0 | | |
| test | 192.168.10.10-192.168.10.50 | 0 | | |

### 10.6.2 查看地址组

点击**模板和对象->对象管理>地址对象>地址组**，如下图：



| 名称 | 成员 | 引用 | 描述 | |
|---|---|---|---|---|
| test1 | aa,test | 0 | | |

### 10.6.3 地址对象的备份和恢复

点击**模板和对象->对象管理>地址对象>备份恢复**，如下图：


**参数说明：**

**恢复：**可导入包含地址对象配置的文本文件，系统会读取问题中的配置并执行下发。地址对象的配置格式必须如下：

- **IPv4 类型地址对象**

address NAME

host-address A.B.C.D

net-address A.B.C.D/M

range-address A.B.C.D E.F.G.H

isp-address NAME

- **IPv6 类型地址对象**

address-v6 NAME

host-v6 X:X::X:X

net-v6 X:X::X:X/M

range-v6 X:X::X:X X:X::X:X

- **MAC 类型地址对象**

address-mac NAME

mac-host FF-FF-FF-FF-FF-FF

- **IP+MAC 类型地址对象**

address-ip-mac NAME

bind A.B.C.D FF-FF-FF-FF-FF-FF

- **地址组**

address-group NAME

address-object NAME

**备份：**可将地址对象的配置导出至一个文本文件中。

## 10.7 常见故障分析

### 10.7.1 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。 |

# 11 第11章 应用对象

## 11.1 概述

为了方便用户的配置和管理，应用交付设备中引入了应用对象的概念。在路由策略的配置中，可以引用应用对象来定义配置生效的条件。

应用对象，实际上包括预定义应用、自定义应用、应用组、域名几个部分。

- **预定义应用**：具体的用户应用，如下载软件、即时通信软件，目前有 20 大类 1000 多种应用，通过应用于特征库更新，不需要用户配置。
- **自定义应用**：需要用户自行配置。
- **应用组**：需要用户自行配置，可引用预定义应用和自定义应用。
- **域名**：需要用户自行配置。

在实际使用中，由路由策略来引用应用对象。配合虚拟链路中的路由策略来使用，可以将某些应用的流量引入到指定链路中，实现“应用引流”的功能。

对具体应用的流量引导，在实际网络环境中有较大的实用价值。例如，某网络环境有两条链路，其中一条为优质链路。用户往往会采用一些措施来保证优质链路的带宽，来避免一些大的流量（如 P2P 下载）对带宽的过度占有。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。

## 11.2 配置应用对象

### 11.2.1 配置自定义应用

**配置步骤：**

1.进入**模板和对象>对象管理>应用对象：自定义应用**，点击**新建**，如下图


**名称**：为新建自定义应用的名称，不得超过 63 个字符。

**协议类型**：选择协议类型，可配置为 TCP 或 UDP。

**源地址**：应用的源地址，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。

**源端口**：应用的源端口，端口号允许的范围为 1~65535。

**目的地址**：应用的目的地址，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。

**目的端口**：应用的目的端口，端口号允许的范围为 1~65535。。

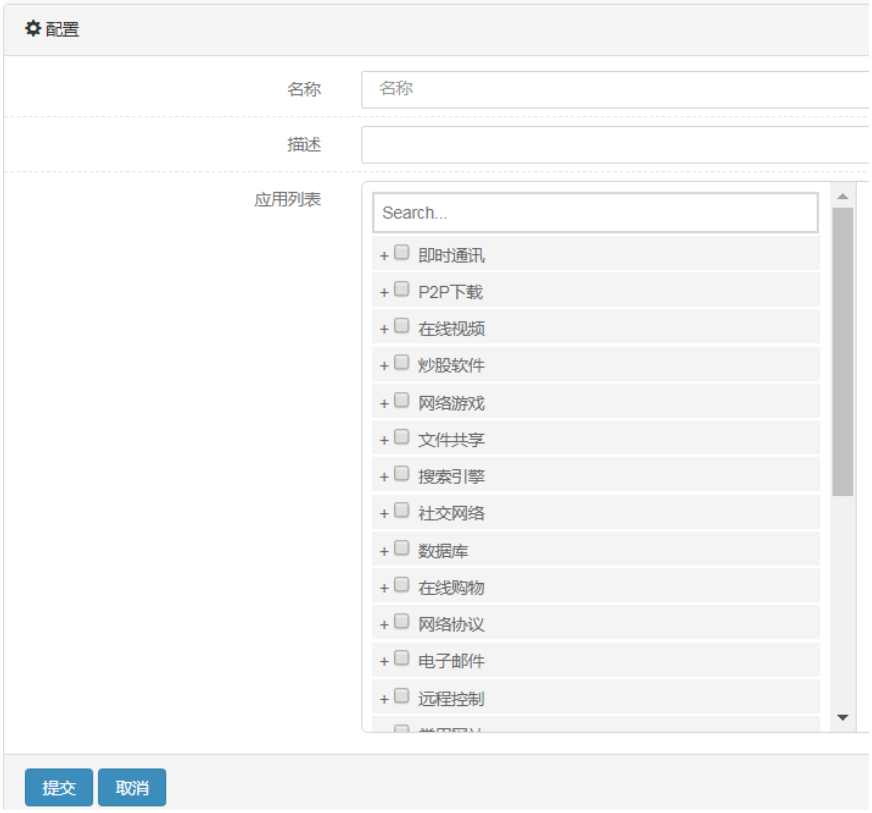
2.点击**提交**。

| | |
|---|---|
| 注意 | 自定义应用对象优先级最高，一定要精确配置各个参数，否则其他流量也被识别成了自定义应用，导致其他控制应用的策略无法匹配到真正应用。 |

### 11.2.2 配置应用组

**配置步骤：**

进入**模板和对象>对象管理>应用对象：应用组**，点击**新建**，如下图




**名称**：为新建应用组的名称，不得超过 63 个字符。

**描述**：为新建应用组的描述，不得超过 127 个字符。

**应用列表**：为系统所支持的所有应用列表。如上图所示。

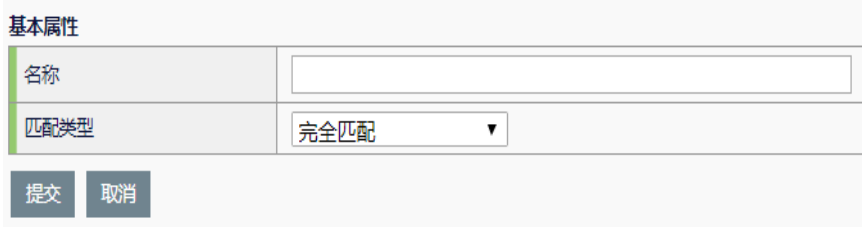
**选中**所想要的应用，点击**提交**。


自定义应用，只有配置了自定义应用才会出现。
自定义域名，只有配置了域名才会出现。
域名地址库，详见“域名地址库”章节。

### 11.2.3 配置域名

**配置步骤：**

进入**模板和对象>对象管理>应用对象：域名列表**，点击**新建**，如下图




**名称**：域名的内容，输入为字符串。

**匹配类型**：下拉，包括：完全匹配、包含。

完全匹配：会将所配置的字符串，与域名进行完整比对。

包含：查找域名中，是否包含了配置的字符串。

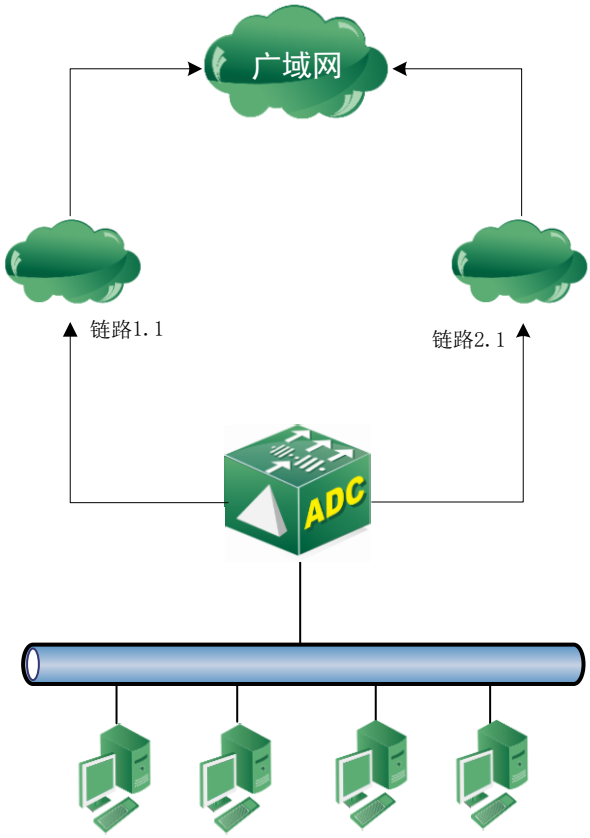
点击**提交**。

## 11.3 配置案例

### 11.3.1 配置案例

**案例描述：**

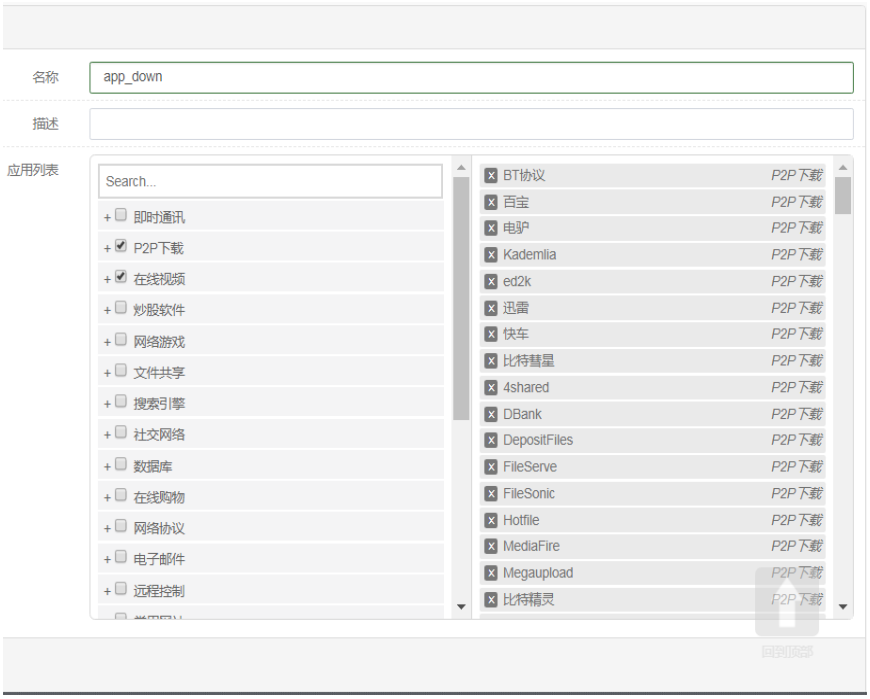
将下载应用等几类占带宽的应用放置于一条链路上，其余流量走另一条链路，从而完成对应用的引流。



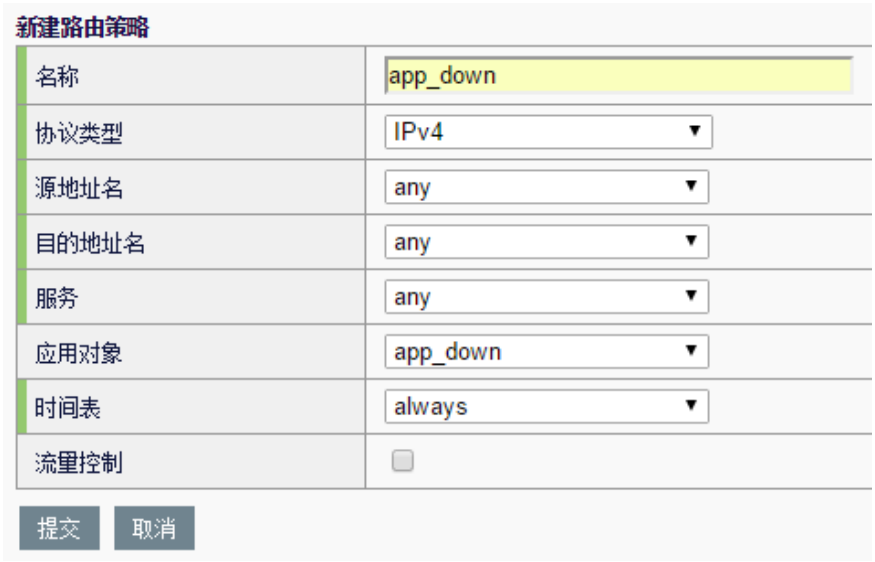

1. 下载流量对应于链路 1.1。
2. 其余流量对应于链路 2.1。
3. 这里的配置会涉及到路由策略、虚拟链路、链路池，请分别参阅对应的章节。

**配置步骤：**

1. 配置应用组，选中 P2P 下载、在线视频。




2. 在路由策略中引用该对象，参照“路由策略”一章。




3. 在虚拟链路中引用该路由策略，需要参照“虚拟链路”、“链路池”。


其中 app_down 的流量导入到 1.1 的链路池中，其余流量走默认链路池 2.1。

4. 具体的链路配置及网络接口配置，请参照“虚拟链路”中的示例，这里不做重点。
5. 访问对应的应用，查看效果。

## 11.4 监控与维护

### 11.4.1 查看预定义应用

进入**模板和对象>对象管理>应用对象：预定义应用**，通过左侧树状目录中选择应用，如下：


## 11.4.2 查看自定义应用

进入**模板和对象>对象管理>应用对象：自定义应用**，如下：


## 11.4.3 查看应用组

进入**模板和对象>对象管理>应用对象：应用组**，如下：

### 11.4.4 查看域名

进入**模板和对象>对象管理>应用对象：域名列表**，如下：

| 名称 | 类型 |
| --- | --- |
| qq | 包含 |
| www.baidu.com | 完全匹配 |

## 11.5 常见故障分析

### 11.5.1 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 |

### 11.5.2 故障现象：配置域名后，无法引流

| | |
| --- | --- |
| 现象 | 配置域名后，发现无法正常引流 |
| 分析 | 着重从下面几个方面查找：<br>域名是完整字符串还是包含，二者效果不同；<br>确认链路配置是否正常；<br>确认DNS服务器有回应DNS请求； |

# 12 第12章 ISP 地址库

## 12.1 ISP地址库概述

ISP 地址库是运营商提供的公网地址的集合，该地址库可以被地址对象引用，地址对象被策略路由引用使用在出站链路负载均衡中。通过对出站流量的目的地址与 ISP 地址库的匹配，将流量引导到最合适的链路中去。

注意

1.ISP 地址库用于出站链路负载均衡的时候，不要将该地址库用于源地址对象。

2.ISP 地址库的格式是唯一的，只能是 A.B.C.D-A.B.C.D，其他的格式出现加载错误。

## 12.2 配置ISP地址库

ISP 地址库分为两类：预定义和自定义，预定义为系统自带，预定义 ISP 地址库不管有没有被地址对象引用都不能被删除；自定义为用户上传，自定义 ISP 地址库在没有被地址对象引用的情况下可以被删除。

### 12.2.1 配置ISP地址库

进入**模板和对象>对象管理>ISP 地址库**


**名称**：ISP 地址库的名称，不可以包含中文。

**类型**：ISP 地址库的类型。

**ISP 地址库导入**：导入 ISP 地址库。

**ISP 地址库导出**：导出 ISP 地址库。

### 12.2.2 ISP地址库导入

进入**模板和对象>对象管理>ISP 地址库，如下图：**


**选择文件**：选择合法的 ISP 地址库文件，如果文件名起始不是 ISP，则上传之后会被自动加上 ISP_。

**导入**：上传文件到系统存储设备中。

注意

1.导入的 ISP 地址库文件最多支持 10M 大小，大于 10M 会导入失败。

2.导入的 ISP 地址库只有被地址对象引用时才会进行加载，ISP 地址库的行数如果超过 1 万行，则加载时只会加载前 1 万行，后面的 ISP 地址不会被加载，即，ISP 地址库中一万行之后的地址不会生效。

### 12.2.3 ISP地址库导出

进入**模板和对象>对象管理>ISP 地址库，如下图：**


**导出**：选择需要导出的 ISP 地址库文件，从设备导出到本地。

### 12.2.4 ISP地址库删除

进入**模板和对象>对象管理>ISP 地址库，如下图：**


点击 删除


注意

当删除按钮为灰色时，表明该 ISP 地址库正在被地址对象引用，或者为预定义 ISP 地址库，不能被删除。

## 12.1 常见故障分析

### 12.1.1 ISP地址加载不完整

| | |
|---|---|
| 故障现象 | 当ISP地址库被地址对象引用之后，会被解析加载到内存中，当查看ISP地址库的时候发现部分ISP地址不存在。 |
| 分析与解决 | 1)ISP地址库行数超过一万行，大于一万行的地址范围不会被解析加载，该情况建议将ISP地址库文件分拆。 |

# 13 第13章 域名地址库

## 13.1 域名地址库概述

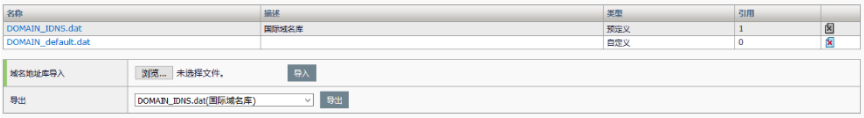
域名地址库是域名地址的集合，该地址库可以被应用对象和 DNS 代理策略引用，应用对象被策略路由引用使用在出站链路负载均衡中。通过对出站流量的域名地址与域名地址库的匹配，将流量引导到最合适的链路中去。

## 13.2 配置域名地址库

域名地址库分为两类：预定义和自定义，预定义为系统自带，预定义域名地址库不管有没有被引用都不能被删除；自定义为用户上传，自定义域名地址库在没有被引用的情况下可以被删除。

### 13.2.1 配置域名地址库

进入**模板和对象>对象管理>域名地址库**




**名称**：域名地址库的名称，不可以包含中文。

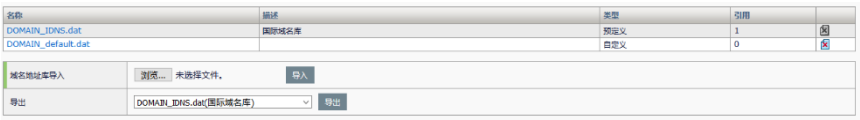
**类型**：域名地址库的类型。

**域名地址库导入**：导入域名地址库。

**域名地址库导出**：导出域名地址库。

### 13.2.2 域名地址库导入

进入**模板和对象>对象管理>域名地址库，如下图：**




**选择文件**：选择合法的域名地址库文件，如果文件名起始不是 DOMAIN_，则上传之后会被自动加上 DOMAIN_。

**导入**：上传文件到系统存储设备中。

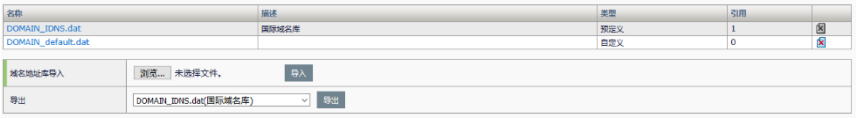
注意

可以导入任意后缀的文件，导入后，系统会自动修改为.dat 文件。

导入的域名地址库文件最多支持 10M 大小，大于 10M 会导入失败。

### 13.2.3 域名地址库导出

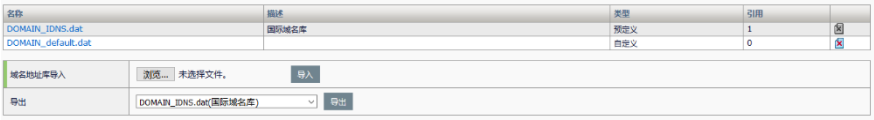
进入**模板和对象>对象管理>域名地址库，如下图：**




**导出：**选择需要导出的域名地址库文件，从设备导出到本地。

### 13.2.4 域名地址库删除

进入**模板和对象>对象管理>域名地址库，如下图：**



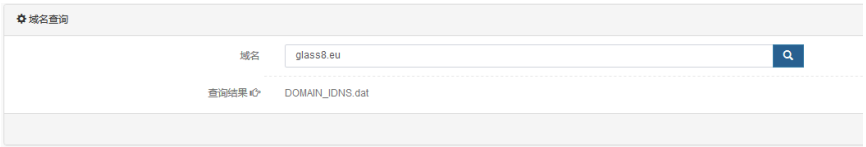

点击 删除

注意

当删除按钮为灰色时，表明该域名地址库正在被应用对象或者 DNS 代理策略引用，不能被删除。

### 13.2.5 域名查询

进入**模板和对象>对象管理>域名地址库>域名查询**




**域名：**为待查询域名，不得超过 127 个字符。

输入待查询域名，点击 。

## 13.3 常见故障分析

### 13.3.1 域名地址加载不完整

| | |
|---|---|
| 故障现象 | 当域名地址库被导入设备之后，会被解析加载到内存中，当查询域名地址的时候发现部分域名地址不存在。 |
| 分析与解决 | 域名地址库加载的总条目数超过两万行之后将不会再继续解析加载，该情况建议将未使用的域名地址库删除之后再进行导入。 |

# 14 第14章 路由策略

## 14.1 路由策略概述

路由策略是源地址、目的地址、服务、应用和时间表的集合，源地址和目的地址分别引用地址对象，服务引用服务对象，应用引用应用对象，时间表引用时间对象。用户可以根据需求，将匹配路由策略的流量引导到指定的链路上。


注意

路由策略用于出链路选路中，对于源地址对象尽量避免使用 ISP 地址库。

## 14.2 配置路由策略

### 14.2.1 配置路由策略

1. 配置路由策略之前，需要配置相应的地址对象、服务对象、应用对象和时间对象。
2. 进入**模板对象>路由策略**，点击**新建**。


**参数说明：**

**名称：**路由策略名称，可以为中文。

**协议类型：**IPv4 或者 IPv6。

**源地址名：**引用地址对象，用于匹配报文的源地址。

**目的地址名：**引用地址对象，用于匹配报文的目的地址。

**服务：**引用服务对象，用于匹配报文的服务类型。

**应用对象：**引用应用对象，用于匹配流量的应用类型。

**时间表：**引用时间对象，用于匹配当前时间。

**流量控制：**

对匹配上述条件的流量进行控制，勾选后，会出现下列选项：

**总上行带宽限制：**限制符合该策略匹配条件的上行流量，范围为 10-40000000Kb/s。

**总下行带宽限制：**限制符合该策略匹配条件的下行流量，范围为 10-

40000000Kb/s。

**主机上行带宽限制：**限制符合该策略匹配条件的每主机上行流量，范围为10-40000000Kb/s。

**主机下行带宽限制：**限制符合该策略匹配条件的每主机下行流量，范围为10-40000000Kb/s。

**上行带宽保证：**在链路负载均衡环境下，当链路节点发生拥塞时，对符合该策略匹配条件的流量进行上行带宽保证，范围为 10-40000000Kb/s。

**下行带宽保证：**在链路负载均衡环境下，当链路节点发生拥塞时，对符合该策略匹配条件的流量进行下行带宽保证，范围为 10-40000000Kb/s。

**优先级：**指定符合该策略匹配条件的流量的优先级，优先级分为高、中、普通、低，缺省设置为普通。在链路负载均衡环境下，当链路节点发生拥塞时，优先级较高的流量会被优先发送。

3. 点击**提交**。


注意

对于上行带宽保证、下行带宽保证、优先级这三个选项，配置时需要注意:

1、 只有在链路负载均衡环境下，才需要配置。

2、要和链路节点带宽同时配置。只有在配置了链路节点带宽的前提下，当链路节点发生拥塞时，以上功能才会生效。

3、配置链路节点带宽时，上行带宽保证的值必须不大于链路节点上行带宽的值，下行带宽保证的值必须不大于链路节点下行带宽的值。

### 14.2.2 查看路由策略列表

1. 进入**模板和对象>路由策略**，如下图：


2. 点击**名称**字段可编辑对应路由策略。

3. 点击 即可删除对应路由策略。


注意

路由策略的参数栏目为灰色表示不能编辑。

代表该条路由策略正在被引用，不能被删除。

## 14.3 配置案例

### 14.3.1 路由策略案例 1

**案例描述：**

企业需要通过 ADC 访问外网，财务部门在工作时间需要通过电信专线访问外网，财务部门 IP 地址范围 192.168.0.10 – 192.168.0.20

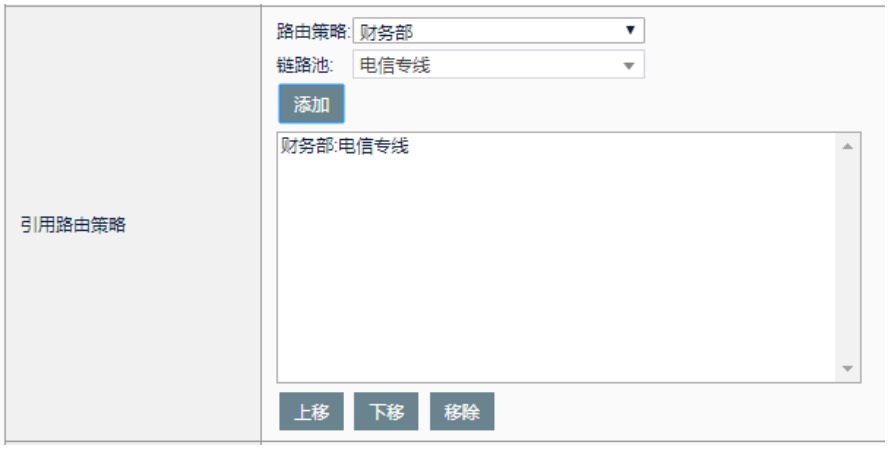
**配置步骤：**

1. 进入**模板和对象>对象管理>地址对象**，创建**财务部**地址对象。


2. 进入**模板和对象>对象管理>时间对象**，创建**工作时间对象**。


3. 进入**模板对象>路由策略**，创建**财务部路由策略**。

4. 进入**链路负载>虚拟链路**，编辑“lc”




**路由策略**选择**财务部**，**链路池**选择**电信专线**，点击**添加**即可实现财务部在工作时间通过电信专线访问外网。

## 14.4 常见故障分析

### 14.4.1 配置路由策略不生效

| | |
|---|---|
| 现象 | 在虚拟链路（Vlink）中配置的引用路由策略无法生效 |
| 分析 | 有可能是以下几种情况导致该策略无法生效：<br>➢ 当引用多条路由策略时，路由策略的匹配是按照自上而下的顺序进行匹配的，数据流可能匹配到前面的某条策略，请检查配置是否冲突。<br>➢ 匹配条件有一项或多项未匹配。 |
| 解决 | 可以根据需求修改路由策略或者改变路由策略的顺序。 |

# 15 第15章 会话保持

## 15.1 会话保持概述

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

会话保持功能提供了 11 种类型，共计 13 种会话保持方法。

- HTTP Cookie（包括 HTTP Cookie Insert 和 HTTP Cookie Rewrite）
- HTTP SessionID
- HTTP ServerID（包括 Default ServerID 和 Custom ServerID）
- HTTP 自定义头域
- 源地址
- SSL SessionID
- 目的地址
- Radius
- 基于 SIP Call-id
- DNS 代理
- DNS 代理源地址

## 15.2 会话保持和“TCP连接复用”的关系

当虚拟服务没有开启“TCP 连接复用”的时候，会话保持是基于一条 TCP 连接的，若当前的 TCP 连接已经通过会话保持建立，那么同一条连接中的后续请求，会话保持会忽略。比如：虚拟服务引用了 cookie 会话保持模版，同时不开启“TCP 连接复用”，这样在一条 TCP 连接第一个请求的 cookie 中携带了服务器 A 的信息，那么会话保持会把请求发送给 A，若第二个请求的 cookie 中携带了服务器 B 的信息，那么会话保持将会忽略 B 的

信息，而把请求同样发给 A。这种情况一般出现在多个访问者通过同一个代理访问虚拟服务，并且这个代理会把多个访问者的请求在一个 TCP 连接里进行复用的环境中发生。

当虚拟服务开启“TCP 连接复用”的时候，会话保持将会基于每个请求的。每个请求来的时候都会独立的重新做会话保持。这样在上面的例子中，同一个 TCP 连接中，第一个请求携带服务器 A 的信息，那么会话保持会把请求发给 A，同时第二个请求携带了服务器 B 的信息，会话保持会把请求发给 B。

## 15.3 会话保持中多虚拟服务协同工作选项

当配置了多个互相关联的虚拟服务的时候，有时需要这些虚拟服务协同配合工作，也就是某些虚拟服务需要用到其它虚拟服务的会话保持结果。那么就需要三个用于虚拟服务协同工作的选项。

- 跨服务匹配
- 跨虚拟服务匹配
- 跨服务池匹配

其中 HTTP SessionID、源地址、SSL SessionID 和目的地址这 4 类会话保持模版上提供了这三个选项，默认是关闭的。如下图：


### 15.3.1 跨服务匹配

如果多个虚拟服务的 IP 相同，端口不同，那么把这些虚拟服务看成是一组端口不同的服务。如果开启了“跨服务匹配”，在所请求的虚拟服务中，若会话保持失败时，会尝试查询 IP 相同但端口不同的其它的虚拟服务的会话保持结果。

比如：配置了两个虚拟服务 vs1（vs_ip:80）和 vs2（vs_ip:443），这两个虚拟服务的 IP 相同，端口一个为 80，一个为 443。vs1 的服务池 http_pool 中包含成员 ip1:80 和 ip2:80，vs2 的服务池 https_pool 中包含成员 ip1:443 和 ip2:443。

假设第一个请求访问了 vs1，并且通过负载均衡算法把请求发给了 ip1:80，之后相同客户端来的请求访问了 vs2，如果 vs2 的会话保持没有开启“跨服务匹配”，那么这个请求会重新用负载均衡算法选出要转发的成

员，如果 vs2 的会话保持开启了“跨服务匹配”，那么会话保持会借用 vs1:vs_ip:80 的会话保持结果 ip1:80，在 https_pool 中选出 ip1:443 作为会话当次的会话保持结果。这样就可以让 vs1 和 vs2 关联的会话保持协同工作。

> 能够协同工作的前提是各自的服务池内必须有 IP 相同的成员。例如上述例子中，服务池 https_pool 中存在服务池 http_pool 中 IP 相同的成员。也就是说，如果服务池 http_pool 中有 ip1:80，那么服务池 https_pool 中必须配有 ip1:443。

### 15.3.2 跨虚拟服务匹配

当开启了“跨虚拟服务匹配”，那么只要当前虚拟服务的会话保持失败，就会去查询所有虚拟服务的会话保持结果。

比如：配置了两个虚拟服务 vs1（vs_ip1:80）和 vs2（vs_ip2:443），这两个虚拟服务的 IP 不相同。vs1 的服务池 http_pool 中包含成员 ip1:80 和 ip2:80，vs2 的服务池 https_pool 中包含成员 ip1:443 和 ip2:443。

假设第一个请求访问了 vs1，并且通过负载均衡算法把请求发给了 ip1:80，之后相同客户端来的请求访问了 vs2，如果 vs2 的会话保持没有开启“跨虚拟服务匹配”，那么这个请求会重新用负载均衡算法选出要转发的成员，如果 vs2 的会话保持开启了“跨虚拟服务匹配”，那么会话保持会借用 vs1（vs_ip1:80）的会话保持结果 ip1:80，在 https_pool 中选出 ip1:443 作为会话当次的会话保持结果。这样就可以让 vs1 和 vs2 关联的会话保持协同工作。

> 能够协同工作的前提和“跨服务匹配”的前提相同，各自的服务池内必须有 IP 相同的成员。

### 15.3.3 跨服务池匹配

当开启这个选项后，会话保持会使用所有的服务池。比如当开启了跨虚拟服务匹配选项，在其他的虚拟服务的会话保持表中找到了结果，但这个结果的成员并不在当前使用的服务池中，那么依然会把这个结果当做会话保持的结果。

会导致请求发给没有和当前虚拟服务关联的服务池，要小心使用。

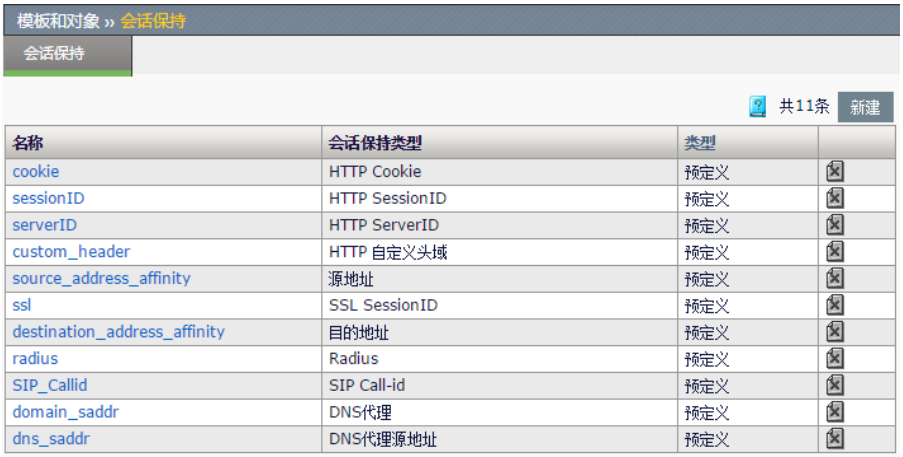
若与“跨服务匹配”或“跨虚拟服务匹配”同时开启，则不需要协同工作的服务池中有相同 IP 的成员。

## 15.4 会话保持配置

**配置步骤：**

1. 配置会话保持模板

进入**模版和对象>会话保持**，如下图：




| 名称 | 会话保持类型 | 类型 | |
|---|---|---|---|
| cookie | HTTP Cookie | 预定义 | |
| sessionID | HTTP SessionID | 预定义 | |
| serverID | HTTP ServerID | 预定义 | |
| custom_header | HTTP 自定义头域 | 预定义 | |
| source_address_affinity | 源地址 | 预定义 | |
| ssl | SSL SessionID | 预定义 | |
| destination_address_affinity | 目的地址 | 预定义 | |
| radius | Radius | 预定义 | |
| SIP_Callid | SIP Call-id | 预定义 | |
| domain_saddr | DNS代理 | 预定义 | |
| dns_saddr | DNS代理源地址 | 预定义 | |

**新建**：添加一个会话保持模板。

：删除掉该模板。

所有会话保持方法的配置都是基于会话保持模版，为了用户方便使用，系统自带了 11 个预定义模版，见上图所示，用户在使用中可以直接使用系统提供的预定义模版，也可以点击**新建**按钮选已存在的模版中的一个为基础，创建新的自定义模版。

自定义模板的具体配置方法见后面章节。

11 个预定义模版不可删除，可以修改，但建议不对默认模版做修改。

2. 在**虚拟服务**或**虚拟链路**中引用会话保持模板

在**虚拟服务**或**虚拟链路**中的**默认会话保持模版**和**备选会话保持模版**的下拉菜单中，可以看到创建好的会话保持模版。只有在下拉菜单中选中的模版

才会生效，见下图所示：


“虚拟服务”中的“默认会话保持模版”可以选择所有会话保持模版，“备选会话保持模版”的下拉菜单可以看到源地址类型的模版。

“虚拟链路”中的“默认会话保持模版”可以源地址和目的地址类型的会话保持模版，“备选会话保持模版”的下拉菜单可以看到源地址类型的模版。

## 15.5 HTTP Cookie模版配置

点击**模版和对象>会话保持**界面的**新建**按钮，在**会话保持类型**中选**基于HTTP Cookie**，出现下面界面：


**名称**：该模版的名称。

**会话保持类型**：可选择 11 个类型之一。

**继承模版**：在创建自定义的模版时，可以选择一个已经存在的模版做为基础，进行修改。

**Cookie 方法选择**：选择 HTTP Cookie Insert 或 HTTP Cookie Rewrite。默认 HTTP Cookie Insert。

**Cookie 名称**：指定要插入或重写的 cookie 的名称。默认为空，采用系统内部定的默认值。

**过期时间**：指定插入或重写的 cookie 的过期时间。可以指定过期的时间，或选择“Cookie 同浏览器时间”，表示只要浏览器不关 cookie 一直有效。默认选中“Cookie 同浏览器时间”。

**忽略服务池成员连接限制**：当选中时，连接限制超出了服务池成员的连接限制，依然能通过会话保持建立连接，但不可超出服务器的连接限制。

**Cookie 版本**：0 表示服从 Netscape 准则，1 表示服从 rfc2109 的标准，默认选择版本 0。

**提交**：配置生效。

---

版本 0 兼容度最高，目前几乎所有浏览器都支持。负载均衡设备要自己计算过期的日期和时间。版本 1，个别老浏览有可能不支持，但负载均衡设备不需要自己计算过期的日期和时间。考虑兼容性，推荐采用版本 0。

---

## 15.5.1 Cookie 插入方法

这种方法会在 HTTP 的响应中插入类似：
“SetCookie: Cookie 名称+服务池名称
=XXXXXXX.XXXX;expires=XXX;path=/”
的头域。

其中包括了编码过的服务池成员信息。当客户端请求再次到达，会携带之前插入的信息，我们重新解码出服务池成员的信息，把请求发往同一个服务池成员。

---

这种方法不需要后台服务器做任何配置改变，相比较”Cookie 重写”，我们推荐用户用此方法。

---

## 15.5.2 Cookie 重写方法

和 Cookie 插入方法原理类似，会把后台服务器响应中固定的一段“SetCookie”头域用编码过的服务池成员信息重写。当客户端请求再次到达，会携带之前重写的信息，我们重新解码出服务池成员的信息，把请求发往同一个服务池成员。

这种方法需要后台的服务器做一定的配置，使服务器主动 Setcookie。如下：

以 Apache 服务器为例，假设用户配置的 Cookie 名称为"testrewrite"，打开 apache 的配置文件 conf/httpd.conf，把下面这句话的前注释去掉。若没有这句话，则添加：

LoadModule headers_module modules/mod_headers.so

同时在文件末尾添加这样一句话：

Header add Set-Cookie "testrewrite=00000000...."

0 的个数要大于 120 个。若配置的 Cookie 名称很长，那么 0 的个数还要相应的增加，建议 0 的个数为：cookie 名称的长度+70，这是为了给后面重写 Cookie 提供足够的空间。

## 15.6 HTTP SessionID模版配置

点击**模版和对象>会话保持**界面的**新建**按钮，在**会话保持类型**中选**基于 HTTP SessionID**，出现下面界面：


**名称**：该模版的名称。

**会话保持类型**：可选择 11 个类型之一。

**继承模版**：在创建自定义的模版时，可以选择一个已经存在的模版做为基础，进行修改。

**SessionID 名称**：记录 sessionid 的变量的名称，大小写敏感。

> 这里 sessionid 名称对不同的应用系统往往不同，需要根据应用来配置。这里举几个例子，例如一些用 javeEE 开发的项目，常用“jsessionid”；discuz 论坛常用的是“discuz_2132_auth”；部分 asp 开发的应用是“ASPSESSIONID”。

**超时时间**：sessionid 的超时时间。可以指定秒数，或设为无穷。

**开启 HA 同步**：开启 sessionid 会话保持表的同步。当会话保持表表项有增减，则做表项的同步。如果开启系统性能会有下降。默认关闭。

**跨服务匹配**：用 sessionid 来区分是否是相同的客户端。默认关闭。

**跨虚拟服务匹配**：用 sessionid 来区分是否是相同的客户端。默认关闭。

**跨服务池匹配**：可以调度到非虚拟服务关联的服务池。默认关闭。

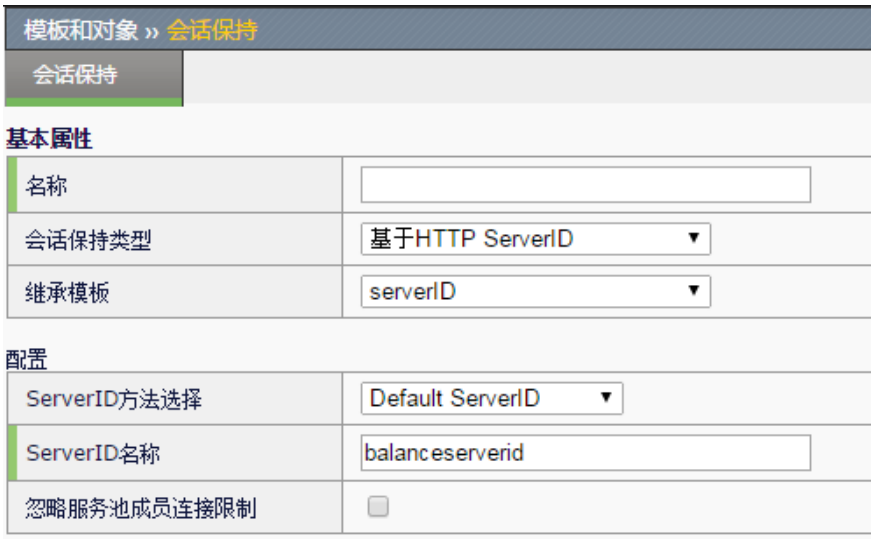
**忽略服务池成员连接限制**：当选中时，连接限制超出了服务池成员的连接限制，依然能通过会话保持建连接。但不可超出服务器的连接限制。

**提交**：配置生效。

> HTTP SessionID 方法的工作过程：当用户登陆的时候，后台服务器会产生一个 sessionid，通过 SetCookie，返回给客户端。会话保持把这个 sessionid 和后台的服务器进行关联，当客户端的后续请求带有此 sessionid 时，会话保持把请求发给同一台服务器。

## 15.7 HTTP ServerID模版配置

点击**模版和对象>会话保持**界面的**新建**按钮，在**会话保持类型**中选**基于 HTTP ServerID**，出现下面界面：




**名称**：该模版的名称。

**会话保持类型**：可选择 11 个类型之一。

**继承模版**：在创建自定义的模版时，可以选择一个已经存在的模版做为基础，进行修改。

**ServerID 方法选择**：Default ServerID 或 Custom ServerID。

**ServerID 名称**：存放 ServerID 的变量的名称，默认 balanceserverid。

**忽略服务池成员连接限制**：当选中时，连接限制超出了服务池成员的连接限制，依然能通过会话保持建连接，但不可超出服务器的连接限制。

**提交**：配置生效。

### 15.7.1 Default ServerID方法

这种方法的工作过程为，客户端后续的请求会携带服务池成员返回的 ServerID，会话保持根据 ServerID 解码出服务池成员的 IP 和端口。从而把后续请求发给同一个服务池成员。

这种方法需要后台的服务器做一定的配置。假设用户配置的 ServerID 名称为“testserverid”，以 Apache 服务器为例，打开 Apache 的配置文件 conf/httpd.conf，把下面这句话的前注释去掉，若没有这个话，则添加：

LoadModule headers_module modules/mod_headers.so

同时在文件末尾添加这样一句话：

Header add Set-Cookie "testserverid=AAAAAAA.BBBBB"

“testserverid”后跟的内容为服务器的编码。其中“AAAAAAA”为 IP 地址的编码，“PPPP”为端口的编码，编码方式如下：

若 IP 为 ipv4（a.b.c.d），那么编码为 d*(256^3) + c*(256^2) + b*256 +a；

若 PORT 为 1433，因为 1433=5*256 + 153，编码为 153*256 + 5 = 39173；

例如：后台服务器为 192.168.31.57:1443 编码为“958376128.39173”

若 IP 为 ipv6，把完整地址拆成 16 个 16 进制数，每 4 个为一组 a1 a2 a3 a4 b1 b2 b3 b4 c1 c2 c3 c4 d1 d2 d3 d4。每组 4 个数计算一个值：

A=a1+256*a2+256^2*a3+256^3*a3，

B=b1+256*b2+256^2*b3+256^3*b3，

C=c1+256*c2+256^2*c3+256^3*c3，

D=d1+256*d2+256^2*d3+256^3*d3，

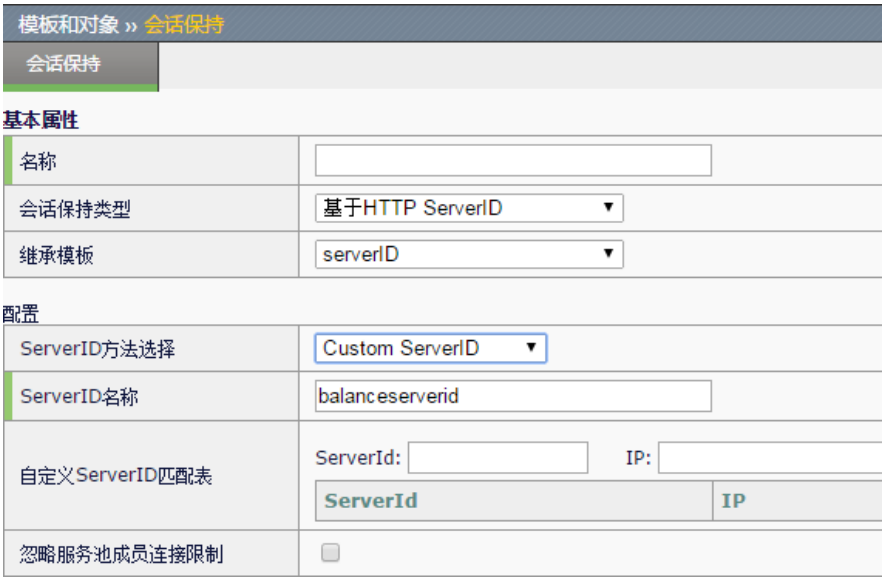
端口编码方法同上；

最后编码为 A_B_C_D:PPPP，

例如后台服务器为 0102:0304:0505::1 :80 编码为“67305985_1285_0_16777216.20480”。

## 15.7.2 Custom ServerID方法

“ServerID 方法选择”中，选中“Custom ServerID”后出现可编辑的“自定义 ServerID 匹配表”，可以输入 serverid、IP 和端口。




与 Default ServerID 方法不同是，后台服务器携带的不是编码过的 IP 和端口，而是用户自定义的 ServerID。

这种方法的工作过程为，客户端后续的请求会携带服务池成员返回的 ServerID，会话保持根据 ServerID 查表得到服务池成员的 IP 和端口。从而把后续请求发给同一个服务池成员。

这种方法需要后台服务器需要做一定的配置。假设用户配置的 ServerID 名称为“testserverid”。

以 Apache 服务器为例，打开 Apache 的配置文件 conf/httpd.conf，把下面这句话的前注释去掉。若没有这个话，则添加：

LoadModule headers_module modules/mod_headers.so

同时在文件末尾添加这样一句话：

Header add Set-Cookie "testserverid=XXXXX..."

其中“XXXX...”为表中添加的服务器 id，范围 0~65535。

> 自定义 ServerID 匹配表中的 IP 和 PORT 必须是虚拟服务所关联的服务池中的或内容交换选出的服务池中的健康成员。否则此行配置无效。

## 15.8 HTTP自定义头域模版配置

点击**模版和对象>会话保持**界面的**新建**按钮，在**会话保持类型**中选**基于 HTTP 自定义头域**，出现下面界面：


**自定义头域名称**：指定会话保持所用的自定义头域的名称。参考 RFC 文档中 HTTP 头域格式为“名称：值”的格式，名称大小写不敏感。所以本方法支持对所有这种格式的自定义头域做会话保持。比如常见的“Host”、“User-Agent”、“Accept-Encoding”等等，也可以用自定义的头域，比如“CALL-ID”，”PHONE_NUM”等等。

对于其它非这种格式的头域，我们给出了几个特殊的名称，比如 uri，method，如果需要使用可以直接用。比如在名称中填写“uri”，那么下面就取 http 请求的 uri 路径作为匹配的头域。例如访问 http://www.abc.com/a/b/c?aaa=111，那么取“/a/b/c?aaa=111”来做会话保持。若名称填写“method”，那么根据请求的 method 做会话保持，比如“GET”、“POST”等。

**忽略服务池成员连接限制**：当选中时，连接限制超出了服务池成员的连接限制，依然能通过会话保持建连接，但不可超出服务器的连接限制。

**开启 HA 同步**：开启自定义头域会话保持表的同步。当会话保持表表项有增减，则做表项的同步。如果开启系统性能会有下降。默认关闭。

**超时时间**：自定义头域的超时时间。可以指定秒数，或设为无穷。

**自定义头域匹配表**：

**添加按钮**：添加表项。

表中可配置多行匹配项：分为“字符串”、“正则”和“默认”，三种类型。匹配时从上到下依次进行。

 **按钮**：上下移动来修改匹配顺序。

 **按钮**：删除当前行。

**字符串**：若自定义头域中包含此字符串，则命中，用后面的 ip 和端口做会话保持，注意这个是字符串大小写敏感的。

**正则**：若自定义头域能完全匹配这个正则表达式，则命中，用后面的 ip 和端口做会话保持。

**默认**：通过计算完整自定义头域的 hash，做会话保持。默认的只可以有一行，通常都放在最后一行。

**提交**：配置生效。

自定义头域匹配表中的 IP 和 PORT 必须是虚拟服务所关联的服务池中的或内容交换选出的服务池中的健康成员。否则此行配置无效。（默认类型除外）。

建议把“默认”方法放在最后。

HTTP 自定义头域方法的工作过程：会话保持根据 HTTP 自定义头域中内容，按表中从上到下依次匹配字符串或正则以及查自定义头 hash 表来做会话保持。

## 15.9 源地址模版配置

点击**模版和对象>会话保持**界面的**新建**按钮，在**会话保持类型**中选**基于源地址**，出现下面界面：


**开启 HA 同步**：开启源地址会话保持表的同步。当会话保持表表项有增减，则做表项的同步。如果开启系统性能会有下降。默认关闭。

**跨服务匹配**：用源地址来区分是否是相同的客户端。默认关闭。

**跨虚拟服务匹配**：用源地址来区分是否是相同的客户端。默认关闭。

**跨服务池匹配**：可以调度到非虚拟服务关联的服务池。默认关闭。

**IPv4 掩码**：当指定了 IPv4 掩码后，会把掩码和 IP 地址进行“AND”运算，若结果相同，则把这些当成一个源地址来调度。

**IPv6 掩码**：当指定了 IPv6 掩码后，会把掩码和 IP 地址进行“AND”运算，若结果相同，则把这些当成一个源地址来调度。

---

这里的“掩码”，是广义的掩码。不一定非得是 255.255.255.0 或者是 255.255.128 这种，也可以是 0.255.0.128 这种。

---

**超时时间**：源地址的超时时间。可以指定秒数，或设为无穷。

**忽略服务池成员连接限制**：当选中时，连接限制超出了服务池成员的连接限制，依然能通过会话保持建连接，但不可超出服务器的连接限制。

**提交**：配置生效。

---

源地址会话保持的工作过程：当后续客户端 IP 地址相同的请求，发给相同的服务池成员。

---

## 15.10 SSL SessionID模版配置

点击**模版和对象>会话保持**界面的**新建**按钮，在**会话保持类型**中选**基于SSL SessionID**，出现下面界面：


**开启 HA 同步**：开启 SSL 会话保持表的同步。当会话保持表表项有增减，则做表项的同步。如果开启系统性能会有下降。默认关闭。

**跨服务匹配**：用 SSL SessionID 来区分是否是相同的客户端。默认关闭。

**跨虚拟服务匹配**：用 SSL SessionID 来区分是否是相同的客户端。默认关闭。

**跨服务池匹配**：可以调度到非虚拟服务关联的服务池。默认关闭。

**超时时间**：SSL SessionID 的超时时间。可以指定秒数，或设为无穷。

**忽略服务池成员连接限制**：当选中时，连接限制超出了服务池成员的连接限制，依然能通过会话保持建连接，但不可超出服务器的连接限制。

**提交**：配置生效。

> SSL SessionID 方法的工作过程：当客户端和服务池成员进行 SSL 握手的过程中，服务池成员会产生一个 SSL SessionID，会话保持把这个 SSLSessionID 和服务池成员关联起来。当客户端再次携带次 SSLSessionID 到来，把请求发给相同的服务池成员。

## 15.11 目的地址模版配置

点击**模版和对象>会话保持**界面的**新建**按钮，在**会话保持类型**中选**基于目的地址**，出现下面界面：


**开启 HA 同步**：开启目的地址会话保持表的同步。当会话保持表表项有增减，则做表项的同步。如果开启系统性能会有下降。默认关闭。

**跨服务匹配**：用目的地址来区分是否是相同的客户端。默认关闭。

**跨虚拟服务匹配**：用目的地址来区分是否是相同的客户端。默认关闭。

**跨服务池匹配**：可以调度到非虚拟服务关联的服务池。默认关闭。

**IPv4 掩码**：当指定了 IPv4 掩码后，会把掩码和 IP 地址进行“AND”运算，若结果相同，则把这些当成一个源地址来调度。

**IPv6 掩码**：当指定了 IPv6 掩码后，会把掩码和 IP 地址进行“AND”运算，若结果相同，则把这些当成一个源地址来调度。

---

这里的“掩码”，是广义的掩码。不一定非得是 255.255.255.0 或者是 255.255.128 这种，也可以是 0.255.0.128 这种。

---

**超时时间**：目的地址的超时时间。可以指定秒数，或设为无穷。

**忽略服务池成员连接限制**：当选中时，连接限制超出了服务池成员的连接限制，依然能通过会话保持建连接，但不可超出服务器的连接限制。

**提交**：配置生效。

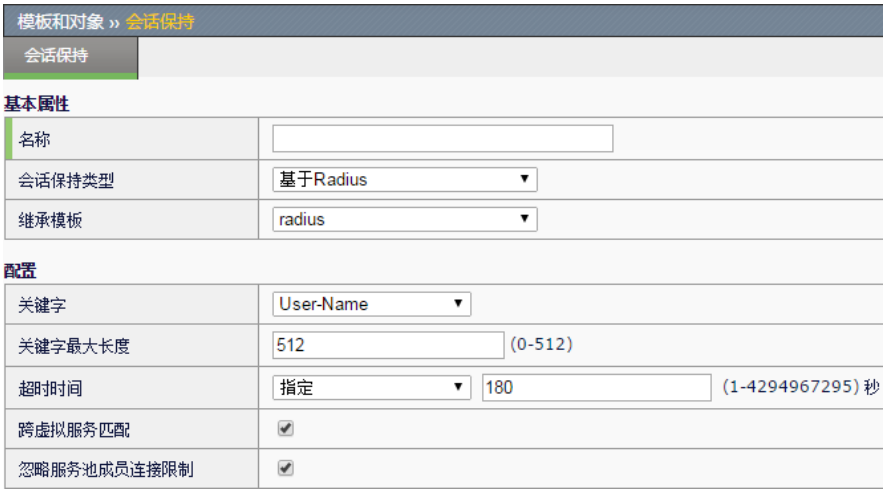
---

目的地址方法的工作过程：当后续请求访问的相同的目的地址，发给相同的服务池成员。

---

## 15.12 Radius模版配置

点击**模版和对象>会话保持**界面的**新建**按钮，在**会话保持类型**中选**基于 Radius**，出现下面界面：




**关键字**：Radius 会话保持类型，指定根据哪个关键字进行会话保持，目前支持 username，framed-ip-address，calling-station-id，默认 username。

**关键字长度**：关键字有效的最大长度，默认 512。

**超时时间**：Radius 会话保持超时时间。可以指定秒数，或设为无穷，默认 180 秒。

**跨虚拟服务匹配**：本 VS 的 Radius 会话保持表项没有查到，查找其他 VS 上的 Radius 会话保持，默认开启。

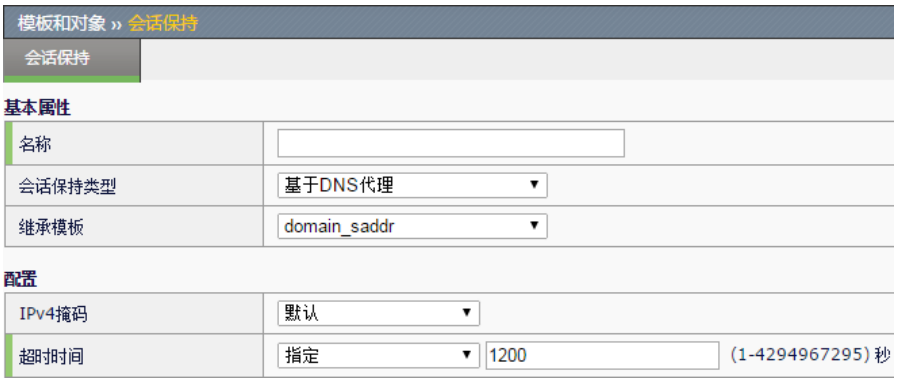
**忽略服务池成员连接限制**：当选中时，连接限制超出了服务池成员的连接限制，依然能通过会话保持建连接，但不可超出服务器的连接限制，默认开启。

**提交**：配置生效。

> Radius 会话保持的工作过程：当后续 Radius 请求带有相同关键字时，发给相同的服务池成员。

## 15.13 DNS代理会话保持模版配置

点击**模版和对象>会话保持**界面的**新建**按钮，在**会话保持类型**中选**基于 DNS 代理**，出现下面界面：




**IPv4 掩码**：当指定了 IPv4 掩码后，会把掩码和 IP 地址进行“AND”运算，若结果相同，则把这些当成一个源地址来调度。

> 这里的“掩码”，是广义的掩码。不一定非得是 255.255.255.0 或者是 255.255.128 这种，也可以是 0.255.0.128 这种。

**超时时间**：源地址的超时时间。可以指定秒数，或设为无穷。默认为 1200 秒。

**提交**：配置生效。

> DNS 请求域名和源地址会话保持的工作过程：当后续客户端 IP 地址相同并且请求的域名相同时，发给相同的服务池成员。

## 15.14 DNS代理源地址会话保持模版配置

点击**模版和对象>会话保持**界面的**新建**按钮，在**会话保持类型**中选**基于 DNS 代理源地址**，出现下面界面：


**IPv4 掩码**：当指定了 IPv4 掩码后，会把掩码和 IP 地址进行“AND”运

算，若结果相同，则把这些当成一个源地址来调度。

> 这里的“掩码”，是广义的掩码。不一定非得是 255.255.255.0 或者是 255.255.128 这种，也可以是 0.255.0.128 这种。

**超时时间**：源地址的超时时间。可以指定秒数，或设为无穷。默认为 1200 秒。

**提交**：配置生效。

> DNS 请求源地址会话保持的工作过程：当后续客户端 IP 地址相同时，发给相同的服务池成员。

## 15.15 SIP Call-id会话保持模板配置

点击**模版和对象>会话保持**界面的**新建**按钮，在**会话保持类型**中选**基于 SIP Call-id**，出现下面界面：


**超时时间**：基于 SIP Call-id 会话保持超时时间。可以指定秒数，或设为无穷，默认 600 秒。

## 15.16 常见故障分析

### 15.16.1 故障现象1：会话保持不起作用

| | |
|---|---|
| 现象 | 配了会话保持导致虚拟服务不通，或会话保持一直无效 |
| 分析 | 有可能是以下几种情况导致的：<br>1. HTTP Cookie、HTTP SessionID、HTTP ServerID、 |

| | |
|---|---|
| | HTTP自定义头域这四中会话保持方法，必须在配置了HTTP模版的前提下才会生效。<br>2. SSL SessionID会话保持模版不可与SSL的客户端模版和SSL的服务器模版同时配置。<br>3. Custom ServerID表或自定义头域表中中服务池成员不健康或不在池中。 |
| 解决 | 检查上面分析中的配置是否正确。 |

# 16 第16章 健康检查

## 16.1 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，TCP，UDP，HTTP，HTTPS，RADIUS，LDAP，FTP，POP3，SMTP 等等，除了使用 ICMP 能够对连通性监控外，对具体的服务可以使用相应的检查方式提供更准确的监控。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。

应用交付设备提供了 IPv4 和 IPv6 服务器的健康检查功能。

## 16.2 配置健康检查

进入**模板和对象>健康检查>健康检查列表**，点击**新建**。


**名称**：健康检查模板的名称。

**类型**：健康检查的类型。选择类型后弹出具体类型的模板配置。

**应用范围**：健康检查使用的范围。通用是指可以在系统任何使用健康检查的模块使用；全局负载是指只能在智能 DNS 页面的全局负载模块使用。

**配置步骤**：

1. 输入**名称**。
2. 选择**类型**。

当类型为 ICMP 时，配置界面如下：


**名称**：指定新建健康检查模板的名称。

**类型**：指定新建健康检查模板的协议类型。

**应用范围**：健康检查使用的范围。通用是指可以在系统任何使用健康检查的模块使用；全局负载是指只能在智能 DNS 页面的全局负载模块使用。

**间隔**：健康检查发送状态探测包的间隔时间，单位为秒。

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

**超时时间**：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

**覆盖 IP 地址类型**：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

**覆盖 IP**：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机或链路时填写此项。

**透明模式**：用于配置模板采用透明传输方式进行检查。选择透明模式，则以引用该模板的对象作为下一跳，去探测覆盖 IP，此时覆盖 IP 必须配置。通常用于出站链路负载均衡的链路状态监控。

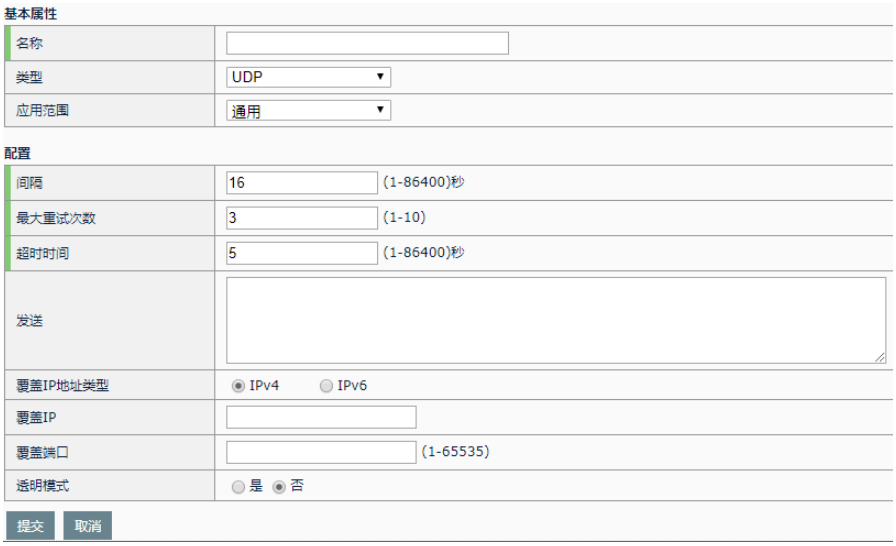
**探测延时**：计算使用该健康检查模板的对象的探测延迟时间。

**源 IP**：使用指定源 IP 发送 icmp 检查

**配置步骤：**

1. 根据需求选择应用范围使用**通用**或则**全局负载**
2. 输入**间隔**。
3. 输入**最大重试次数**。
4. 输入**超时时间**。
5. 选择**覆盖 IP 地址类型**。
6. 选择输入**覆盖 IP**。
7. 选择是否启用**透明模式**。
8. 填写**源 IP**
9. 点击**提交**。

当类型为 UDP 时，配置界面如下：




**名称：**指定新建健康检查模板的名称。

**类型：**指定新建健康检查模板的协议类型。

**应用范围：**健康检查使用的范围。通用是指可以在系统任何使用健康检查的模块使用；全局负载是指只能在智能 DNS 页面的全局负载模块使用。

**间隔：**健康检查发送状态探测包的间隔时间，单位为秒。

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

**超时时间：**发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

**发送：**UDP 报文中的发送内容。

**覆盖 IP 地址类型：**选择覆盖 IP 的地址类型，IPv4 或 IPv6。

**覆盖 IP**：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机或链路时填写此项。

**覆盖端口**：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置。

**透明模式**：用于配置模板采用透明传输方式进行检查。选择透明模式，则以引用该模板的对象作为下一跳，去探测覆盖 IP，此时覆盖 IP 必须配置。

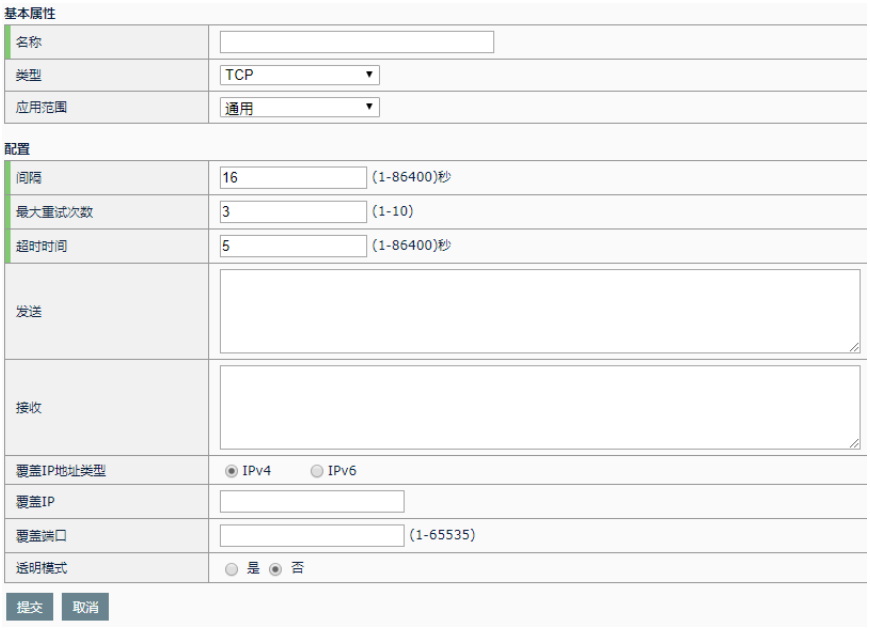
**配置步骤：**

1. 根据需求选择应用范围使用**通用**或则**全局负载**
2. 输入**间隔**。
3. 输入**最大重试次数**。
4. 输入**超时时间**。
5. 选择输入**发送**。
6. 选择**覆盖 IP 地址类型**。
7. 选择输入**覆盖 IP 和覆盖端口**。
8. 选择是否启用**透明模式**。
9. 点击**提交**。


提示

UDP 健康检查必须组合其他方式的健康检查使用，如 ICMP。因为 UDP 在服务不可用或者探测地址根本不存在时现象是相同的。

当类型为 TCP 时，配置界面如下：



**名称**：指定新建健康检查模板的名称。

**类型**：指定新建健康检查模板的协议类型。

**应用范围**：健康检查使用的范围。通用是指可以在系统任何使用健康检查的模块使用；全局负载是指只能在智能 DNS 页面的全局负载模块使用。

**间隔**：健康检查发送状态探测包的间隔时间，单位为秒。

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

**超时时间**：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

**发送**：TCP 报文中的发送内容。

**接收**：接收到报文中应含的内容。当接收到的内容不包含此内容时，状态为 DOWN。

**覆盖 IP 地址类型**：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

**覆盖 IP**：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机或链路时填写此项。

**覆盖端口**：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置。

**透明模式**：用于配置模板采用透明传输方式进行检查。选择透明模式，则以引用该模板的对象作为下一跳，去探测覆盖 IP，此时覆盖 IP 必须配置。

**配置步骤：**

1. 根据需求选择应用范围使用**通用**或则**全局负载**
2. 输入**间隔**。
3. 输入**最大重试次数**。
4. 输入**超时时间**。
5. 选择输入**发送**内容。
6. 选择输入**接收**内容。
7. 选择**覆盖 IP 地址类型**。
8. 选择输入**覆盖 IP 和覆盖端口**。
9. 选择是否启用**透明模式**。
10. 点击**提交**。

当类型为 TCP HALF OPEN 时，配置界面如下：


**名称**：指定新建健康检查模板的名称。

**类型**：指定新建健康检查模板的协议类型。

**应用范围**：健康检查使用的范围。通用是指可以在系统任何使用健康检查的模块使用；全局负载是指只能在智能 DNS 页面的全局负载模块使用。

**间隔**：健康检查发送状态探测包的间隔时间，单位为秒。

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

**超时时间**：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

**覆盖 IP 地址类型**：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

**覆盖 IP**：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机或链路时填写此项。

**覆盖端口**：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置。

**透明模式**：用于配置模板采用透明传输方式进行检查。选择透明模式，则以引用该模板的对象作为下一跳，去探测覆盖 IP，此时覆盖 IP 必须配置。

**探测延时**：计算使用该健康检查模板的对象的探测延迟时间。

**配置步骤：**

1. 根据需求选择应用范围使用**通用**或则**全局负载**
2. 输入**间隔**。
3. 输入**最大重试次数**。
4. 输入**超时时间**。
5. 选择**覆盖 IP 地址类型**。
6. 选择输入**覆盖 IP**。
7. 勾选是否启用**透明模式**。
8. 点击**提交**。


同 TCP 类型健康检查相比，TCP HALF OPEN 类型健康检查在设备和服务器之间不建立连接，减少了报文交互。

当类型为 FTP 时，配置界面如下：


**名称：**指定新建健康检查模板的名称。

**类型：**指定新建健康检查模板的协议类型。

**应用范围：**健康检查使用的范围。通用是指可以在系统任何使用健康检查的模块使用；全局负载是指只能在智能 DNS 页面的全局负载模块使用。

**间隔**：健康检查发送状态探测包的间隔时间，单位为秒。

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

**超时时间**：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

**用户名**：FTP 认证的用户名。

**密码**：FTP 用户的密码。

**覆盖 IP 地址类型**：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

**覆盖 IP**：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机或链路时填写此项。

**覆盖端口**：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置。

**配置步骤：**

1. 根据需求选择应用范围使用**通用**或则**全局负载**
2. 输入**间隔**。
3. 输入**最大重试次数**。
4. 输入**超时时间**。
5. 输入**用户名。**
6. 输入**密码。**
7. 选择**覆盖 IP 地址类型**。
8. 选择输入**覆盖 IP 和覆盖端口**。
9. 点击**提交**。

当类型为 HTTP/HTTPS 时，配置界面如下：


**名称**：指定新建健康检查模板的名称。

**类型**：指定新建健康检查模板的协议类型。

**应用范围**：健康检查使用的范围。通用是指可以在系统任何使用健康检查的模块使用；全局负载是指只能在智能 DNS 页面的全局负载模块使用。

**间隔**：健康检查发送状态探测包的间隔时间，单位为秒。

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

**超时时间**：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

**发送**：HTTP/HTTPS 报文中的发送内容。

**接收**：接收到报文中应含的内容。当接收到的内容不包含此内容时，状态为 DOWN。

**用户名**：HTTP/HTTPS 认证的用户名。

**密码**：HTTP/HTTPS 用户的密码。

**覆盖 IP 地址类型**：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

**覆盖 IP**：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机或链路时填写此项。

**覆盖端口**：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置。

**透明模式**：用于配置模板采用透明传输方式进行检查。选择透明模式，则以引用该模板的对象作为下一跳，去探测覆盖 IP，此时覆盖 IP 必须配置。

**探测延时**：计算使用该健康检查模板的对象的探测延迟时间。

**配置步骤：**

1. 根据需求选择应用范围使用**通用**或则**全局负载**
2. 输入**间隔**。
3. 输入**最大重试次数**。
4. 输入**超时时间**。
5. 选择输入**发送**内容。
6. 选择输入**接收**内容。
7. 选择输入**用户名。**
8. 选择输入**密码。**
9. 选择**覆盖 IP 地址类型**。
10. 选择输入**覆盖 IP 和覆盖端口**。
11. 勾选是否启用**透明模式**。
12. 点击**提交**。

当类型为 SNMP 时，配置界面如下：


**名称：**指定新建健康检查模板的名称。

**类型：**指定新建健康检查模板的协议类型。

**应用范围：**健康检查使用的范围。通用是指可以在系统任何使用健康检查的模块使用；全局负载是指只能在智能 DNS 页面的全局负载模块使用。

**间隔：**健康检查发送状态探测包的间隔时间，单位为秒。

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

**超时时间：**发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

**团体名:**SNMP 代理认证的密码。

**代理类型：**可以选择 UCD(linux)和 windows 两种类型。

**cpu 最大值：**cpu 使用率阈值，超过此值认为服务器不可用。

**cpu 权重：**cpu,内存，磁盘三者参与负载计算时所占的权重比例。

**内存最大值：**内存使用率阈值，超过此值认为服务器不可用。

**内存权重：**cpu,内存，磁盘三者参与负载计算时所占的权重比例。

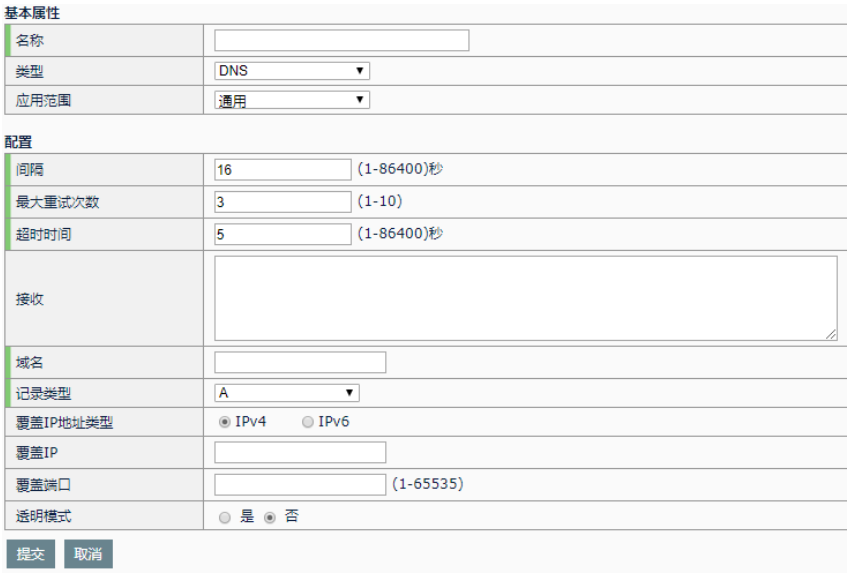
**磁盘最大值：**磁盘使用率阈值，超过此值认为服务器不可用。

**磁盘权重：** cpu,内存，磁盘三者参与负载计算时所占的权重比例。

**配置步骤：**

1. 根据需求选择应用范围使用**通用**或则**全局负载**
2. 输入**间隔**。
3. 输入**最大重试次数**。
4. 输入**超时时间**。
5. 输入**团体名。**
6. 选择**代理类型**。
7. 输入 **cpu 最大值**。
8. 输入 **cpu 权重**。
9. 输入**内存最大值**。
10. 输入**内存权重**。
11. 输入**磁盘最大值**。
12. 输入**磁盘权重**。
13. 点击**提交**。

当类型为 DNS 时，配置界面如下：




**名称：**指定新建健康检查模板的名称。

**类型：**指定新建健康检查模板的协议类型。

**应用范围：**健康检查使用的范围。通用是指可以在系统任何使用健康检查

的模块使用；全局负载是指只能在智能 DNS 页面的全局负载模块使用。

**间隔**：健康检查发送状态探测包的间隔时间，单位为秒。

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

**超时时间**：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

**接收**：接收到报文中应含的内容。当接收到的内容不包含此内容时，状态为 DOWN。

**域名**：去 DNS 服务器上解析的域名。

**记录类型**：指定域名请求的记录类型，默认是 A 记录

**覆盖 IP 地址类型**：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

**覆盖 IP**：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机或链路时填写此项。

**覆盖端口**：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置。

**配置步骤**：

1. 根据需求选择应用范围使用**通用**或则**全局负载**
2. 输入**间隔**。
3. 输入**最大重试次数**。
4. 输入**超时时间**。
5. 选择输入**接收**内容。
6. 输入**域名**。
7. 选择**记录类型**。
8. 选择**覆盖 IP 地址类型**。
9. 选择输入**覆盖 IP 和覆盖端口**。
10. 点击**提交**。

当类型为 RADIUS 时，配置界面如下：


**名称**：指定新建健康检查模板的名称。

**类型**：指定新建健康检查模板的协议类型。

**应用范围**：健康检查使用的范围。通用是指可以在系统任何使用健康检查的模块使用；全局负载是指只能在智能 DNS 页面的全局负载模块使用。

**间隔**：健康检查发送状态探测包的间隔时间，单位为秒。

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

**超时时间**：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

**用户名**：RADIUS 认证用户名称。

**密码**：RADIUS 用户密码。

**密钥**：和 RADIUS 服务器的协商密钥。

**覆盖 IP 地址类型**：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

**覆盖 IP**：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康检查方式的健康状况依赖于其他 IP 的主机或链路时填写此项。

**覆盖端口**：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置。

**配置步骤：**

1. 根据需求选择应用范围使用**通用**或则**全局负载**
2. 输入**间隔**。
3. 输入**最大重试次数**。
4. 输入**超时时间**。
5. 输入**用户名**。
6. 输入**密码**。
7. 输入**密钥**。
8. 选择**覆盖 IP 地址类型**。
9. 选择输入**覆盖 IP**。
10. 选择输入**覆盖端口**。
11. 点击**提交**。

当类型为 LDAP 时，配置界面如下：


**名称：**指定新建健康检查模板的名称。

**类型：**指定新建健康检查模板的协议类型。

**应用范围：**健康检查使用的范围。通用是指可以在系统任何使用健康检查的模块使用；全局负载是指只能在智能 DNS 页面的全局负载模块使用。

**间隔**：健康检查发送状态探测包的间隔时间，单位为秒。

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

**超时时间**：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

**用户名**：LDAP 用户名称。

**密码**：LDAP 用户密码。

**覆盖 IP 地址类型**：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

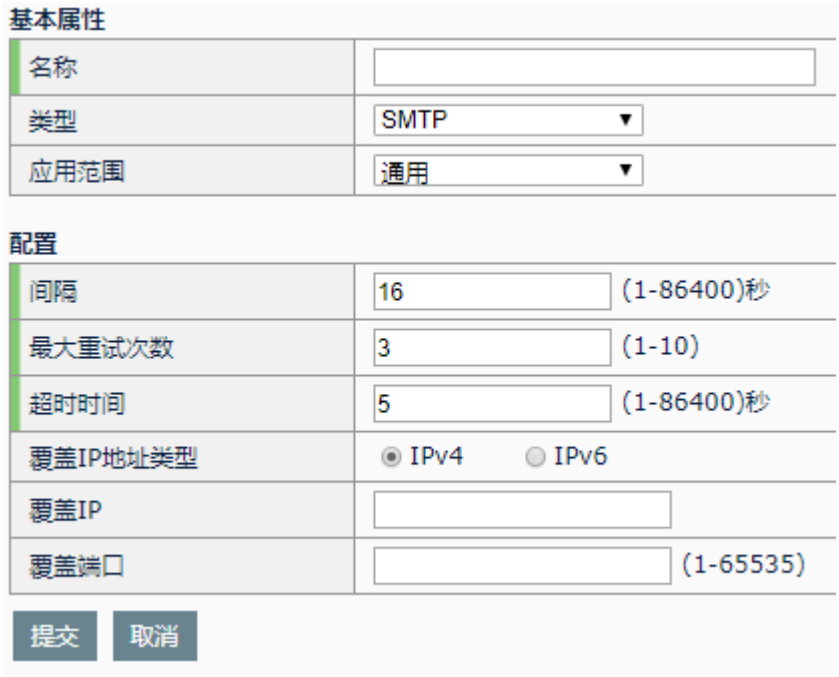
**覆盖 IP**：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机或链路时填写此项。

**覆盖端口**：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置。

**配置步骤：**

1. 根据需求选择应用范围使用**通用**或则**全局负载**
2. 输入**间隔**。
3. 输入**最大重试次数**。
4. 输入**超时时间**。
5. 输入**用户名**。
6. 输入**密码**。
7. 选择**覆盖 IP 地址类型**。
8. 选择输入**覆盖 IP**。
9. 选择输入**覆盖端口**。
10. 点击**提交**。

当类型为 SMTP 时，配置界面如下：




**名称**：指定新建健康检查模板的名称。

**类型**：指定新建健康检查模板的协议类型。

**应用范围**：健康检查使用的范围。通用是指可以在系统任何使用健康检查的模块使用；全局负载是指只能在智能 DNS 页面的全局负载模块使用。

**间隔**：健康检查发送状态探测包的间隔时间，单位为秒。

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

**超时时间**：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

**覆盖 IP 地址类型**：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

**覆盖 IP**：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机或链路时填写此项。

**覆盖端口**：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置。

**配置步骤：**

1. 根据需求选择应用范围使用**通用**或则**全局负载**
2. 输入**间隔**。
3. 输入**最大重试次数**。
4. 输入**超时时间**。

5. 选择**覆盖 IP 地址类型**。
6. 选择输入**覆盖 IP**。
7. 选择输入**覆盖端口**。
8. 点击**提交**。

当类型为 POP3 时，配置界面如下：


**名称**：指定新建健康检查模板的名称。

**类型**：指定新建健康检查模板的协议类型。

**应用范围**：健康检查使用的范围。通用是指可以在系统任何使用健康检查的模块使用；全局负载是指只能在智能 DNS 页面的全局负载模块使用。

**间隔**：健康检查发送状态探测包的间隔时间，单位为秒。

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

**超时时间**：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

**用户名**：POP3 用户名。

**密码**： POP3 用户密码。

**覆盖 IP 地址类型**：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

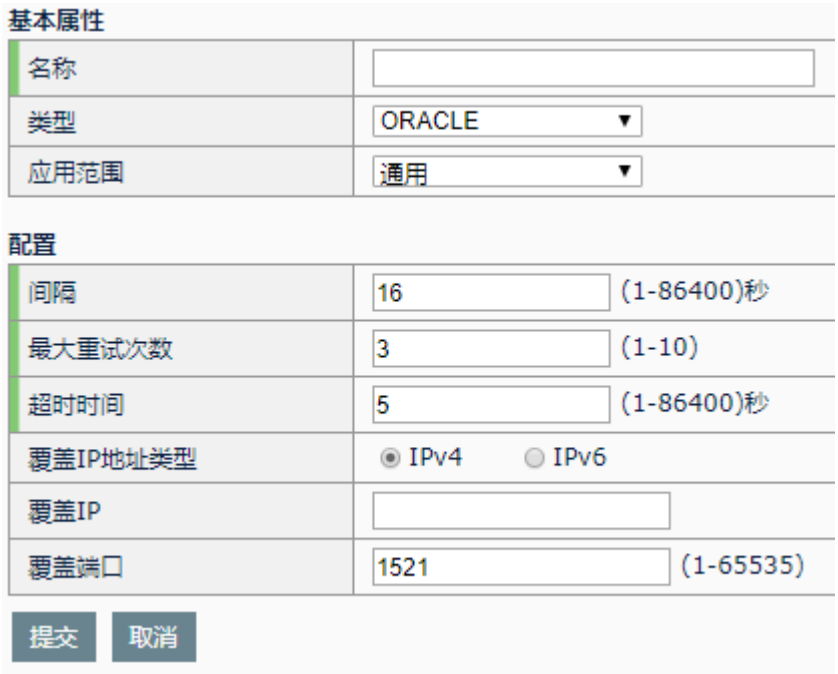
**覆盖 IP**：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机或链路时填写此项。

**覆盖端口**：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置。

**配置步骤：**

1. 根据需求选择应用范围使用**通用**或则**全局负载**
2. 输入**间隔**。
3. 输入**最大重试次数**。
4. 输入**超时时间**。
5. 选择输入**用户名**。
6. 选择输入**密码**。
7. 选择**覆盖 IP 地址类型**。
8. 选择输入**覆盖 IP**。
9. 选择输入**覆盖端口**。
10. 点击**提交**。

当类型为 ORACLE 时，配置界面如下：




**名称**：指定新建健康检查模板的名称。

**类型**：指定新建健康检查模板的协议类型。

**应用范围**：健康检查使用的范围。通用是指可以在系统任何使用健康检查的模块使用；全局负载是指只能在智能 DNS 页面的全局负载模块使用。

**间隔**：健康检查发送状态探测包的间隔时间，单位为秒。

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

**超时时间**：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

**覆盖 IP 地址类型**：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

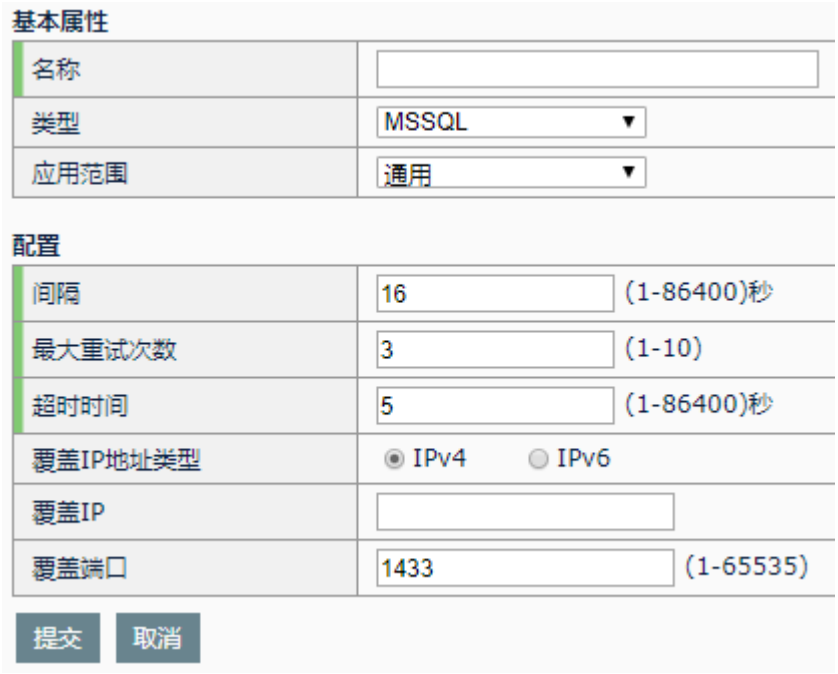
**覆盖 IP**：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机或链路时填写此项。

**覆盖端口**：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置，默认端口 1521。

**配置步骤**：

1. 根据需求选择应用范围使用**通用**或则**全局负载**
2. 输入**间隔**。
3. 输入**最大重试次数**。
4. 输入**超时时间**。
5. 选择**覆盖 IP 地址类型**。
6. 选择输入**覆盖 IP**。
7. 点击**提交**。

当类型为 MSSQL 时，配置界面如下：




**名称**：指定新建健康检查模板的名称。

**类型**：指定新建健康检查模板的协议类型。

**应用范围**：健康检查使用的范围。通用是指可以在系统任何使用健康检查的模块使用；全局负载是指只能在智能 DNS 页面的全局负载模块使用。

**间隔**：健康检查发送状态探测包的间隔时间，单位为秒。

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

**超时时间**：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

**覆盖 IP 地址类型**：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

**覆盖 IP**：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机或链路时填写此项。

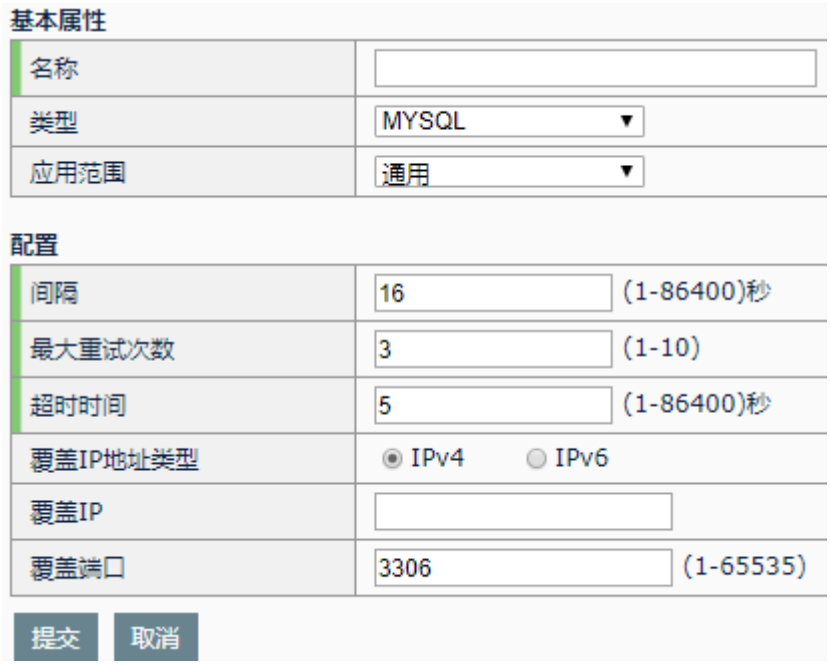
**覆盖端口**：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置，默认端口 1433。

**配置步骤：**

1. 根据需求选择应用范围使用**通用**或则**全局负载**
2. 输入**间隔**。
3. 输入**最大重试次数**。
4. 输入**超时时间**。

5. 选择**覆盖 IP 地址类型**。
6. 选择输入**覆盖 IP**。
7. 点击**提交**。

当类型为 MYSQL 时，配置界面如下：




**名称**：指定新建健康检查模板的名称。

**类型**：指定新建健康检查模板的协议类型。

**应用范围**：健康检查使用的范围。通用是指可以在系统任何使用健康检查的模块使用；全局负载是指只能在智能 DNS 页面的全局负载模块使用。

**间隔**：健康检查发送状态探测包的间隔时间，单位为秒。

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

**超时时间**：发送的健康检查探测包在此时间内如果没收到回应包，则此次健康检查探测失败，单位为秒。

**覆盖 IP 地址类型**：选择覆盖 IP 的地址类型，IPv4 或 IPv6。

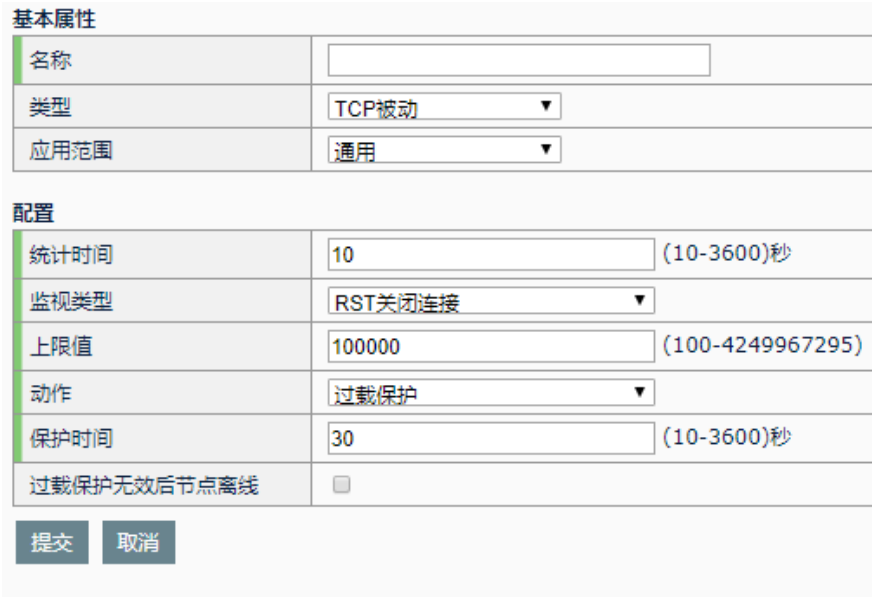
**覆盖 IP**：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机或链路时填写此项。

**覆盖端口**：用于配置模板检查真实去探测的端口。当引用对象的健康状况依赖于其他端口时填写此项，此时覆盖 IP 必须配置，默认端口 3306。

**配置步骤**：

1. 根据需求选择应用范围使用**通用**或则**全局负载**
2. 输入**间隔**。
3. 输入**最大重试次数**。
4. 输入**超时时间**。
5. 选择**覆盖 IP 地址类型**。
6. 选择输入**覆盖 IP**。
7. 点击**提交**。

当类型为 TCP 被动时，配置界面如下：




**名称**：指定新建健康检查模板的名称。

**类型**：指定新建健康检查模板的协议类型。

**应用范围**：健康检查使用的范围。通用是指可以在系统任何使用健康检查的模块使用；全局负载是指只能在智能 DNS 页面的全局负载模块使用。

**统计时间**：收集服务器 TCP 响应的时间，单位为秒，默认 10 秒。

**监视类型**：监视服务器 TCP 响应的类型，分为 RST 关闭连接和零窗口报文。

**上限值**：统计时间内，收集到服务器发送的 RST 关闭连接或零窗口报文的上限值，默认为 100000。一旦统计值超过上限值，认为该服务器进入过载状态，需要进行过载保护。

**动作**：服务器过载后，对其进行的保护动作，分为过载保护和离线两种。如果采取过载保护动作，那么只会对该服务器进行会话保持和连接保持；如果采取离线动作，那么只会对该服务器进行连接保持。两种情况下服务器都不再参与调度。

**保护时间**：对服务器进行保护的时间，单位为秒，默认 30 秒。

**过载保护无效后节点离线：**如果对服务器进行过载保护动作超过保护之间之后，服务器依然超载，将对服务器进行离线动作。

**配置步骤：**

1. 根据需求选择应用范围使用**通用**或则**全局负载**
2. 输入**统计时间**。
3. 输入**监视类型**。
4. 输入**上限值**。
5. 输入**动作**。
6. 输入**保护时间**。
7. 勾选**过载保护无效后节点离线**。
8. 点击**提交**。

当类型为 PACKET LOSS RATE 时，配置界面如下：


**名称：**指定新建健康检查模板的名称。

**类型：**指定新建健康检查模板的协议类型。

**应用范围：**健康检查使用的范围。通用是指可以在系统任何使用健康检查的模块使用；全局负载是指只能在智能 DNS 页面的全局负载模块使用。

**周期发包数：**每个测试周期发送数据包的个数。

**间隔：**健康检查发送状态探测包的间隔时间，单位为秒。

**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，则此数

据包被认为探测失败，单位为秒。

**阈值**：丢包百分比高于此值将认为检查失败。

**覆盖 IP**：用于配置模板检查真实去探测的 IP 地址。当引用对象的健康状况依赖于其他 IP 的主机或链路时填写此项。

透明模式：

**配置步骤：**

1. 根据需求选择应用范围使用**通用**或则**全局负载**
2. 输入**周期发包数**。
3. 输入**间隔**。
4. 输入**超时时间**。
5. 输入**阈值**。
6. 选择输入**覆盖 IP**。
7. 根据需求判断是否开启**透明模式**。
8. 点击**提交**。

## 16.3 配置默认健康检查

默认健康检查模板由**服务器节点**或者**链路节点**引用，将一些通用的健康检查模板加入到默认健康检查列表中，使用户更加容易配置。默认健康检查模板中支持的健康检查协议类型只有 ICMP 和 SNMP 两种。

进入**模板和对象>健康检查>默认健康检查**：

**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。

**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**。

## 16.4 配置案例

**案例描述**：

新建一个 ICMP 类型的健康检查模板，然后在服务池中引用此模板，对服务池的成员进行探测，返回探测结果显示。

**配置步骤**：

1. 新建 ICMP 类型的模板：


2. 新建服务池并新建两个成员，在服务池中引用此模板：


3. 服务池中的成员继承服务池的健康检查，然后对成员进行检查，并返回结果：

如上图所示：

| 状态 | 服务成员 |
| --- | --- |
| ● | 123.123.123.1 |
| ◆ | 192.168.1.1 |

成员 1,123.123.123.1 存在并且能 ping 通，所以返回检查成功。

成员 2,192.168.1.1 是一个不存在的地址，所以返回检查失败。

# 17 第17章 TRule

## 17.1 TRule自动化脚本概述

TRule 是一种强大的，可编程的智能脚本，TRule 在标准的工具命令语言（Tcl）上进行扩展，可以通过 TRule 编程来控制系统的各个模块和处理环节，最大限度的实现业务的精细化控制和个性化需求，从容应对应用系统的频繁升级和调整。借助 TRule 引擎，可以对某些数据流进行复杂的逻辑判断后，再决定后续的处理，实现图形配置界面上所无法完成的定制策略。例如：动态结合客户端的网络延迟状况，浏览器类型，访问对象等多种因素来决定是否对其进行数据压缩或其他操作。

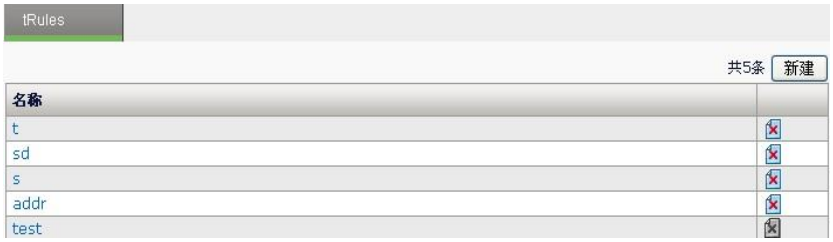
TRule 脚本的语法基于工具命令语言（Tcl）编程标准，有关标准 Tcl 语法的信息，请参阅以下网址：http://www.tcl.tk/man/tcl8.5/tutorial/tcltutorial.html。TRule 脚本包含了如下基本元素：事件声明；运算符；TRule 命令。系统中预定义了一组事件，TRule 脚本中可以引用这些事件，当此事件在系统中发生后即会执行与该事件所关联的 TRule 脚本段。TRule 中不但可以使用众多标准的 Tcl 命令，而且可以使用 TRule 提供的一组扩展命令来实现强大灵活的功能。

## 17.2 配置TRule

TRule 脚本只有在虚拟服务中引用后才能生效。

**配置步骤：**

1. 进入**模板和对象>tRules**，如下图所示：




2. 点击**新建**，如下图所示：


**TRule 配置参数说明：**

**名称**：TRule 脚本名称，最多输入 31 个英文字符，15 个中文字符。

**内容**：输入 TRule 脚本内容，最多输入 2008 个英文字符。

3. 点击**提交**，保存配置；点击  ，删除一个脚本，如果删除按钮变灰，表示当前脚本被其他虚拟服务引用，此时不可删除；点击脚本名称可以查看并编辑该脚本内容。

## 17.3 TRule语法及命令

1. TRule 脚本语法

#注释

when 事件名称 E {

Tcl 内置命令或扩展命令 1

Tcl 内置命令或扩展命令 2

.....

Tcl 内置命令或扩展命令 N

}

一个 TRule 脚本是由多个上述脚本段组成的，每个脚本段的格式都要符合上述格式，即首先是关键字 when，然后是事件名称，最后是被大括号括起来的脚本体，脚本体中可以使用 TCL 内置的命令也可以使用 TRule 支持的扩展命令。该脚本段的含义：当事件 E 发生时依次执行命令 1 到 N。

注意

1.花括号'{'必须跟在事件名称后并以空格分隔,不能另起一行书写。

2.事件名称只能使用 TRule 支持的事件，其他事件是不合法的。

3.每个脚本中不允许有重复事件名称。

4.注释语句以'#'开头。

如下是一段格式正确的脚本：

```
sd
when HTTP_REQUEST {
  # Don't allow data to be chunked
  if { [HTTP::version] eq "1.1" } {
      if { [HTTP::header is_keepalive] } {
         HTTP::header replace "Connection" "Keep-Alive"
      }
      HTTP::version "1.0"
   }
}

when HTTP_RESPONSE {
  if { [HTTP::header "Content-Type"] starts_with "text/" } {
      set content_length 4294967295
  }
}
```

TRule 的触发是基于事件的，当满足事件的定义时则表明该事件发生了，此时系统就会执行该事件所对应的脚本体，比如当虚拟服务收到一个 HTTP 请求并且协议解析完毕，此时就会触发 HTTP_REQUEST 事件并执行对应的脚本体。

2. TRule 支持的事件

| 事件名称 | 含义 |
|---|---|
| RULE_INIT | 创建一个包含 RULE_INIT 声明的脚本并下发时该事件触发，该事件只会在第一次下发时触发，通常用来初始化全局变量。 |
| CLIENT_ACCEPTED | 与客户端完成三次握手 |
| CLIENT_DATA | 接收到客户端数据 |
| HTTP_REQUEST | HTTP 请求报文头部解析完成 |
| HTTP_RESPONSE | HTTP 响应报文头部解析完成 |
| HTTP_CLASS_FAILED | 当前定义了至少一个 HTTP class（内容交换），且所有的 HTTP class（内容交换）都没有匹配上 |
| HTTP_CLASS_SELECTED | 当前选择了一个 HTTP class |

虚拟服务引用的 TRule 脚本中如果包含 HTTP_REQUEST 事件，则该虚拟服务必须引用 HTTP Profile。

1. TRule 支持的扩展命令

| 指令 | 支持的事件 | 描述 |
|---|---|---|
| HTTP::class | HTTP_CLASS_SELECTED | 返回匹配上的 class 的名称，若未匹配上，返回空 |
| HTTP::class [enable\|disable] | | 启用或不启用 HTTP class 匹配 |
| HTTP::class select <name> | | 从设备上存在的 class 中强制选中一个 class |
| HTTP::close | HTTP_REQUEST, HTTP_RESPONSE | 关闭当前的 HTTP 连接。发送 rst |
| HTTP::cookie names | | 返回包含的所有 cookie 名 |
| HTTP::cookie count | | Header 中 cookie 的数量 |
| HTTP::cookie name <name> [<string>] | | 设置、获取给定名称的 cookie（必须存在）的值。 |
| HTTP::cookie version <name> [version] | | 设置、获取 cookie 的版本<br>Request 时，version 对应的是整个 cookie 头域，跟 name 无关 |
| HTTP::cookie path <name> [path] | | 设置、获取 cookie 的 path |
| HTTP::cookie domain <name> [domain] | | 设置、获取 cookie 的 domain |
| HTTP::cookie ports <name> | | 设置、获取版本 |

| | | |
|---|---|---|
| [portlist] | | 2 cookie 的 port 列表 |
| HTTP::cookie insert name <name> value <value> [path <path>] [domain <domain>] [version <0 \| 1 \| 2>] | | 向 request 或 Set-Cookie response 的 Cookie 头中加入一个 cookie。默认版本为 0。<br>如果 cookie 已存在，还会再插入一个<br>若 Request 中存在 cookie 头域，则这里设置 version 无效。因为 request 的版本是针对整个 cookie 头域，所以就不去修改原有 cookie 的 version |
| HTTP::cookie remove <name> | | 移除 cookie |
| HTTP::cookie sanitize [attribute]+ | | 保留指定的 cookie。如果未指定，不做处理 |
| HTTP::cookie exists <name> | | 存在则返回 true |
| HTTP::cookie maxage <name> [seconds] | | 设置、获取 maxage。<br>适用于版本 1、2，以及 response 中 |
| HTTP::cookie expires <name>[seconds] [absolute \| relative] | | 设置、获取 expire。仅适用于版本 0。<br>如果指定了 absolute，seconds 就表示从 UNIX epoch |

| | | |
|---|---|---|
| | | (January 1, 1970)的秒数。Seconds 的默认值为 relative，从设备当前时间算起。<br>仅应用于 response |
| HTTP::cookie comment <name> [comment] | | 设置、获取 comment。<br>仅适用于版本 1、2，仅应用于 response |
| HTTP::cookie secure <name> [enable\|disable] | | 设置、获取 secure。仅应用于 response。<br>返回的是 true 或 false，取决于是否设置了 secure。如果 HTTP::cookie secure <name> enable 用在一个设置了 secure 的 cookie 上，就不会对该 cookie 做改动。 |
| HTTP::cookie commenturl <name> [commenturl] | | 设置、获取 comment url。仅适用于版本 2<br>应用于 response |
| HTTP::cookie encrypt <name><pass phrase> ["128" \| "192" \| "256"] | | 用 pass phrase 生成的 key 加密指定名称的 cookie。默认 key 长度为 128。加密算法为 AES |
| HTTP::cookie decrypt <name><pass phrase> ["128" \| "192" \| "256"] | | 用 pass phrase 生成的 key 解密指定名称的 |

| | | |
|---|---|---|
| | | cookie。默认 key 长度为 128。加密算法为 AES |
| HTTP::cookie httponly <name> [enable\|disable] | | 类似于 secure<br>仅应用于 response。 |
| HTTP::cookie discard <name> [enable\|disable] | | 类似于 secure<br>只适用于版本 2<br>仅应用于 response。 |
| HTTP::header name <name> | HTTP_REQUEST, HTTP_RESPONSE, | 返回 header 为 name 的值<br>如果该 name 对应多个头，只应用于第一个 header 的值 |
| HTTP::header values <name> | | 返回 name 头的值，可能多个值。如果有多个该 name 的头，返回所有的值。 |
| HTTP::header names | | 返回所有头的列表<br>相同 name 的头，将会列出多次 |
| HTTP::header count [name] | | 返回 header 的数量。如果指定了 name，返回该 name 的数量<br>相同 name 的头，算多次 |
| HTTP::header at <index> | | 返回从 0 开始的 index 对应的头 |
| HTTP::header exists <name> | | request 或 response 中存在 name 的头，返回 true |
| HTTP::header insert ["lws"] | | 在 request 或 |

| | | |
|---|---|---|
| [<name><value>]+<br>Lws 是 http profile 里面配置的 | | response 的尾部，插入一个或多个头域。<br>如果指定了 lws，长的值中将添加 lws |
| HTTP::header lws | | 判断头域中是否分行<br>未测，直接使用的协议变量 |
| HTTP::header is_keepalive | | 等同于 HTTP::is_keepalive |
| HTTP::header is_redirect | | 等同于 HTTP::is_redirect |
| HTTP::header replace <name> [<string>] | | 用 string 替换最先出现的 name 头域的值。如果头不存在，执行插入操作。 |
| HTTP::header remove <name> | | 移除该名称的所有头 |
| HTTP::header insert_modssl_fields [addr] [service \| port] | | 若指定了 addr port，插入头 ClientIPAddress，值为 client IP、port<br>若指定了 addr，插入头 ClientIPAddress，值仅为 client IP<br>若指定了 addr service，插入头 ClientTCPService，值为 client port<br>仅用于 request，不能用于 |

| | | |
|---|---|---|
| | | response |
| HTTP::header sanitize [header name]+ | | 移除所有的头，除了指定的和下面的：<br>Connection, Content-Encoding, Content-Length, Content-Type,<br>Set-Cookie,<br>Set-Cookie2,<br>Transfer-Encoding.<br>如果在 server-side 使用，应考虑增加 Location 到保留的 header 中<br>如果在 client-side 使用，应考虑增加 Cookie, Accept、Accept-Encoding 到保留的 header 中 |
| HTTP::host | HTTP_REQUEST | 返回当前请求的 host 值，如果端口号非标准，需要同时返回端口号 |
| HTTP::is_keepalive | HTTP_REQUEST, HTTP_RESPONSE, | 当前 HTTP 连接是否为 keepalive，返回 1、0 |
| HTTP::is_redirect | HTTP_RESPONSE, | 当前 HTTP 响应连接是否为重定向响应。返回 1、0<br>300 和 304 不认为是重定向<br>其余状态码如： |

| | | |
|---|---|---|
| | | * 301 (Moved Permanently)<br>* 302 (Found)<br>* 303 (See Other)<br>* 305 (Use Proxy)<br>*307(Temporary Redirect)认为是重定向报文 |
| HTTP::method | HTTP_REQUEST | 返回当前 HTTP 请求的方法 |
| HTTP::path [<string>] | HTTP_REQUEST, | 返回或改写 uri 中的 path |
| HTTP::query | HTTP_REQUEST, | 返回 HTTP 的 query 字段 |
| HTTP::redirect <url> | HTTP_CLASS_SELECTED, HTTP_CLASS_FAILED, HTTP_REQUEST, HTTP_RESPONSE, | 给客户端返回一个 302 重定向的响应。后续不能执行任何改写 respond 头部的命令 |
| HTTP::request | HTTP_REQUEST, | 返回报文中的 HTTP 请求头部 |
| HTTP::request_num | HTTP_REQUEST, HTTP_RESPONSE, , | 返回当前的 HTTP 连接已经进行了多少次请求 |
| HTTP::respond <status code> [content <content Value>] [noserver] [<Header name><Header Value>]+ | HTTP_REQUEST, HTTP_RESPONSE, | 给客户端返回一个自定义的响应，如果发生在请求阶段，可以直接发送返回；如果发生在响应阶段，丢弃服务器的真实响应，换成这个自定义的响应。<br>默认只有 |

| | | |
|---|---|---|
| | | “Content-Length”头域，配置时不应添加该头域，其余需要的头域要手动添加 |
| HTTP::status | HTTP_RESPONSE, | 返回响应的状态码 |
| HTTP::uri<br>HTTP::uri <string> | HTTP_CLASS_SELECTED,<br>HTTP_CLASS_FAILED,<br>HTTP_REQUEST, | 返回或改写当前 request 的 uri |
| HTTP::version ["1.0"\|"1.1"]<br>不支持 0.9 | HTTP_REQUEST,<br>HTTP_RESPONSE,<br>, | 返回或设置 http 版本 |
| IP::client_addr | HTTP_CLASS_FAILED,<br>HTTP_CLASS_SELECTED,<br>HTTP_REQUEST,<br>HTTP_RESPONSE,<br>CLIENT_ACCEPTED | 返回连接到设备的客户端 ip |
| IP::local_addr | HTTP_REQUEST<br>HTTP_RESPONSE | Client 侧，应该<br>返回 vs 的 ip ；<br>Server 侧，返回<br>本地 ip |
| IP::addr<addr1>[/<mask>] equals<br><addr2>[/<mask>] | HTTP_CLASS_FAILED,<br>HTTP_CLASS_SELECTED,<br>HTTP_REQUEST,<br>HTTP_RESPONSE,<br>CLIENT_ACCEPTED | 比较（子网/IP）和（子网/IP）是否相等，或者判断某一个 IP 地址是否属于某子网 |
| IP::local_addr | HTTP_REQUEST,HT | Client 侧，应该 |

| | | |
|---|---|---|
| | TP_RESPONSE | 返回 vs 的 ip,Server 侧,返回本地 ip(主动发起连接的那个) |
| IP::remote_addr | HTTP_REQUEST,HTTP_RESPONSE | Client 侧，为 client ip,Server 侧,为 member ip |
| TCP::payload [size] | CLIENT_DATA | 获取 tcp 的 payload；size，表示只收集收集 size 个字节 |
| TCP::payload length | | 获取 tcp payload 的长度 |
| TCP::payload offset <off> [size] | | 从 payload 起始位置偏移 off 个字节开始收集。<br>若配置 size，则收集 size 个字节 |
| TCP::client_port | HTTP_CLASS_FAILED, HTTP_CLASS_SELECTED, HTTP_REQUEST, HTTP_RESPONSE | 返回连接的 client 的端口 |
| pool <pool_name> | HTTP_CLASS_SELECTED, HTTP_REQUEST | 选定服务池 |
| pool <pool_name> [member <addr> [<port>]] | | 选定服务池中的成员 |
| persist none | HTTP_REQUEST: | 把会话保持设为无效 |
| persist add uie <key> [timeout] | HTTP_RESPONSE | 向 uie 表中插入记录 |
| persist lookup uie <key> pool <pool_name> | HTTP_REQUEST<br>HTTP_RESPONSE<br>HTTP_CLASS_FAILED<br>HTTP_CLASS_SELECTED | 查询对应对应服务池中对应 key 的记录（当前 vs 下的记录） |
| persist delete uie <key> pool <pool_name> | HTTP_REQUEST | 删除对应对应服务池中对应 key |

| | | |
|---|---|---|
| | HTTP_RESPONSE<br>HTTP_CLASS_FAILED<br>HTTP_CLASS_SELECTED | 的记录（当前 vs 下的记录） |
| persist uie <key> [timeover] | HTTP_REQUEST | 用此 key 做会话保持 |

2. TRule 支持的扩展操作符

| 操作符 | 格式 | 含义 |
|---|---|---|
| equals | STR1 equals STR2 | 判断字符串 STR1 是否和字符串 STR2 相等，区分大小写。 |
| contains | STR1 contains STR2 | 判断字符串 STR1 是否包含字符串 STR2，区分大小写。 |
| ends_with | STR1 ends_with STR2 | 判断字符串 STR1 是否是以字符串 STR2 结尾，区分大小写。 |
| starts_with | STR1 starts_with STR2 | 判断字符串 STR1 是否是以字符串 STR2 开始，区分大小写。 |
| matches_regex | STR1 matches_regex STR2 | 判断字符串 STR1 是否能匹配上正则表达式 STR2。 |

3. TRule 中禁止使用的 Tcl 内置命令

| | | | | |
|---|---|---|---|---|
| after | auto_execok | auto_import | auto_load | auto_mkindex |
| auto_qualify | auto_reset | bgerror | cd | close |
| eof | exec | exit | fblocked | fconfigure |
| fcopy | file | fileevent | filename | flush |
| gets | glob | http | interp | load |
| memory | namespace | open | package | pid |

| | | | | |
|---|---|---|---|---|
| pkg::create | pkg_mkindex | proc | pwd | rename |
| seek | socket | source | tell | unknown |
| update | uplevel | upvar | vwait | |

## 17.4 配置案例

**修改重定向报文内容：**

在某些 ERP 系统中，基本上都不会使用 80 端口，比如 Oracle 使用 9080 等，而服务器经过 ADC 设备端口转化之后用户看到的端口是 80，这个时候，如果系统中有重定向的时候会有问题，由于 ADC 只是作四层的端口转化，七层不作修改，而重定向内容会放在 HTTP 包头中的 Location 中，默认情况下，重定向内容不变，这时候 ADC 只是开放了 80 端口，重定向后会访问 9080 端口，所以访问会被 ADC 拒绝，导致访问不通。

处理这个问题可以从服务器上把重定向信息修改，这样会很麻烦，并且开发人员在开发过程中调试很困难。

我们可以使用 ADC 设备处理这个问题，就是通过 TRule 来修改 HTTP 包头中的 Location 中的端口就可以了。

sample

```
when HTTP_RESPONSE {
     set location [HTTP::header "Location"]
     if { [HTTP::status] == 302 } {
          regsub -all {:9080} $location ":80" location
          HTTP::respond 302 Location $location
     }
}
```

# 18 第18章 CA 证书

## 18.1 证书概述

PKI（公钥基础设施）技术采用证书管理公钥，通过第三方的可信任机构--认证中心 CA(Certificate Authority)，把用户的公钥和用户的其他标识信息（如名称、e-mail、身份证号等）捆绑在一起，在 Internet 上验证用户的身份。目前，通用的办法是采用建立在 PKI 基础之上的数字证书，通过把要传输的数字信息进行加密和签名，保证信息传输的机密性、真实性、完整性和不可否认性，从而保证信息的安全传输。

设备上的 PKI 本地证书功能是：当设备作为 PKI 客户端时，选择本地证书作为本设备的身份标识，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。

## 18.2 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。

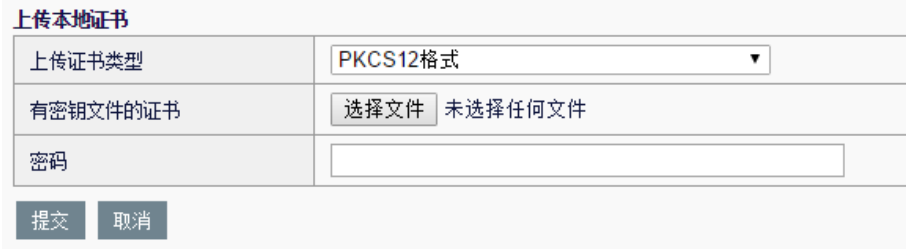
### 18.2.1 配置本地证书

**上传证书配置步骤**

1. 进入**模板和对象>CA 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、证书密钥分离和证书链三种。

**有密钥文件的证书：**PKCS12 格式文件的位置。

**密码：**数字证书的密码。


为保护私钥安全性，导入的 PKCS12 格式证书必须有密码保护。

导入证书密钥分离的证书。


**参数说明：**

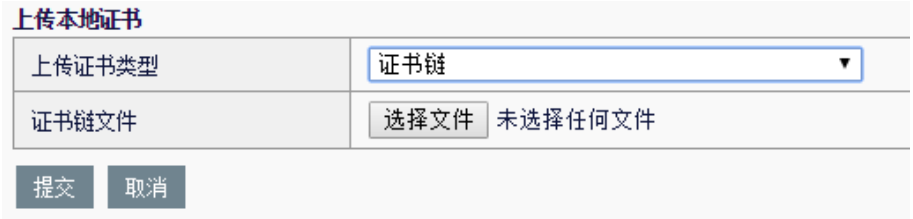
**上传证书类型：**可选择上传证书的类型，下拉菜单中可选项为 PKCS12 格式、证书密钥分离和证书链三种。

**证书文件：**数字证书文件位置。

**密钥文件：**数字证书私钥文件位置，可选择在本机自动匹配或者手动上传。

**密码：**数字证书的密码。

导入证书链。




**参数说明：**

**上传证书类型：**可选择上传证书的类型，下拉菜单中可选项为 PKCS12 格式、证书密钥分离和证书链三种。

**证书链文件：**证书链文件位置。

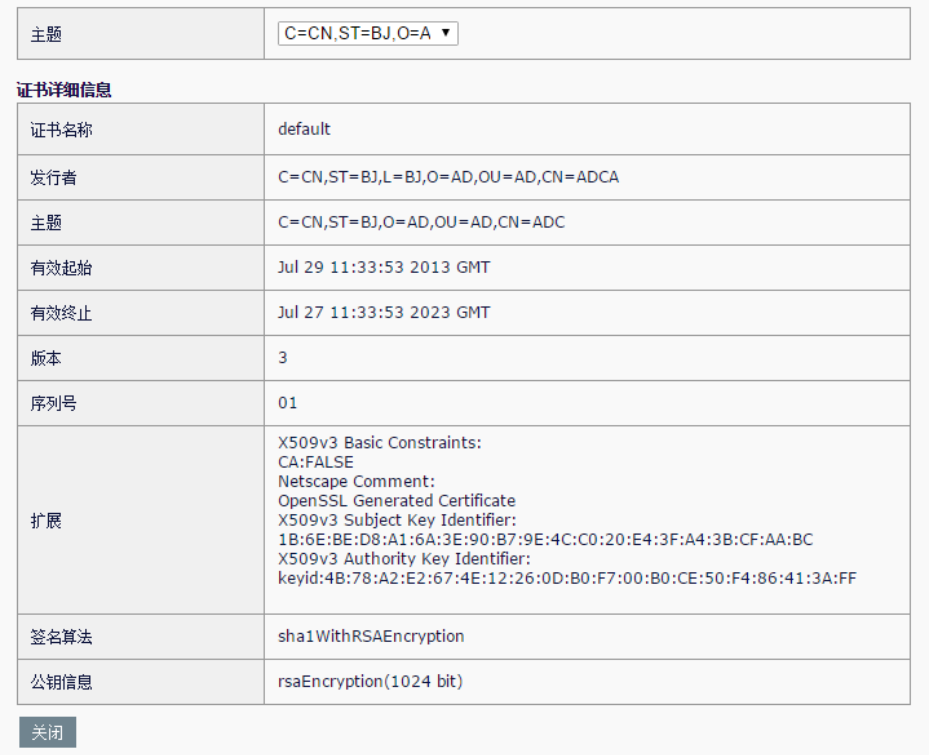
2. 点击**提交**。

**查看证书配置步骤**

1. 进入**模板和对象>CA 证书>本地证书**

该界面显示已导入的数字证书。


2. 点击 查看某一个证书的具体信息，显示证书详细信息。




**参数说明：**

**主题：**证书的主题列表，如果是证书链可以通过下拉框选择多个主题切换证书

**证书名称：**证书的名称

**发行者：**证书的发行者

**主题：**证书的主题

**有效起始：**证书生效的开始时间

**有效终止：**证书生效的终止时间

**版本：**证书的版本号

**序列号：**证书的序列号

**扩展：**证书的扩展信息

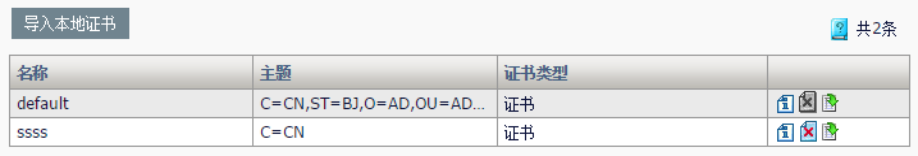
**签名算法：**证书的签名算法

**公钥信息：**证书的公钥信息

**导出证书配置步骤**

1. 进入**模板和对象>CA 证书>本地证书**

该界面显示全部导入的数字证书列表。




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

**删除证书配置步骤**

1. 进入**模板和对象>CA 证书>本地证书**

该界面显示已导入的数字证书。


2. 点击 删除某一个证书。

3. 点击**确认**删除证书。

提示

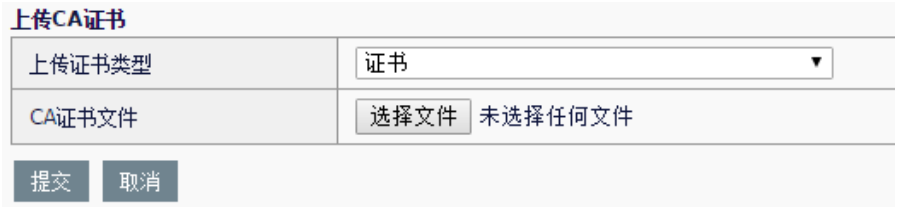
删除证书时出现 时表明证书正在被引用或者是默认证书，无法删除。

## 18.2.2 配置CA证书

**上传证书配置步骤**

1. 进入**模板和对象>CA 证书>CA**，点击**导入 CA 中心证书**，可以选择两种上传 CA 证书的方式。

导入单个 CA 证书




**参数说明：**

**上传证书类型：**选择上传 CA 证书的类型，分别为证书以及证书集合

**CA 证书文件：**要上传的 CA 证书文件位置

导入 CA 证书集合


**参数说明：**

**上传证书类型：**选择上传 CA 证书的类型，分别为证书以及证书集合

**CA 证书集合文件：**要上传的 CA 证书集合文件位置

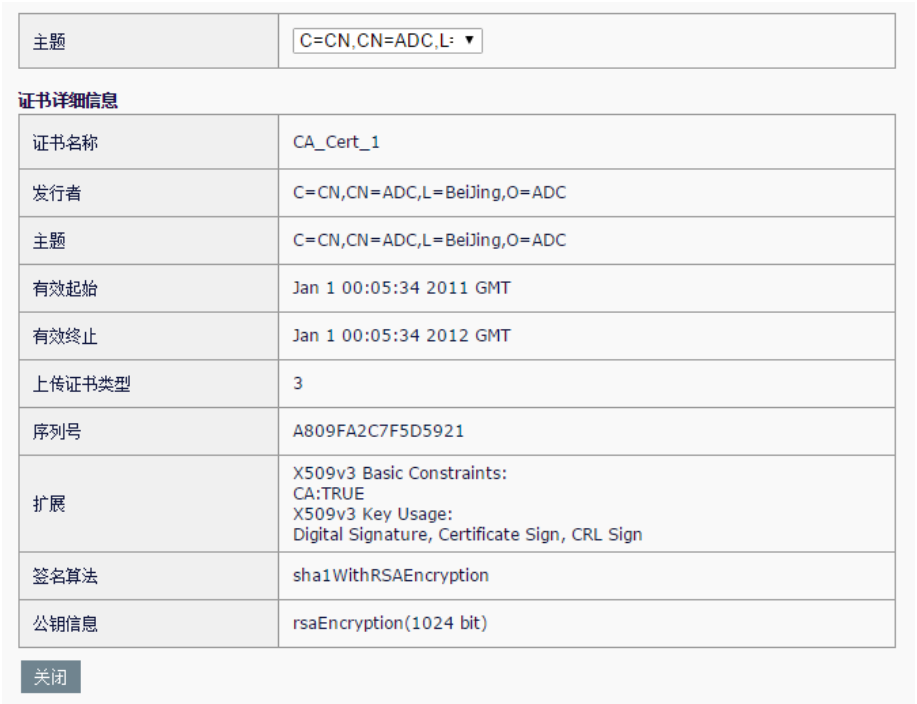
2. 点击**提交**

**查看证书配置步骤**

1. 进入**模板和对象>CA 证书>CA**

该界面显示已导入的 CA 证书。


2. 点击 查看某一个 CA 证书的具体信息，显示证书详细信息。



| 主题 | C=CN,CN=ADC,L= |
|---|---|

证书详细信息

| | |
|---|---|
| 证书名称 | CA_Cert_1 |
| 发行者 | C=CN,CN=ADC,L=BeiJing,O=ADC |
| 主题 | C=CN,CN=ADC,L=BeiJing,O=ADC |
| 有效起始 | Jan 1 00:05:34 2011 GMT |
| 有效终止 | Jan 1 00:05:34 2012 GMT |
| 上传证书类型 | 3 |
| 序列号 | A809FA2C7F5D5921 |
| 扩展 | X509v3 Basic Constraints:<br>CA:TRUE<br>X509v3 Key Usage:<br>Digital Signature, Certificate Sign, CRL Sign |
| 签名算法 | sha1WithRSAEncryption |
| 公钥信息 | rsaEncryption(1024 bit) |

关闭

**参数说明：**

**主题：**证书的主题列表，如果是 CA 证书集合可以通过下拉框在多个主题中选择一个主题来切换证书

**证书名称：**证书的名称

**发行者：**证书的发行者

**主题：**证书的主题

**有效起始：**证书生效的开始时间

**有效终止：**证书生效的终止时间

**版本：**证书的版本号

**序列号：**证书的序列号

**扩展：**证书的扩展信息

**签名算法：**证书的签名算法

**公钥信息：**证书的公钥信息

**导出证书配置步骤**

1. 进入**模板和对象>CA 证书>CA**

该界面显示已导入的 CA 证书。


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

**删除证书配置步骤**

1. 进入**模板和对象>CA 证书>CA**

该界面显示全部导入的 CA 证书。


2. 点击 删除某一个证书。

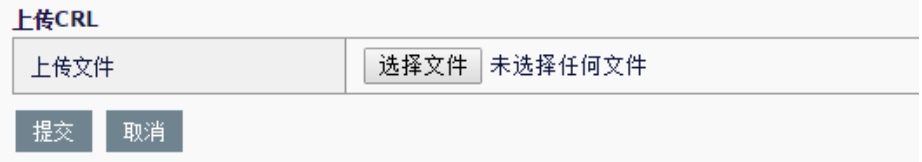
3. 点击**确认**删除证书。

提示 删除证书时出现 时表明证书正在被引用，无法删除。

### 18.2.3 配置CRL证书

**上传 CRL 配置步骤**

1. 进入**模板和对象>CA 证书>CRL**，点击**导入 CRL**。




**参数说明：**

**上传文件：**要上传的 CRL 证书文件位置

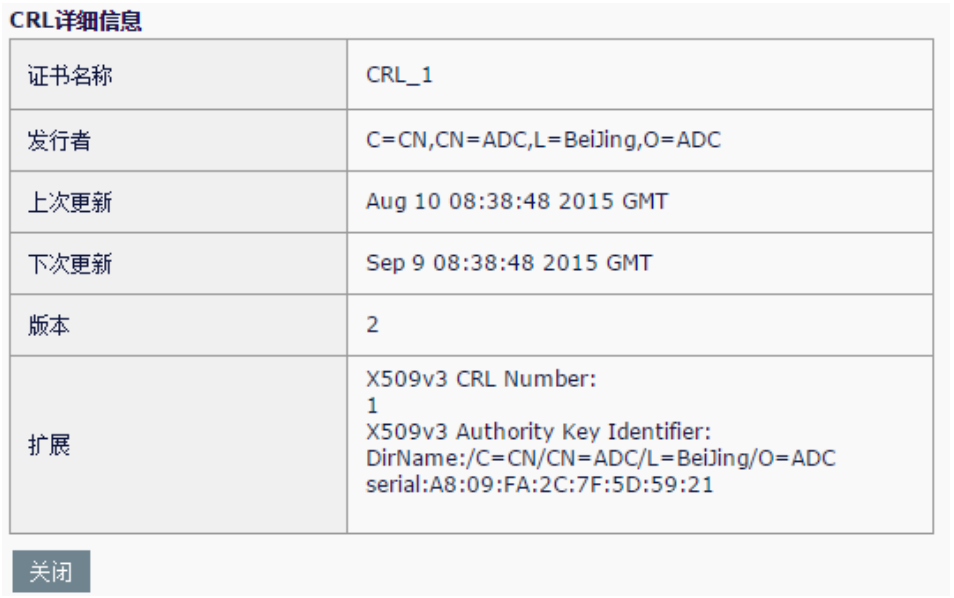
2. 点击**提交**。

**查看 CRL 配置步骤**

1. 进入**模板和对象>CA 证书>CRL**

该界面显示已导入的 CRL 证书。


2. 点击 查看某一个 CRL 证书的具体信息，显示证书详细信息。




**参数说明：**

**证书名称：**证书的名称

**发行者：**证书的发行者

**上次更新：**证书上次更新时间

**下次更新：**证书下次更新时间

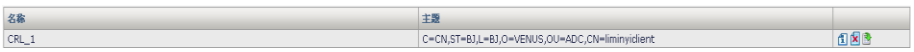
**版本：**证书的版本号

**扩展：**证书的扩展信息

**导出 CRL 配置步骤**

1. 进入**模板和对象>CA 证书>CRL**

该界面显示已导入的 CRL 证书。



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

**删除 CRL 配置步骤**

1. 进入**模板和对象>CA 证书>CRL**

该界面显示已导入的 CRL 证书。


2. 点击 删除某一个 CRL 证书。

3. 点击**确认**删除证书。

提示 删除证书时出现 时表明证书正在被引用，无法删除。

### 18.2.4 配置管理根CA配置

**生成根 CA 配置步骤**

1. 进入**模板和对象>CA 证书>根 CA 配置管理**

该界面显示根 CA 配置中心。


2. 点击 生成CA根证书，在弹出的窗口确认覆盖原 CA 根证书，进入 CA 证书请求界面。


**参数说明：**

**CN**：证书 common name 信息

**部门**：证书部门信息

**组织**：证书组织信息

**位置（城市）**：证书位置信息

**州/省**:证书州/省信息

**国家/地区**：证书国家/地区信息

**电子邮件**：证书电子邮件信息

**有效期**：设置证书有效期，范围 1 到 7300 天

**密钥大小**：设置证书密钥大小，可选 1024bit 和 2048bit 的证书

3. 点击**更新**按钮，生成根 CA 证书。

**导入根 CA 配置步骤**

1. 进入**模板和对象>CA 证书>根 CA 配置管理**

该界面显示根 CA 配置中心。


2. 点击 导入CA根证书， 在弹出的窗口确认覆盖原 CA 根证书，进入证书导入界面，导入方式分为 PKCS12 格式和证书密钥分离两种。

导入 PKCS12 格式根 CA 证书的界面。


**参数说明：**

**上传证书类型：**选择导入 CA 根证书的类型，可选择 PKCS12 格式和证书密钥分离两种。

**有密钥文件的证书：**点击选择证书文件存放的位置。

**密码：**配置证书文件的密码。

导入证书密钥分离格式根 CA 证书的界面。


**参数说明：**

**上传证书类型：**选择导入 CA 根证书的类型，可选择 PKCS12 格式和证书密钥分离两种。

**证书文件：**点击选择证书文件存放的位置。

**密钥文件：**点击选择密钥文件存放的位置。

**密码：**配置密钥文件的密码。

3. 点击**更新**按钮，完成根 CA 证书上传。

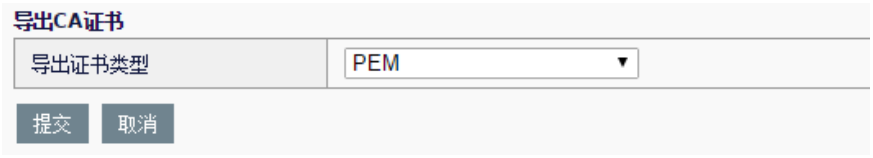
**导出根 CA 配置步骤**

1. 进入**模板和对象>CA 证书>根 CA 配置管理**

该界面显示根 CA 配置中心。


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

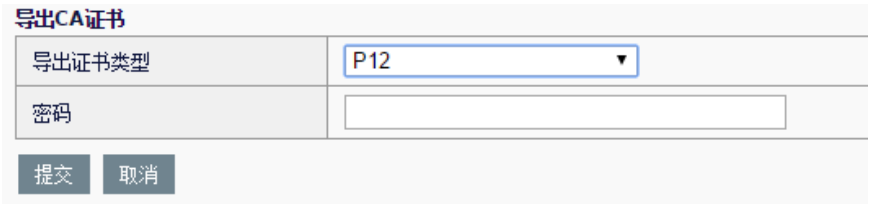
导出为 PEM 格式证书的界面。




**参数说明：**

**导出证书类型：**选择导出证书的类型，可选择 PEM 格式和 P12 格式两种

导出为 P12 格式证书的界面。




**参数说明：**

**导出证书类型：**选择导出证书的类型，可选择 PEM 格式和 P12 格式两种。

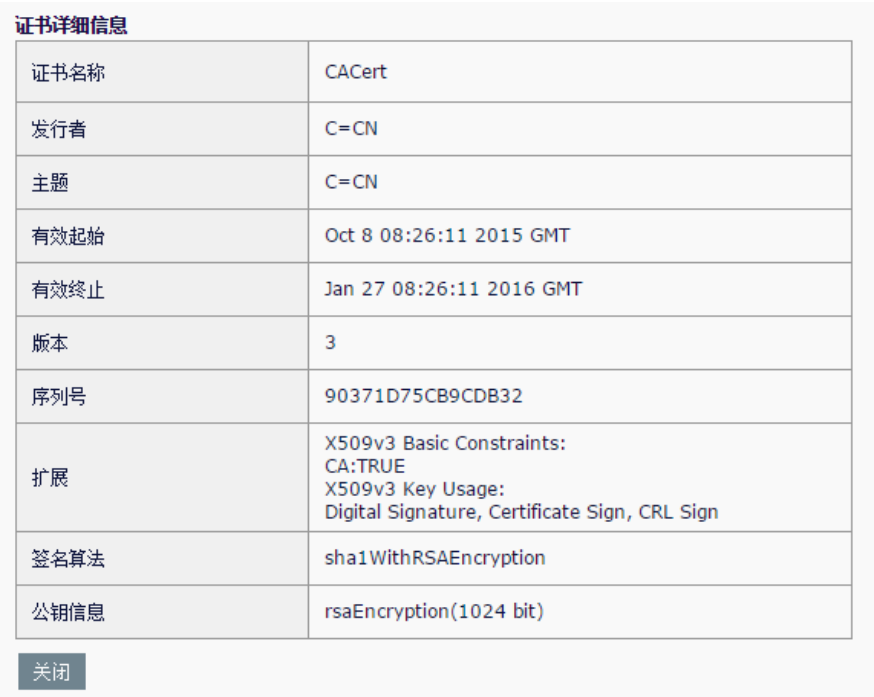
**密码：**设置导出后 P12 证书的密码。

**查看根 CA 配置步骤**

1. 进入**模板和对象>CA 证书>根 CA 配置管理**

该界面显示根 CA 配置中心。


2. 点击 查看CA根证书，查看 CA 根证书。



证书详细信息

| | |
|---|---|
| 证书名称 | CACert |
| 发行者 | C=CN |
| 主题 | C=CN |
| 有效起始 | Oct 8 08:26:11 2015 GMT |
| 有效终止 | Jan 27 08:26:11 2016 GMT |
| 版本 | 3 |
| 序列号 | 90371D75CB9CDB32 |
| 扩展 | X509v3 Basic Constraints:<br>CA:TRUE<br>X509v3 Key Usage:<br>Digital Signature, Certificate Sign, CRL Sign |
| 签名算法 | sha1WithRSAEncryption |
| 公钥信息 | rsaEncryption(1024 bit) |

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

**签名算法：**证书的签名算法

**公钥信息：**证书的公钥信息

**加载根 CA 证书到本机配置步骤**

1. 进入**模板和对象>CA 证书>根 CA 配置管理**

该界面显示根 CA 配置中心。


2. 点击 加载CA证书到本机，在弹出的窗口确认加载 CA 证书到本机。

**管理根 CA 的 CRL 配置步骤**

1. 进入**模板和对象>CA 证书>根 CA 配置管理**

该界面显示根 CA 配置中心。

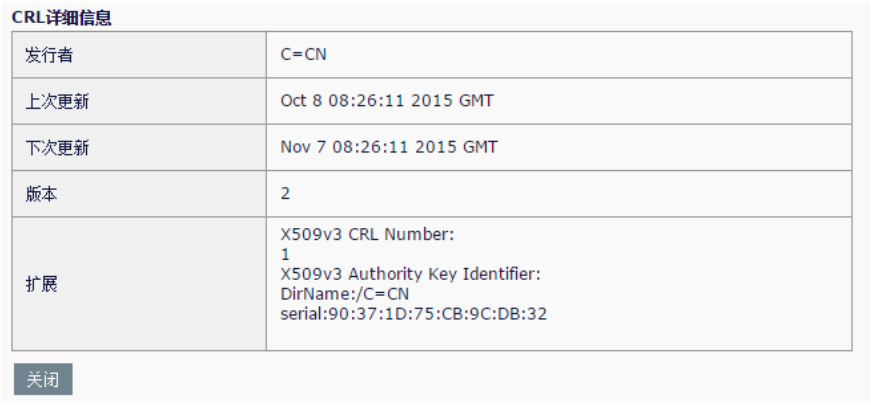

在 CRL 管理一栏，可以对 CRL 自动更新周期进行配置，CRL 周期配置范围为 1-30 天

**查看 CRL 详细信息配置步骤**

1. 进入**模板和对象>CA 证书>根 CA 配置管理。**

该界面显示根 CA 配置中心。


在 CRL 一栏，点击 查看 CRL 详细信息。




**参数说明：**

**发行者：**证书的发行者

**上次更新：**证书上次更新时间

**下次更新：**证书下次更新时间

**版本：**证书的版本号

**扩展：**证书的扩展信息

### 导出 CRL 配置步骤

1. 进入**模板和对象>CA 证书>根 CA 配置管理**

该界面显示根 CA 配置中心。


在 CRL 一栏，点击 导出 CRL 文件。

### 更新 CRL 配置步骤

1. 进入**模板和对象>CA 证书>根 CA 配置管理**

该界面显示根 CA 配置中心。

在 CRL 一栏，点击手动更新 CRL。

**加载 CRL 到本机配置步骤**

1. 进入**模板和对象>CA 证书>根 CA 配置管理**

该界面显示根 CA 配置中心。

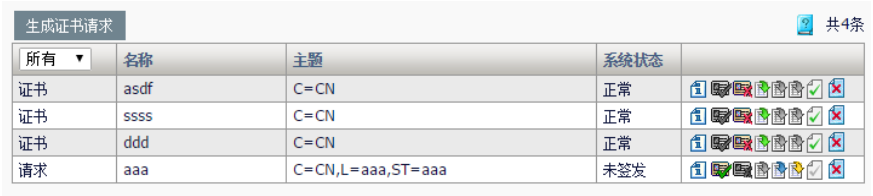

在 CRL 一栏，点击 加载 CRL 到本机。

## 18.2.5 配置管理用户证书

**生成用户证书请求步骤**

1. 进入**模板和对象>CA 证书>用户证书管理**

该界面显示用户证书列表。




2. 点击 生成证书请求，进入证书请求配置页面。


**参数说明：**

**证书名称**：配置证书的 CN 信息

**密码**：数字证书的密码

**确认密码**：数字证书的密码

**部门**：配置证书的部门信息

**组织**：配置证书的组织信息

**位置（城市）**：配置证书的位置信息

**州/省**：配置证书的州/省信息

**国家/地区**：配置证书的国家/地区信息

**通用名称（域名）**：证书通用名称（域名）

**电子邮件**：配置证书的电子邮件信息

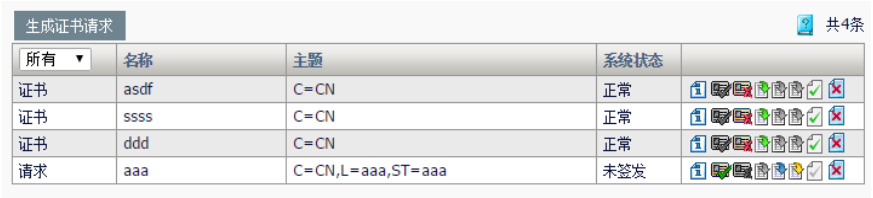
**密钥大小**：配置证书的密钥大小，可以选择 1024bit 或者 2048bit 的证书

3. 点击**更新**，生成证书请求。

**签发用户证书步骤**

1. 进入**模板和对象>CA 证书>用户证书管理**

该界面显示用户证书列表。

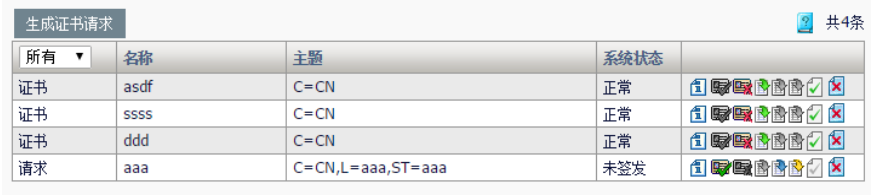



选择系统状态为未签发的用户证书请求，点击  图标对证书请求进行签发。

**吊销用户证书步骤**

1. 进入**模板和对象>CA 证书>用户证书管理**

该界面显示用户证书列表。




选择系统状态为正常的用户证书，点击  图标对证书进行吊销，进入证书吊销界面。


**参数说明：**

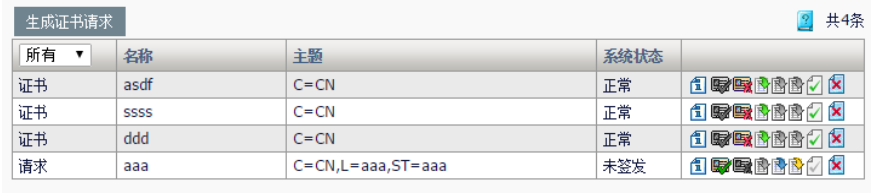
**撤销原因**：配置证书的吊销原因，可选择未指定、密钥泄露、CA 密钥泄露和附属关系改变四种。

2. 点击**提交**，完成对证书的吊销。

**删除用户证书步骤**

1. 进入**模板和对象>CA 证书>用户证书管理**

该界面显示用户证书列表。

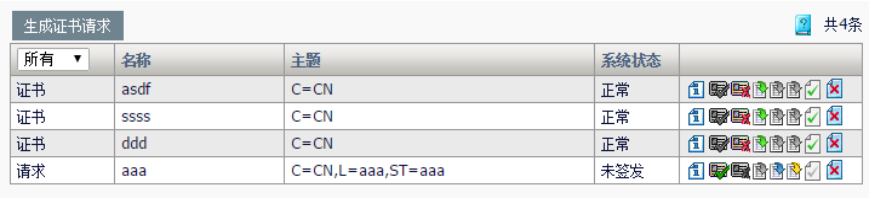


点击  图标删除证书或者证书请求。

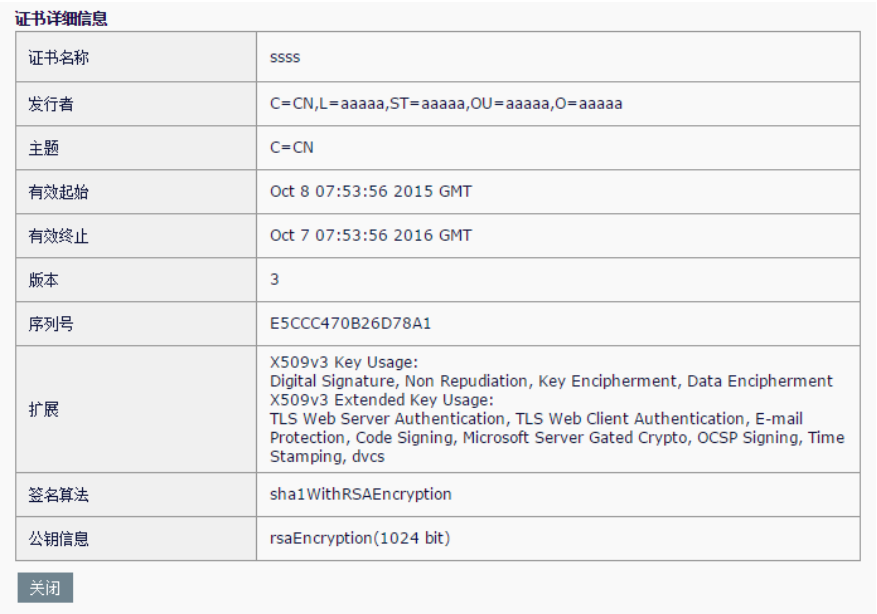
**查看用户证书信息步骤**

1. 进入**模板和对象>CA 证书>用户证书管理**

该界面显示用户证书列表。




点击  图标查看证书或者证书请求详细信息。




**参数说明：**

**证书名称：**证书的名称

**发行者：**证书的发行者

**主题：**证书的主题

**有效起始：**证书生效的开始时间

**有效终止：**证书生效的终止时间

**版本：**证书的版本号

**序列号：**证书的序列号

**扩展：**证书的扩展信息

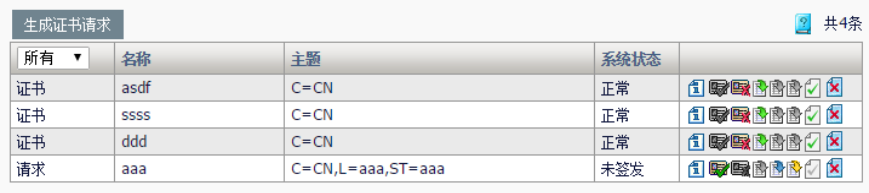
**签名算法：**证书的签名算法

**公钥信息：**证书的公钥信息

**导出用户证书步骤**

1. 进入**模板和对象>CA 证书>用户证书管理**

该界面显示用户证书列表。

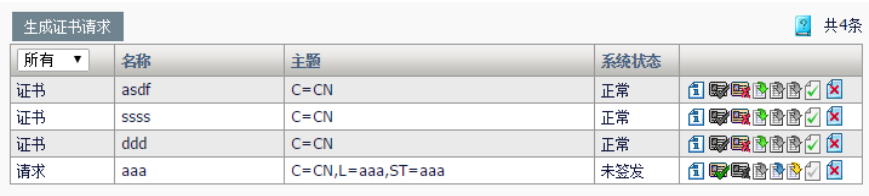



选择系统状态为正常的证书，点击图标导出证书。

**导出证书请求步骤**

1. 进入**模板和对象>CA 证书>用户证书管理**

该界面显示用户证书列表。

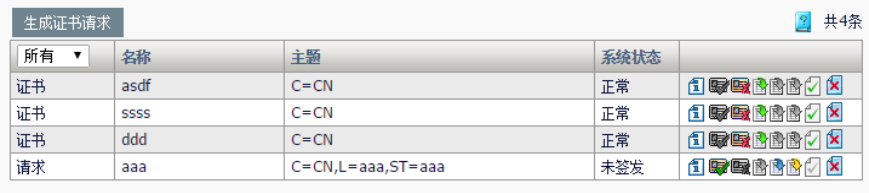



选择系统状态为未签发的证书，点击图标导出证书请求。

**导出证书密钥步骤**

1. 进入**模板和对象>CA 证书>用户证书管理**

该界面显示用户证书列表。

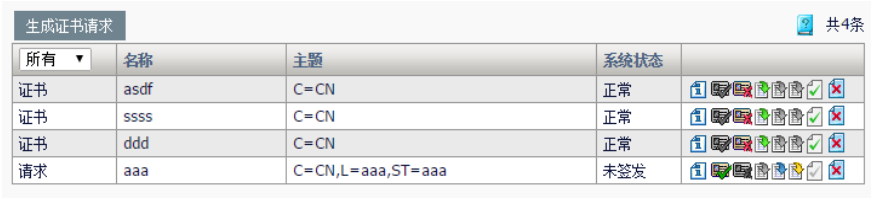



选择系统状态为未签发的证书，点击图标导出证书密钥。

**加载证书到本机步骤**

1. 进入**模板和对象>CA 证书>用户证书管理**

该界面显示用户证书列表。

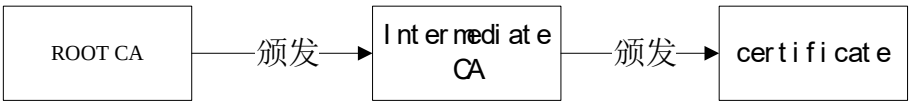



选择系统状态为正常的证书，点击 图标加载证书到本机。

## 18.3 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：

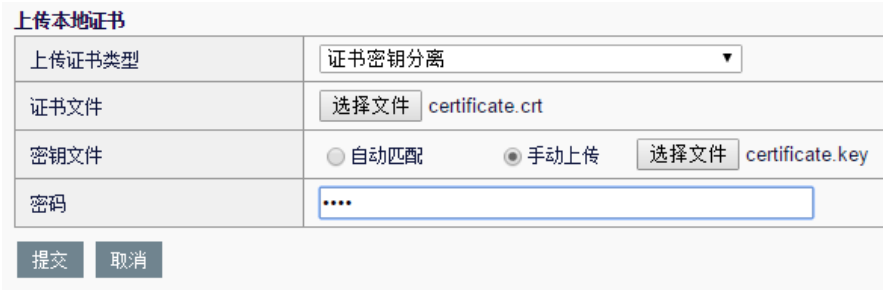



**配置方法：**

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**模板和对象>CA 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**模板和对象>CA 证书>CA**。
5. 点击**导入 CA 中心证书**，将制作好的证书链文件导入到 CA 中。

## 18.4 常见故障

### 18.4.1 导入证书链失败

| | |
|---|---|
| 现象 | 导入证书链失败。 |
| 分析 | 1、证书链制作错误；2、证书链没有包含根CA。 |
| 解决 | 1、 检查各级证书链是否能够验证。<br>2、 证书链应当包含根 CA。 |

# 19 第19章 虚拟服务

## 19.1 虚拟服务概述

虚拟服务是指通过向外提供一个虚拟的 IP 主机地址或者 IP 地址网段（IPv4 或者 IPv6 类型）来接收并响应所有的客户端请求，用户可见的服务器即是虚拟服务，而后端的真实服务器对于用户是不可见的。虚拟服务是进行应用交付的基本配置，所有的负载应用功能都需要通过虚拟服务的引用才会生效。在负载场景中，当虚拟服务接收到客户端请求时，会根据负载均衡算法，将客户端请求转至后台的真实应用服务器进行处理，除此之外还可以对流量进行策略控制以及安全过滤。

使用应用负载均衡部署所带来的好处是：

- 通过本地负载均衡和广域网负载均衡处理，屏蔽用户端对真实服务的感知，使系统运维可以实时、在线进行；
- 通过站点间动态客户调度系统，实现多数据中心灾备模式、多主模式的运行，实现站点高可用；
- 通过对提供同样应用的服务实例进行负载均衡处理，实现对外统一服务，对内将请求分发到多个应用实例上，提高系统的处理能力，减小应用响应时间；
- 通过模拟真实访问的健康检查，判断服务器的工作状态，避免其他检查方式造成的误判，使客户端请求“石沉大海”。

## 19.2 配置虚拟服务

虚拟服务根据负载方式的不同，可分为：代理模式，高性能模式，转发模式以及丢弃等四种类型。每种类型的虚拟服务可配置的参数有所差别。

### 19.2.1 虚拟服务基本属性

每种类型的虚拟服务必须配置的基本参数是一致的，配置时，进入**服务器负载->虚拟服务->虚拟服务列表**，点击**“新建”**，如下图：


**参数说明：**

**名称：**虚拟服务的识别名，最多可输入 63 个有效字符。

**目标地址：**虚拟服务提供服务的地址，客户端可向该目标地址发送请求。设备支持 IPv4 和 IPv6 两种 IP 协议类型。两种协议类型的地址格式为地址/掩码长度，如果是主机地址可省略掩码。

**端口：**虚拟服务提供的服务协议类型的端口号，可以配置单个端口，客户端可向该端口发送对应的请求，配置范围为 0 至 65535，配置为 0 时表示所有端口，也可以配置端口范围。

**入接口：**数据流的流入方向，可以指定为所有接口，也可以自定义接口。

提示

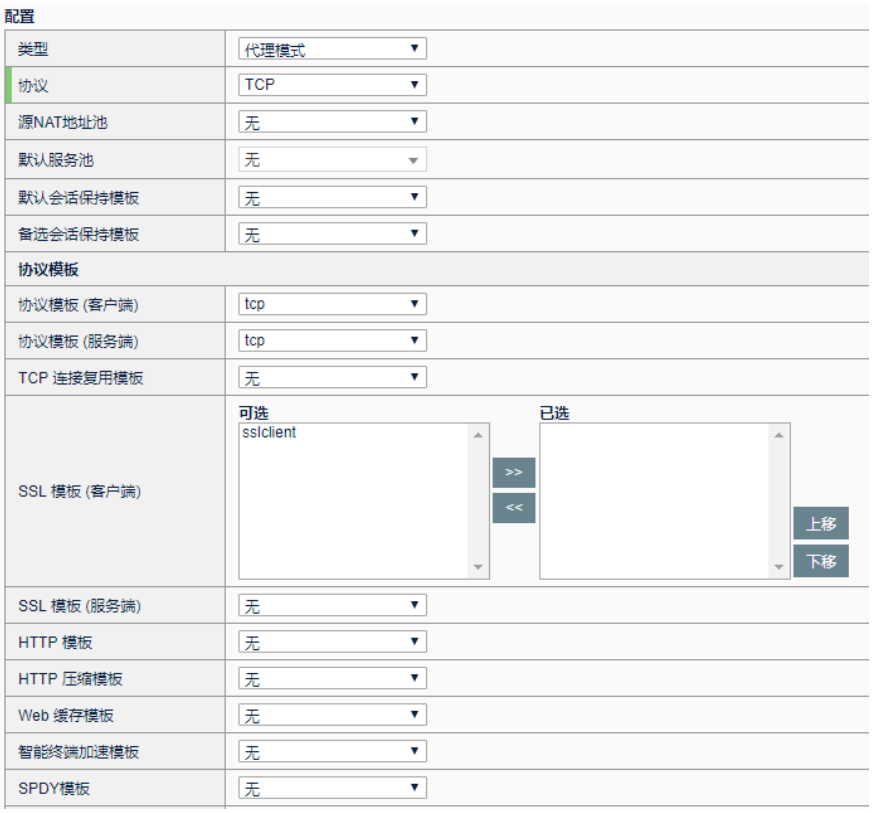
1.虚拟服务以及虚拟链路根据目标地址，端口，协议，以及生效的接口来作冲突检查，如果配置出现重叠或冲突，则会提示配置错误。

2.流量匹配虚拟服务以及虚拟链路时，配置越精细的匹配优先级越高，e.g.配置目的地址为 10.0.0.1 的虚拟服务，和配置目的地址为 10.0.0.0/24 的虚拟服务，前者的匹配优先级会更高。

### 19.2.2 代理模式虚拟服务配置

代理模式的虚拟服务是指：负载设备在客户端与真实服务器的数据交互之间，作为代理分别与双方进行通信，该模式支持 IPv4 和 IPv6 两种 IP 协议类型，，只针对 TCP 协议通信生效，且只支持单连接的应用协议。

配置时，进入**服务器负载->虚拟服务->虚拟服务列表**，点击**“新建”**，**“配置”**中的**“类型”**选择**“代理模式”**。


配置
类型
代理模式
协议
TCP
源NAT地址池
无
默认服务池
无
默认会话保持模板
无
备选会话保持模板
无
协议模板
协议模板 (客户端)
tcp
协议模板 (服务端)
tcp
TCP 连接复用模板
无
SSL 模板 (客户端)
可选
sslclient
已选
>>
<<
上移
下移
SSL 模板 (服务端)
无
HTTP 模板
无
HTTP 压缩模板
无
Web 缓存模板
无
智能终端加速模板
无
SPDY模板
无


内容交换模板
可选
httpclass
已选
>>
<<
上移
下移
类型
基于连接
服务优化
路径一致性
多连接选路
速率控制
源主机连接限制
0
(0-10000000)
源主机连接速率限制
0
(0-1000000)/秒
连接限制
0
(0-10000000)
连接速率限制
0
(0-1000000)/秒
流量控制
安全
HTTP 防护
无
其他
日志
镜像接口
无
tRules
可选
已选
>>
<<


**参数说明：**

**类型：**是指虚拟服务的工作类型，这里选择代理模式。

**协议：**指四层的协议号，范围为 0 至 255，选择 0 时表示所有类型的四层协议。代理模式类型的虚拟服务只支持协议号为 6 的 TCP 协议。

**源 NAT 地址池：**数据流按照该地址池所包含的地址做源地址转换。源 NAT 地址池选择为自动映射时，表示数据流经过设备后，源地址会转换为出接口地址，如果选择为已配置的 NAT 地址池，则数据流的源地址会被转换为所选地址池中的地址。

**默认服务器池：**选择在虚拟服务中作为调度对象的服务器地址池，数据流会根据负载均衡算法被分配至服务器地址池中的真实服务器。服务器地址池的配置详见相关章节。

**默认会话保持模板：**可选择在该虚拟服务中生效的会话保持模板。会话保持模板的具体配置见相关章节。

**备选会话保持模板：**可选择在该虚拟服务中生效的备用会话保持模板。代理模式的虚拟服务允许选择源地址会话保持和目的地址地址会话保持类型的会话保持模板。

**协议模板配置**

**协议模板（客户端）：**虚拟服务作为服务器的代理与客户端建立连接时采用的传输层协议模板，代理模式类型的虚拟服务中必须配置该模板。

**协议模板（服务端）：**虚拟服务作为客户端的代理与真实服务器端建立连接时采用的传输层协议模板，代理模式类型的虚拟服务中必须配置该模板。

**TCP 连接复用模板：**连接复用模板，目前只针对 TCP 协议生效。该配置不允许与 SSL 服务端模板同时配置。已支持 IPv6 协议

**SSL 模板（客户端）：**针对客户端 SSL 流量进行处理的模板，具体配置见相关章节。

**SSL 模板（服务端）：**针对服务端 SSL 流量进行处理的模板，具体配置见相关章节。

**HTTP 模板：**针对 HTTP 数据传输的应用模板，具体配置见相关章节。

**HTTP 压缩模板：**虚拟服务压缩 HTTP 数据量，以加快页面下载速度的应用模板，具体配置见相关章节。

**Web 缓存模板：**虚拟服务启用 Web 缓存功能所需要的应用模板，具体配置见相关章节。

**智能终端加速模板：**通过图片压缩、缓存以及压缩配置，减少智能终端流量的加速方式，具体配置见相关章节。

**SPDY 模板：**虚拟服务处理 SPDY 请求所需要的应用模板，具体配置见相关章节。

**内容交换模板：** HTTP 协议进行内容交换处理的模板，具体配置见相关章节。

**服务优化配置**

**路径一致性：**开启后，数据流的往返路径会一致，该选项默认开启。

**多连接选路：**针对多级子连接的应用协议，选路时进行处理，以保证子连接和主连接往返路径一致的选项。

**速率控制配置**

**源主机连接限制：**访问该虚拟服务的连接数，会收到基于源地址的计数限制。范围为 0 至 10000000，取值为 0 时表示无限制。

**源主机连接速率限制：**访问该虚拟服务的连接，会收到基于源地址的连接速率限制。范围为 0 至 10000000，取值为 0 时表示无限制。

**连接限制：**到该虚拟服务的总连接数的限制值，范围为 0 至 10000000，取值为 0 时表示无限制。

**连接速率限制：**到该虚拟服务的连接速率的限制值，范围为 0 至 1000000，取值为 0 时表示无限制。

**流量控制：**对到该虚拟服务的流量进行限制，选中后，会出现下列选项。

**策略上行带宽限制：**限制虚拟服务的上行流量（客户端流量），范围为 10-40000000Kb/s。

**策略下行带宽限制：**限制虚拟服务的下行流量（服务端流量），范围为 10-40000000Kb/s。

**主机上行带宽限制：**限制访问该虚拟服务的每个客户的流量（以 IP 作为不同客户的区分），范围为 10-40000000Kb/s。

**主机下行带宽限制：**限制虚拟服务与每个真实服务器之间的流量（以 IP 作为不同服务器的区分），范围为 10-40000000Kb/s。

**安全配置**

**HTTP 防护：**针对 HTTP 协议的一些特殊攻击进行防御的模板，具体配置见相关章节。

**其他配置**

**日志：**虚拟服务的日志开关，默认关闭。

**镜像接口：**选择一个物理口，该虚拟服务相关的流量（包含请求和应答）都会发至该物理口，该物理口不允许加入任何 VLAN 或 Trunk，建议所选

的物理口上没有任何其他的流量。

**tRules**：可选择在该虚拟服务中生效的 tRule，tRule 的具体配置见相关章节。

提示

1.代理模式的虚拟服务只允许配置 TCP 协议，目前只支持单连接的应用协议。

2.配置内容交换模板、HTTP 防护模版、HTTP 压缩模板、Web 加速模板、SPDY 模板、基于 HTTP Cookie 会话保持模版、基于 HTTP Sessionid 会话保持模版、基于 HTTP ServerID 会话保持模版、基于 HTTP 自定义头域会话保持模版时，必须选择 http 模板，否则配置无法生效。

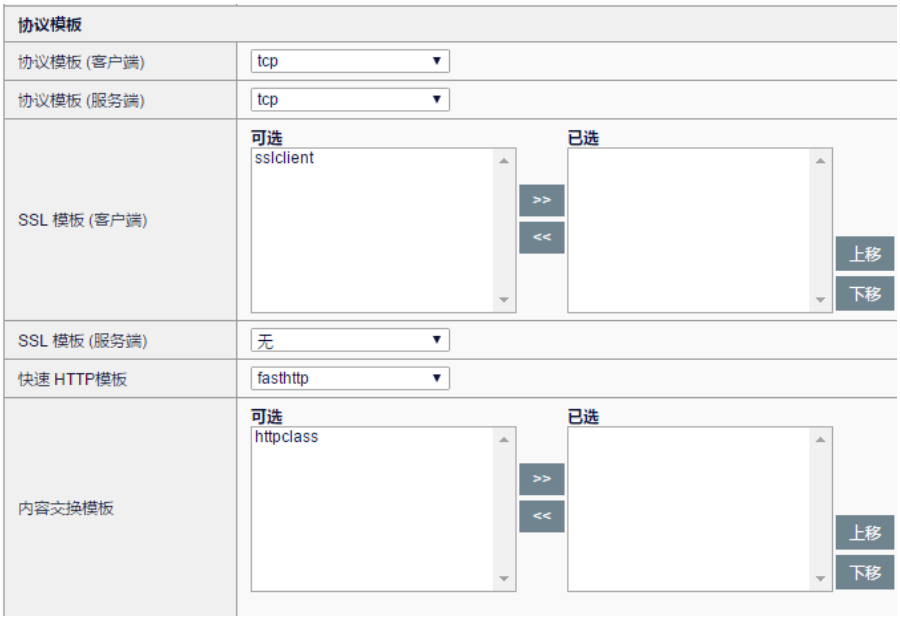
3.SSL 模板（服务端）与 TCP 连接复用模板不能同时配置，否则会导致会话不通的情形。

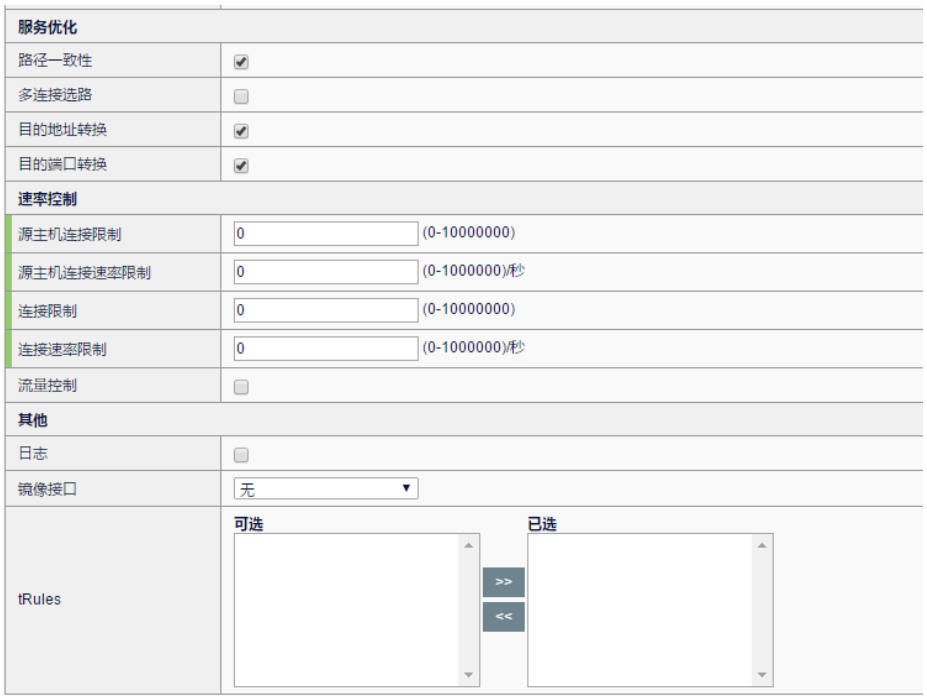
4.SSL 会话保持模板，与 SSL 模板（服务端或客户端）或 HTTP 模板都不能同时配置。

### 19.2.3 快速HTTP模式虚拟服务配置

快速 HTTP 模式的虚拟服务是指：负载设备在客户端与真实服务器的数据交互之间，作为代理分别与双方进行通信，并针对 HTTP 负载应用进行加速。该模式支持 IPv4 与 IPv6 协议配置，但是 IPv6 目前不支持 TCP 连接复用功能，且只针对 HTTP 协议负载应用生效。

配置时，进入**服务器负载->虚拟服务->虚拟服务列表**，点击**“新建”**，**“配置”**中的**“类型”**选择**“快速 HTTP 模式”**。




**参数说明：**

**类型：**是指虚拟服务的工作类型，这里选择快速 HTTP 模式。

**协议：**指四层的协议号，范围为 0 至 255，选择 0 时表示所有类型的四层协议。快速 HTTP 模式类型的虚拟服务只支持协议号为 6 的 TCP 协议。

**源 NAT 地址池：**数据流按照该地址池所包含的地址做源地址转换。源 NAT 地址池选择为自动映射时，表示数据流经过设备后，源地址会转换为出接口地址，如果选择为已配置的 NAT 地址池，则数据流的源地址会被转换为所选地址池中的地址。

**默认服务器池**：选择在虚拟服务中作为调度对象的服务器地址池，数据流会根据负载均衡算法被分配至服务器地址池中的真实服务器。服务器地址池的配置详见相关章节。

**默认会话保持模板**：可选择在该虚拟服务中生效的会话保持模板。快速 HTTP 模式的虚拟服务只支持源地址会话保持，目的地址会话保持两种会话保持方式。

**备选会话保持模板**：可选择在该虚拟服务中生效的备用会话保持模板。快速 HTTP 模式的虚拟服务允许选择源地址会话保持和目的地址会话保持类型的会话保持模板。

**协议模板配置**

**协议模板（客户端）**：虚拟服务作为服务器的代理与客户端建立连接时采用的传输层协议模板，代理模式类型的虚拟服务中必须配置该模板。

**协议模板（服务端）**：虚拟服务作为客户端的代理与真实服务器端建立连接时采用的传输层协议模板，代理模式类型的虚拟服务中必须配置该模板。

**SSL 模板（客户端）**：针对客户端 SSL 流量进行处理的模板，具体配置见相关章节。

**SSL 模板（服务端）**：针对服务端 SSL 流量进行处理的模板，具体配置见相关章节。

**快速 HTTP 模板**：针对 HTTP 数据传输进行加速的应用模板，具体配置见相关章节。

**内容交换模板**： HTTP 协议进行内容交换处理的模板，具体配置见相关章节。

**服务优化配置**

**路径一致性**：开启后，数据流的往返路径会一致，该选项默认开启。

**多连接选路**：针对多级子连接的应用协议，选路时进行处理以保持主连接与子连接往返路径一致的选项。

**目的地址转换**：开启时表示虚拟服务接收到的用户请求的目的地址，会经过转换，再由虚拟服务作为代理发至真实服务器，该选项默认开启。

**目的端口转换**：开启时表示虚拟服务接收到的用户请求的目的端口，会经过转换，再由虚拟服务作为代理发至真实服务器，该选项默认开启。

**速率控制配置**

**源主机连接限制**：访问该虚拟服务的连接数，会收到基于源地址的计数限制。范围为 0 至 10000000，取值为 0 时表示无限制。

**源主机连接速率限制**：访问该虚拟服务的连接，会收到基于源地址的连接

速率限制。范围为 0 至 10000000，取值为 0 时表示无限制。

**连接限制：**到该虚拟服务的总连接数的限制值，范围为 0 至 10000000，取值为 0 时表示无限制。

**连接速率限制：**到该虚拟服务的连接速率的限制值，范围为 0 至 1000000，取值为 0 时表示无限制。

**流量控制：**对到该虚拟服务的流量进行限制，选中后，会出现下列选项。

**策略上行带宽限制：**限制虚拟服务的上行流量（客户端流量），范围为 10-40000000Kb/s。

**策略下行带宽限制：**限制虚拟服务的下行流量（服务端流量），范围为 10-40000000Kb/s。

**主机上行带宽限制：**限制访问该虚拟服务的每个客户的流量（以 IP 作为不同客户的区分），范围为 10-40000000Kb/s。

**主机下行带宽限制：**限制虚拟服务与每个真实服务器之间的流量（以 IP 作为不同服务器的区分），范围为 10-40000000Kb/s。

**其他配置**

**日志：**虚拟服务的日志开关，默认关闭。

**镜像接口：**选择一个物理口，该虚拟服务相关的流量（包含请求和应答）都会发至该物理口，该物理口不允许加入任何 VLAN 或 Trunk，建议所选的物理口上没有任何其他的流量。

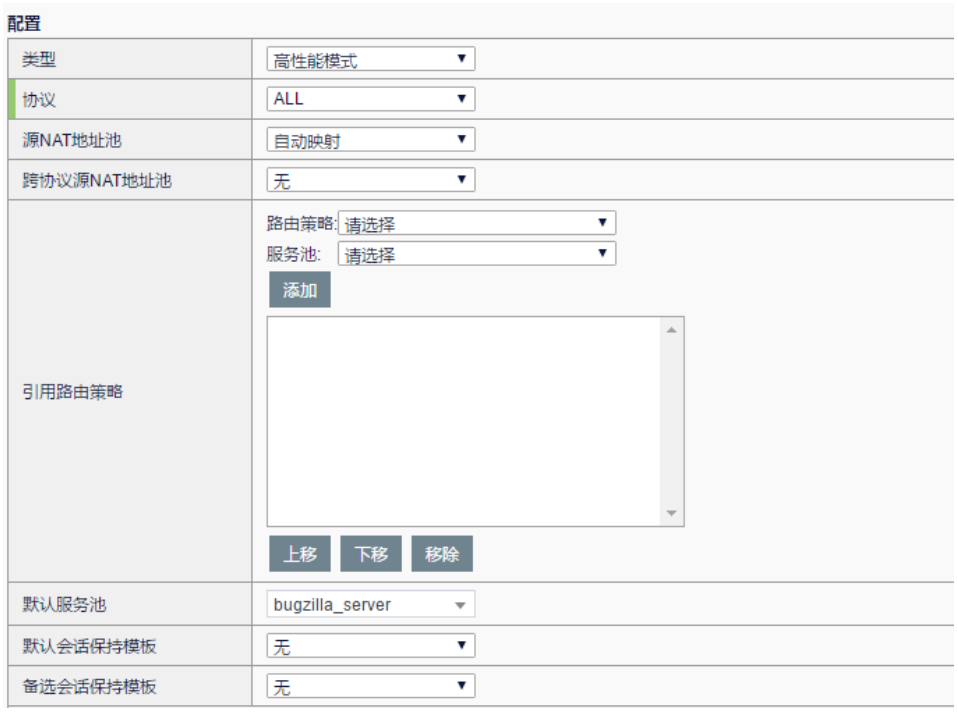
**tRules：**可选择在该虚拟服务中生效的 tRule，tRule 的具体配置见相关章节。


提示

配置内容交换模块时，必须选择快速 http 模板，否则配置无法成功。

### 19.2.4 高性能模式虚拟服务配置

高性能模式的虚拟服务将用户请求的数据包经过处理后，直接转发至后端经过负载算法计算得到的真实服务器中。该模式支持 IPv4 和 IPv6 协议配置，且虚拟服务支持多种传输层协议，并支持多种常见的多连接应用层协议。该模式也支持三角传输模式（只有客户端的报文经过设备，服务端的报文直接发送至客户端的拓扑），三角传输模式下，只支持单连接应用协议。配置时，进入**服务器负载->虚拟服务->虚拟服务列表**，点击**“新建”**，**“配置”**中的**“类型”**选择**“高性能模式”**。





**参数说明：**

**类型：**是指虚拟服务的工作类型，这里选择高性能模式。

**协议：**指四层的协议号，范围为 0 至 255，选择 0 时表示所有类型的四层

协议。其中 UDP 协议支持一些特殊配置，在后面详细说明。

**源 NAT 地址池**：数据流按照该地址池所包含的地址做源地址转换。源 NAT 地址池可选择自动映射或已配置的 NAT 地址池，表示数据流经过设备后，源地址会转换为出接口地址，或转换为所选地址池中的地址。

**跨协议源 NAT 地址池**：如果虚拟服务调度到的真实服务器与虚拟服务的协议类型不一致，那么数据包的源地址会根据该选项所选的地址池进行转换。e.g. 配置了一个 IPv4 类型的虚拟服务，但是调度得到的真实服务器是 IPv6 类型的，那么请求报文会被转换为一个 IPv6 的报文，其源地址就根据这里配置的 IPv6 地址池进行转换。

**引用路由策略**：可配置路由策略，匹配到策略的数据报文会使用对应的服务池作为调度对象，而不是配置的默认服务池。

**默认服务器池**：选择在虚拟服务中供调度的服务器地址池，数据流会根据负载均衡算法被分配至服务器地址池中的真实服务器。服务器地址池的配置详见相关章节。

**默认会话保持模板**：可选择在该虚拟服务中生效的会话保持模板。高性能模式虚拟服务允许选择源地址会话保持类型和目的地址会话保持类型。如果是 UDP 协议的虚拟服务，当服务类型配置为 radius 时，可配置 radius 的会话保持类型。

**备选会话保持模板**：可选择在该虚拟服务中生效的备用会话保持模板。该模板只能为源地址会话保持类型以及目的地址会话保持类型。

**服务优化配置**

**路径一致性**：开启后，数据流的往返路径会一致，该选项默认开启。

**TCP 加速**：开启之后，在网络延时较大、丢包严重以及报文乱序的网络场景中能够起到加速 TCP 数据传输的效果。

**多连接选路**：针对多级子连接的应用协议，选路时进行处理保证子连接与主连接的往返路径一致的选项。

**目的地址转换**：开启时表示虚拟服务接收到的用户请求的目的地址，会经过转换，再由虚拟服务作为代理发至真实服务器，该选项默认开启。

**目的端口转换**：开启时表示虚拟服务接收到的用户请求的目的端口，会经过转换，再由虚拟服务作为代理发至真实服务器，该选项默认开启。

**速率控制配置**

**源主机连接限制**：访问该虚拟服务的连接数，会收到基于源地址的计数限制。范围为 0 至 10000000，取值为 0 时表示无限制。

**源主机连接速率限制**：访问该虚拟服务的连接，会收到基于源地址的连接速率限制。范围为 0 至 10000000，取值为 0 时表示无限制。

**连接限制**：到该虚拟服务的总连接数的限制值，范围为 0 至 10000000，取

值为 0 时表示无限制。

**连接速率限制：**到该虚拟服务的连接速率的限制值，范围为 0 至 1000000，取值为 0 时表示无限制。

**流量控制：**对到该虚拟服务的流量进行限制，选中后，会出现下列选项。

**策略上行带宽限制：**限制虚拟服务的上行流量（客户端流量），范围为 10-40000000Kb/s

**策略下行带宽限制：**限制虚拟服务的下行流量（服务端流量），范围为 10-40000000Kb/s

**主机上行带宽限制：**限制访问该虚拟服务的每个客户的流量（以 IP 作为不同客户的区分），范围为 10-40000000Kb/s

**主机下行带宽限制：**限制虚拟服务与每个真实服务器之间的流量（以 IP 作为不同服务器的区分），范围为 10-40000000Kb/s

**其他配置**

**日志：**虚拟服务的日志开关，默认关闭。

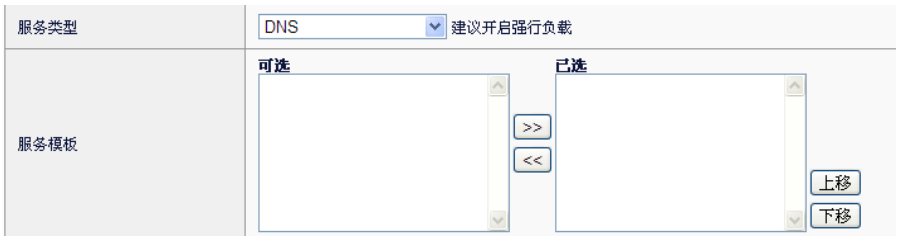
**HA 状态同步：**在启用 HA 时，将该虚拟服务器的相关会话同步至备用设备上。

**镜像接口：**选择一个物理口，该虚拟服务相关的流量（包含请求和应答）都会发至该物理口，该物理口不允许加入任何 VLAN 或 Trunk，建议所选的物理口上没有任何其他的流量。

**tRules：**可选择在该虚拟服务中生效的 tRule，tRule 的具体配置见相关章节。

**UDP 协议的高性能模式虚拟服务包含一些特殊配置如下**

**1. 基本配置选项中**




**服务类型：**该选项主要针对 DNS 和 radius 请求，进行特殊处理。如果选择 radius，需要进行逐包负载的功能，则需要勾选强行负载的选项和配置 radius 类型的会话保持模板；如果选择 DNS,则需要配置服务模板

**服务模板：**选择处理 DNS 请求时需要的 DNS 模板，具体配置见相关章节。

**2. 服务优化配置中**


**强行负载：**如果要对 UDP 报文进行逐包负载，则必须勾选该选项

| | |
|---|---|
| 提示 | 如果要进行 radius 逐包负载的功能，必须服务类型选择 radius，勾选强行负载，并使用 radius 类型的会话保持模板作为默认会话保持模板。 |

| | |
|---|---|
| 提示 | 1. 如果工作在三角传输拓扑下，需要关闭目的地址转换选项和目的端口转换选项，目前三角传输只支持单连接应用协议。<br>如果要进行跨协议负载（即调度到不同 IP 类型的服务器），则必须配置跨协议源 NAT 池，否则报文会被认为是调度失败被丢弃。 |

### 19.2.5 路由模式虚拟服务配置

命中路由模式虚拟服务的流量，会直接根据设备的路由进行转发。该模式支持 IPv4 与 IPv6 协议配置。配置时，进入**服务器负载->虚拟服务->虚拟服务列表**，点击**“新建”**，**“配置”**中的**“类型”**选择**“路由模式”**。


**参数说明：**

**类型：**是指虚拟服务的工作类型，这里选择路由模式。

**协议：**指四层的协议号，范围为 0 至 255，选择 0 时表示所有类型的四层协议。如果选择为 UDP 协议时，服务优化中包含强行负载选项。

**源 NAT 地址池：**数据流按照该地址池所包含的地址做源地址转换。源 NAT 地址池可选择自动映射或已配置的 NAT 地址池，表示数据流经过设备后，源地址会转换为出接口地址，或转换为所选地址池中的地址。

**路径一致性：**开启后，数据流的往返路径会一致，该选项默认开启。

**TCP 加速：**开启之后，在网络延时较大、丢包严重以及报文乱序的网络场景中能够起到加速 TCP 数据传输的效果。

**多连接选路：**针对多级子连接的应用协议，选路时进行处理的选项，具体描述见相关章节。

**速率控制配置**

**源主机连接限制：**访问该虚拟服务的连接数，会收到基于源地址的计数限制。范围为 0 至 10000000，取值为 0 时表示无限制。

**源主机连接速率限制：**访问该虚拟服务的连接，会收到基于源地址的连接速率限制。范围为 0 至 10000000，取值为 0 时表示无限制。

**连接限制：**到该虚拟服务的总连接数的限制值，范围为 0 至 10000000，取值为 0 时表示无限制。

**连接速率限制：**到该虚拟服务的连接速率的限制值，范围为 0 至 1000000，取值为 0 时表示无限制。

**流量控制：**对到该虚拟服务的流量进行限制，选中后，会出现下列选项。

**策略上行带宽限制：**限制虚拟服务的上行流量（客户端流量），范围为 10-40000000Kb/s

**策略下行带宽限制：**限制虚拟服务的下行流量（服务端流量），范围为 10-40000000Kb/s

**主机上行带宽限制：**限制访问该虚拟服务的每个客户的流量（以 IP 作为不同客户的区分），范围为 10-40000000Kb/s

**主机下行带宽限制：**限制虚拟服务与每个真实服务器之间的流量（以 IP 作为不同服务器的区分），范围为 10-40000000Kb/s

**其他配置**

**HA 状态同步：**在启用 HA 时，将该虚拟服务器的相关会话同步至备用设备上。

**镜像接口：**选择一个物理口，该虚拟服务相关的流量（包含请求和应答）都会发至该物理口，该物理口不允许加入任何 VLAN 或 Trunk，建议所选的物理口上没有任何其他的流量。

**tRules：**可选择在该虚拟服务中生效的 tRule，tRule 的具体配置见相关章节。


提示

发至设备的流量如果无法命中任何一个虚拟服务、虚拟链路、静态 nat 或者目的 nat，默认会被丢弃，如果需要使无法匹配任何虚拟服务、虚拟链路、静态 nat 或者目的 nat 的流量也能被转发，可执行命令 no-drop-packet enable，此时流量会经过正常转发流程；若需要还原默认的丢弃操作，执行 no-drop-packet disable.

### 19.2.6 丢弃模式虚拟服务配置

命中丢弃模式虚拟服务的流量，会被直接丢弃，发送端会收到一个 TCP 的 rst 报文或者是 ICMP 错误报文。配置时，进入**服务器负载->虚拟服务->虚拟服务列表**，点击**“新建”**，**“配置”**中的**“类型”**选择**“丢弃”**。


**参数说明：**

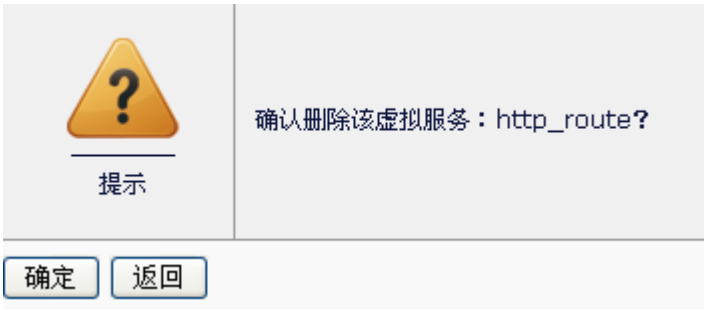
**类型：**是指虚拟服务的工作类型，这里选择丢弃。

**协议：**指四层的协议号，范围为 0 至 255，选择 0 时表示所有类型的四层协议。

**tRules：**可选择在该虚拟服务中生效的 tRule，tRule 的具体配置见相关章节

### 19.2.7 删除虚拟服务

进入**服务器负载->虚拟服务->虚拟服务，**点击虚拟服务后面的对应  ，即出现




点击**确认**，即可删除。


点击虚拟服务的名称即可查看和编辑相应的虚拟服务。

## 19.3 监控与维护

### 19.3.1 查看虚拟服务

1、进入**服务器负载->虚拟服务->虚拟服务**，可查看到已配置的虚拟服务列表，如下图：


2、点击启用按钮  ，启用某个虚拟服务。


3、输入搜索条件，搜索指定的虚拟服务。


4、点击  ，重命名虚拟服务。


5、点击  ，批量删除选中的多个或所有虚拟服务。


6、点击 

，当前页的虚拟服务按照名称排序。


7、虚拟服务支持分页显示，可以显示指定页数的虚拟服务，每页 100 个。


8、状态栏

其中状态栏可直观地看到当前虚拟服务是否可用，各状态的具体含义如下：

：虚拟服务后端的真实服务器是可用的，且该虚拟服务允许访问

：虚拟服务后端的真实服务器可用，但该虚拟服务器不允许访问（用户手动关闭了）

：虚拟服务后端的真实服务器可用，但该虚拟服务器不允许访问（对应的虚拟地址被用户手动关闭了）

：虚拟服务后端的真实服务器可用性未知，该虚拟服务允许访问

：虚拟服务后端的真实服务器可用性未知，该虚拟服务器不允许访问（用户手动关闭了）

：虚拟服务后端的真实服务器可用性未知，该虚拟服务器不允许访问（对应的虚拟地址被用户手动关闭了）

：虚拟服务后端的真实服务器不可用，该虚拟服务允许访问

：虚拟服务后端的真实服务器可不可用，该虚拟服务器不允许访问（用户手动关闭了）

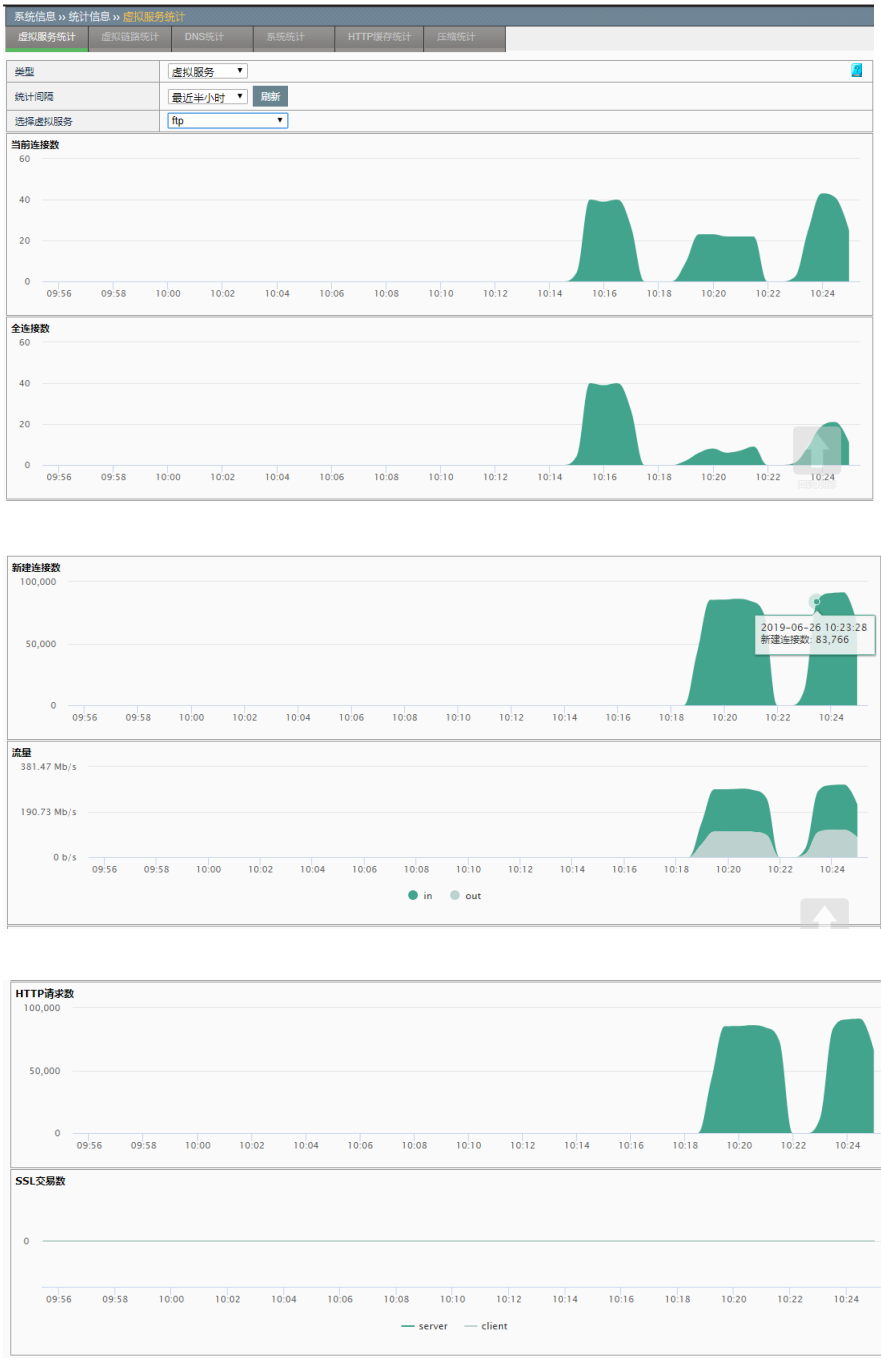
：虚拟服务后端的真实服务器可不可用，该虚拟服务器不允许访问对应的虚拟地址被用户手动关闭了）

## 19.3.2 查看虚拟服务状态

进入**系统信息->状态->虚拟服务状态**，可查看到虚拟服务的连接信息。

### 19.3.3 查看虚拟服务统计

进入**系统信息->统计信息->虚拟服务统计**，可查看到虚拟服务最近一段时间的连接以及流量统计图表。



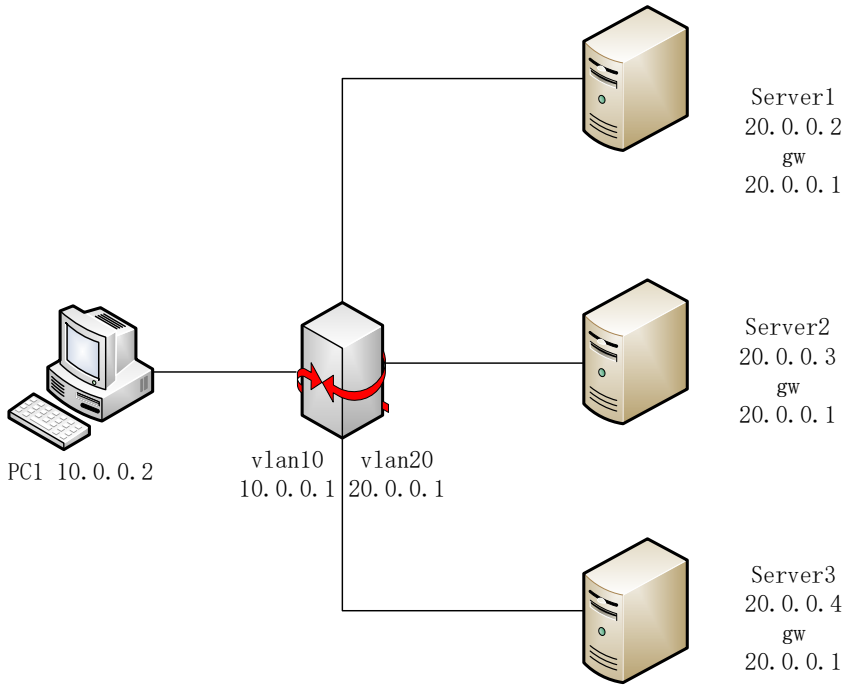
## 19.4 配置案例

### 19.4.1 配置代理模式的虚拟服务

代理模式的虚拟服务，要求客户端流量和服务端流量都必须经过设备。

**案例：**

如下图所示，应用交付设备位于网关位置，PC1 访问虚拟服务 VS1 的 http 服务，VS1 会将该请求调度至后端的真实服务器，真实服务器响应该请求的报文会经由应用交付设备，发至 PC1.

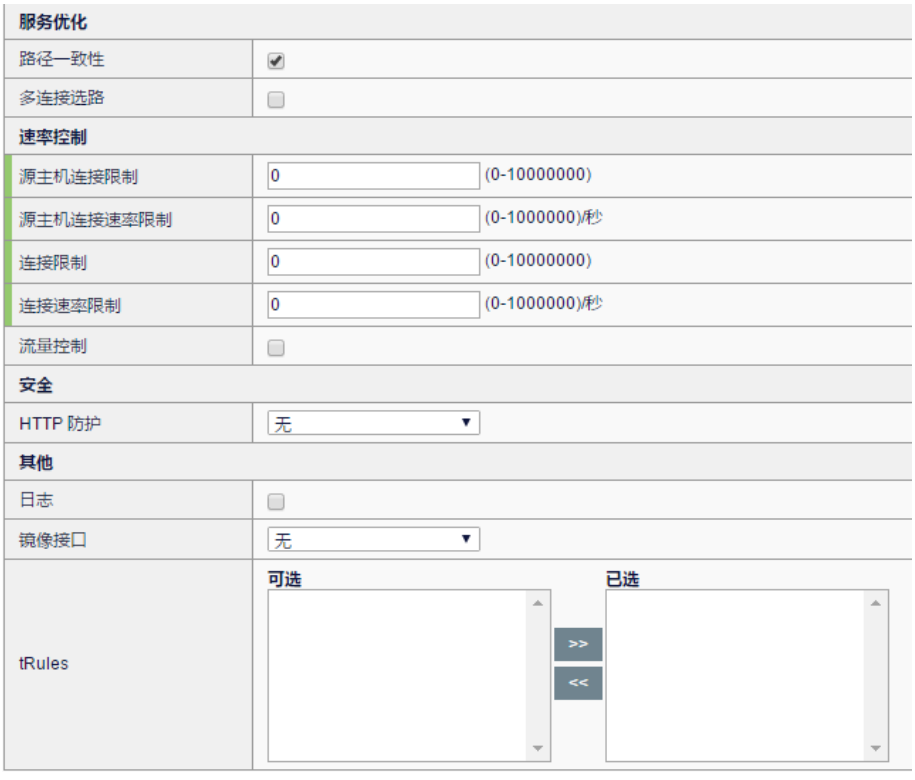



**配置步骤：**

1. **服务器负载->服务池->服务池：**配置一个包含所有后端 http 真实服务器的地址池


2. **服务器负载->虚拟服务->虚拟服务列表->新建：**新建一个虚拟服务，虚拟服务的目标地址必须是客户端可达的。PC1 的流量入口所属的 VLAN 必须包含在虚拟服务中。


将包含后端真实服务器的地址池添至该虚拟服务。

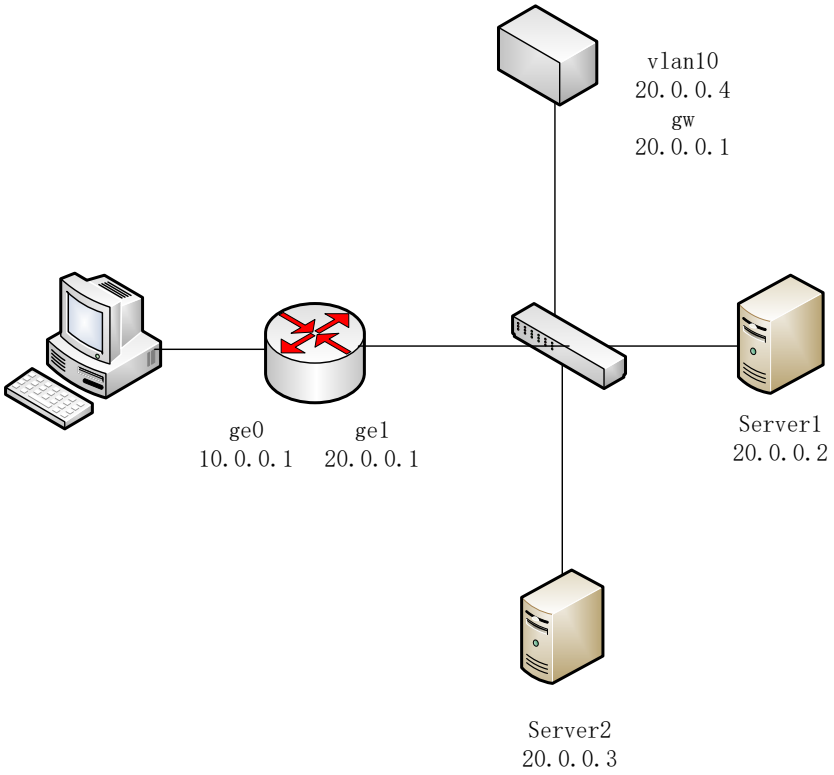




点击“**提交**”，该虚拟服务即可使用。

## 19.4.2 配置高性能模式的虚拟服务

**案例 1：**

如下图所示，应用交付设备位于和真实服务器相同的内部网络中，采用单臂接入的方式，PC1 访问虚拟服务 VS1 的 ftp 服务，VS1 会将该请求调度至后端的真实服务器，真实服务器响应该请求的报文经由应用交付设备处理后，再发至 PC1。




**配置步骤：**

1. **服务器负载->服务池->服务池：**配置一个包含所有后端 ftp 真实服务器的地址池。


2. **服务器负载->虚拟服务->虚拟服务->新建：**新建一个虚拟服务，虚拟服务的目标地址必须是客户端可达的，也可以配为 vlan 接口地址。

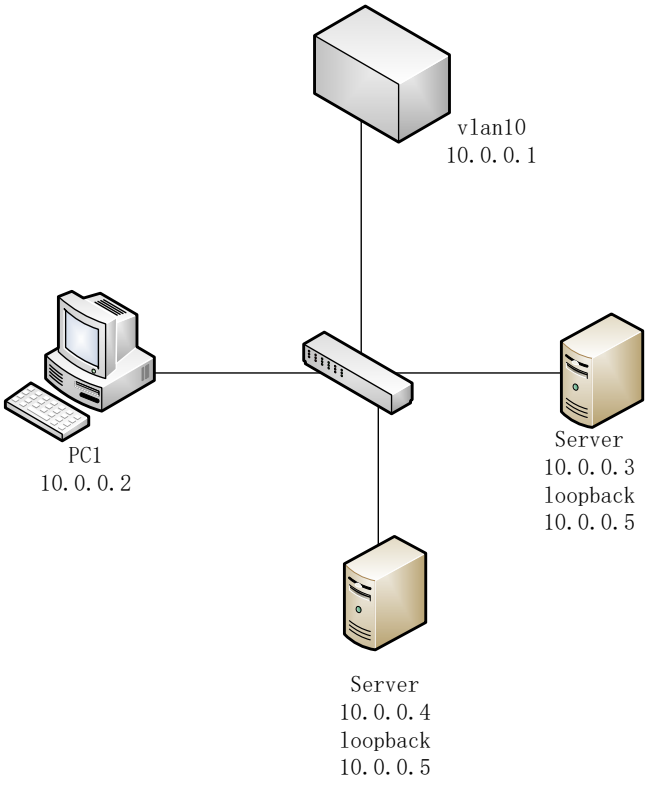

为了保证真实服务器的回复报文必须经过设备，可在虚拟服务中配置源 NAT 地址池，或者是将内网中的真实服务器的网关设置为本设备，这里采用源 NAT 的方式。目的地址转换和目的端口转换必须选中。在“**默认服务池**”中，选中之前配置的服务池。


配置
类型
高性能模式
协议
ALL
源NAT地址池
自动映射
跨协议源NAT地址池
无
引用路由策略
路由策略: 请选择
服务池: 请选择
添加
上移
下移
移除
默认服务池
ftp
默认会话保持模板
无
备选会话保持模板
无
服务优化
路径一致性
TCP加速
多连接选路
目的地址转换
目的端口转换


点击“**提交**”，该虚拟服务即可使用。

**案例 2：**

如下图所示，应用交付设备，客户端 PC，以及真实服务器位于同一局域网内，客户端向虚拟服务发出 http 请求，虚拟服务将请求转至真实服务器，真实服务器的响应直接发至客户端。



**配置步骤：**

1. **服务器负载->服务池->服务池：**配置一个包含所有后端 http 真实服务器的地址池。


2. **服务器负载->虚拟服务->虚拟服务->新建：**新建一个虚拟服务，虚拟服务的目的地址必须和真实服务器的还回地址一致，且虚拟服务的监听端口与后端真实服务器的监听端口必须一致。

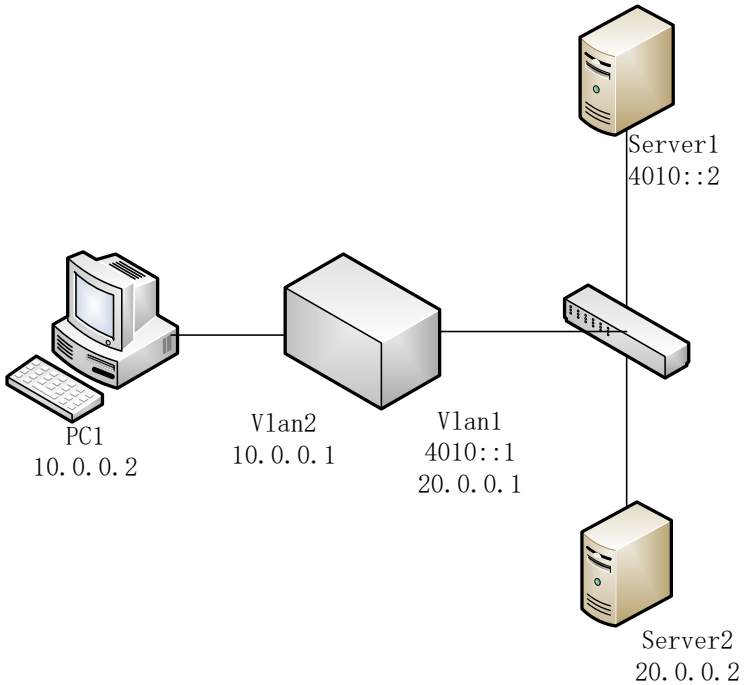
如果要支持三角传输模式，则不能勾选虚拟服务的目的地址转换和目的端口转换。


在“**默认服务池**”中，选中之前配置的服务池。

点击“**提交**”，该虚拟服务即可使用。

**案例 3：**

如下图所示，应用交付设备串行接入网络，客户端 PC 需要访问内网的 FTP 服务器，内网的服务器包含 IPv4 和 IPv6 类型的。




**配置步骤：**

1. 进入**服务器负载->服务池->服务池：**配置一个包含所有 FTP 真实服务

器的地址池。


2. **服务器负载->虚拟服务->虚拟服务->新建：**新建一个高性能模式的虚拟服务。


引用 1 步中配置的地址池，同时必须配置**跨协议 SNAT 地址池。**

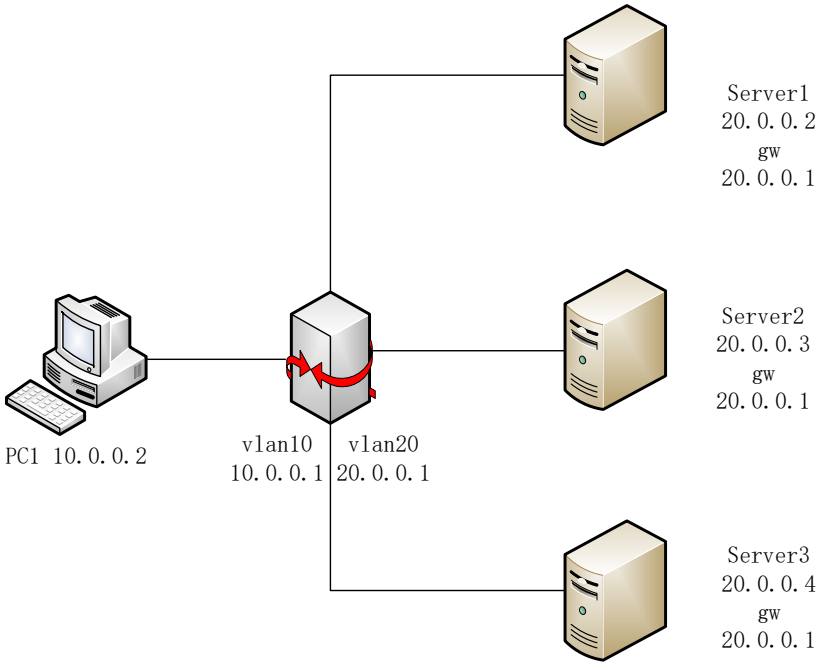

点击“**提交**”，该虚拟服务即可使用。

### 19.4.3 配置路由模式的虚拟服务

路由模式的虚拟服务实际上不进行负载功能，而是直接将请求按路由进行转发。

**案例：**

如下图所示，应用交付设备位于网关，客户端 PC 需要直接访问内网的服务器的 http 服务。



**配置步骤：**

1. **服务器负载->虚拟服务->虚拟服务->新建：**新建一个路由模式的虚拟服务，地址为网段格式的，**“VLAN”**包含流量的入口 VLAN。


2. **“类型”**选择路由模式。


点击“**提交**”，该虚拟服务即可使用。


提示

1、配置 IPv4 网段类型的虚拟服务时，如果需要虚拟服务响应该网段包含的所有地址的 ARP 请求，则需要进入**虚拟地址**节点中去手动开启“ARP”选项。如果是配置的主机类型的虚拟服务，则是默认开启“ARP”选项，允许响应到该地址的 ARP 请求的。

2、如果配置 IPv6 的虚拟服务，类似的有主机地址类型的虚拟地址默认响应邻居请求，如果是网段类型的虚拟服务，则需要进入**虚拟地址**节点中去手动开启“响应邻居请求”选项，如果是主机类型的虚拟服务，则是默认开始“响应邻居请求”选项。

## 19.5 常见故障分析

### 19.5.1 故障现象：虚拟服务不响应ARP

| | |
|---|---|
| 现象 | 客户端访问虚拟服务的地址，发现发送的ARP请求没有应答 |
| 分析 | 有可能是以下几种原因：<br>1. 虚拟服务对应的虚拟地址没有开启ARP响应的选项<br>2. 客户端的数据流入接口没有被包含在虚拟服务生效的VLAN中，虚拟服务不会响应其他VLAN收到的ARP请求 |
| 解决 | 1. 开起对应虚拟地址的ARP响应选项<br>2. 将客户端数据流入接口vlan添加进虚拟服务允许的入接口中 |

### 19.5.2 故障现象：ping虚拟服务地址失败

| | |
|---|---|
| 现象 | ping一个虚拟服务，没有得到响应 |
| 分析 | 有可能是以下几种原因：<br>1. 如果该虚拟服务提供的服务包含响应ping，那么可能是后端的服务器不可用或不在线了<br>2. 如果虚拟服务提供的服务不包含响应ping，可能是虚拟服务配置的VLAN没有包含数据流的入口，或者是虚拟服务的配置的掩码为0，目前掩码为0的虚拟服务是不响应ping请求的 |
| 解决 | 1. 等待后段服务器在线后再执行ping操作<br>2. 根据分析的原因完善相应操作 |

### 19.5.3 故障现象：跨协议访问虚拟服务失败

| | |
|---|---|
| 现象 | 访问一个高性能的虚拟服务失败 |
| 分析 | 查看服务池中是否有多种协议的服务器地址，如果有，则查看虚拟服务是否有配置跨协议SNAT地址池，如果没有配置该项，则跨协议访问会失败。 |
| 解决 | 配置跨协议SNAT地址池，地址池的类型必须与虚拟服务的IP类型不一致。 |

### 19.5.4 故障现象：访问网段地址类型的虚拟服务失败

| | |
|---|---|
| 现象 | 访问一个网段地址类型的虚拟服务失败 |
| 分析 | 有可能是以下原因:<br>如果配置了另外一个掩码更长的虚拟服务，和该虚拟服务的网段地址有重合，由于目前访问的虚拟服务请求采用地址优先的匹配方式来匹配虚拟服务，所以该请求被另外的虚拟服务处理，就可能会出现失败的情形。<br>e.g.配置了两个虚拟服务：<br>VS1：10.0.0.1 TCP 80<br>VS2：10.0.0.0/24 TCP 21<br>如果访问10.0.0.1的TCP 21端口，则设备会认为该请求是发至VS1的，但是VS1并不监听21端口，所以该请求不会被处理，从而失败。 |
| 解决 | 针对这种请求，我们提供了一种解决方式，可在命令行中执行命令：<br>match-vadddr-prior disable<br>该命令的作用是不采用地址优先的方式来查找虚拟服务了，这样请求也就能被正常发至VS2了。 |


默认查找虚拟服务的话，是采用地址优先的方式，也就是指 match-vaddr-prior enable 命令是默认开启的，可采用 show match-vaddr-prior 命令来查看当前的开启状态

# 20 第20章 虚拟地址

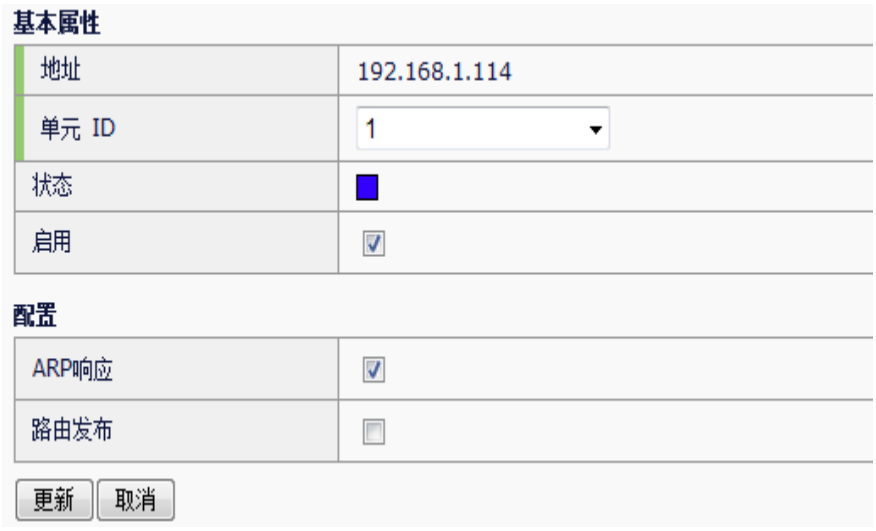
## 20.1 虚拟地址概述

虚拟地址是虚拟服务的目的地址和虚拟链路的目的地址的统称。每新建一个虚拟服务或者是虚拟链路，就会自动生成一个虚拟地址。一个虚拟地址可能对应多个虚拟服务或虚拟链路。通过查看虚拟地址的状态，我们可以得到该地址对应的虚拟服务和虚拟链路的总体状态。虚拟地址也可以控制虚拟服务响应 ARP(IPv4)或响应邻居请求(IPv6)以及 HA 的 ID 设置等功能。

## 20.2 虚拟地址功能配置

配置时，进入**服务器负载->虚拟服务->虚拟地址列表，**点击某一个虚拟地址，如下图：

### 20.2.1 虚拟地址是IPv4的地址：




**参数说明：**

**地址：**虚拟服务地址，无法修改。如果配置的虚拟服务是一个网络地址，则对应的虚拟地址为相应的网络地址。e.g.配置一个地址为 10.10.10.0/24 的虚拟服务，则对应一个地址为 10.10.10.0 的虚拟地址。

**单元 ID：**指明该虚拟地址的单元 ID，在启用 HA 的主主模式时，如果主机的单元 ID 和虚拟地址的单元 ID 不一致，那么该虚拟地址所对应的虚拟服务和虚拟链路在该主机上不生效。默认值为 1。

**状态：**显示当前虚拟地址所对应的所有虚拟服务和虚拟链路中，状态最优

的对象状态。

**启用**：虚拟地址的启用开关，选定时表示启用，不选定时表示停用。停用时，虚拟地址所对应的所有虚拟服务和虚拟链路全部停用。

**ARP 响应**：控制该虚拟地址对应的虚拟服务是否响应到该地址的 ARP 请求。（虚拟链路始终不响应 ARP 请求。）

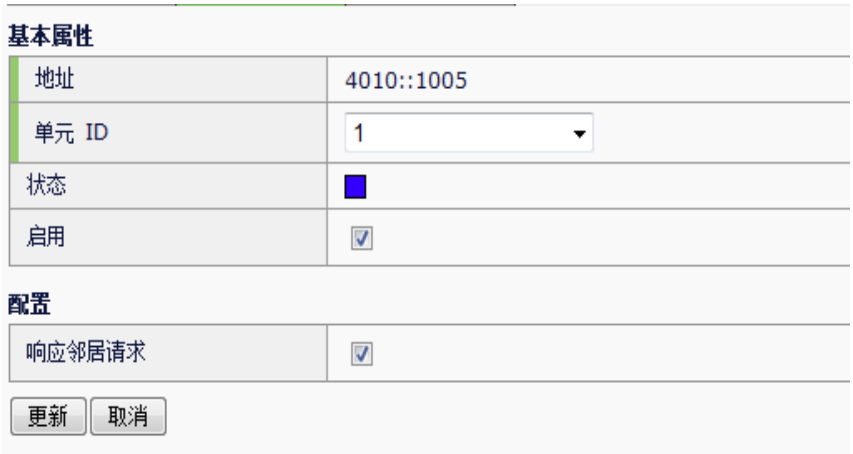
**路由发布**：选中路由发布后，在动态路由协议中启用重发布直连路由时，会发布一条目的地址为该虚地址的路由表项

注意

1.如果虚拟地址是主机地址，ARP 响应选项是默认开启的，否则需要用户手动开启。

2.虚拟链路不管对应的虚拟地址是否开启 ARP 响应选项，始终不响应 ARP 请求。

2. **虚拟地址是 IPv6 的地址：**




**参数说明：**

**地址**：虚拟服务地址，无法修改。如果配置的虚拟服务是一个网络地址，则对应的虚拟地址为相应的网络地址。e.g.配置一个地址为 4010::2000:1005/112 的虚拟服务，则对应一个地址为 4010::2000:0 的虚拟地址。

**单元 ID**：指明该虚拟地址的单元 ID，在启用 HA 的主主模式时，如果主机的单元 ID 和虚拟地址的单元 ID 不一致，那么该虚拟地址所对应的虚拟服务和虚拟链路在该主机上不生效。默认值为 1。

**状态**：显示当前虚拟地址所对应的所有虚拟服务和虚拟链路中，状态最优的对象状态。

**启用**：虚拟地址的启用开关，选定时表示启用，不选定时表示停用。停用时，虚拟地址所对应的所有虚拟服务和虚拟链路全部停用。

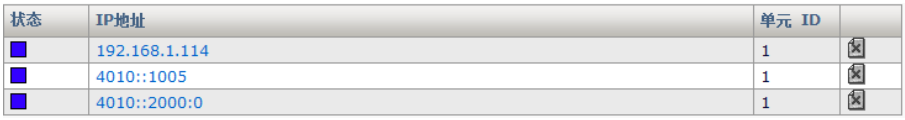
**响应邻居请求**：控制该虚拟地址对应的虚拟服务是否响应到该地址的邻居请求。（虚拟链路始终不响应邻居请求。）（IPV6 是用邻居请求来得到

MAC 地址的。）

## 20.3 监控与维护

### 20.3.1 查看虚拟地址

虚拟地址无法手动新建，而是在新建一个虚拟服务或虚拟链路时自动生成。进入**服务器负载->虚拟服务->虚拟地址列表**可查看当前虚拟地址列表，如下图：



| 状态 | IP地址 | 单元 ID | |
|---|---|---|---|
| | 192.168.1.114 | 1 | |
| | 4010::1005 | 1 | |
| | 4010::2000:0 | 1 | |

虚拟地址的状态取决于对应的的虚拟服务以及虚拟链路的状态，显示的是所有对应的对象中状态最优的状态。状态图如下：

 ：虚拟地址对应的虚拟服务中虚拟链路中，有可以使用的对象

 ：虚拟地址对应的虚拟服务中虚拟链路中，有可以使用的对象，但虚拟地址被用户手动停用了。

 ：虚拟地址对应的虚拟服务中虚拟链路状态未知。

 ：虚拟地址对应的虚拟服务中虚拟链路状态未知，虚拟地址被用户手动停用了。  ：虚拟地址对应的虚拟服务中虚拟链路，没有可以使用的对象。

 ：虚拟地址对应的虚拟服务中虚拟链路，没有可以使用的对象，且虚拟地址被用户手动停用了。

### 20.3.2 删除虚拟地址

进入**服务器负载->虚拟服务->虚拟地址列表**，点击虚拟地址后面的  ，即出现


点击“确认”，即可删除。

注意 虚拟地址如果有对应的虚拟服务或虚拟链路，则不可删除。

# 21 第21章 服务池

## 21.1 服务池概述

服务池是服务器负载中根据实际情况结合起来接受和处理流量的一组设备，如 web 服务器。系统将客户请求的流量发送到服务池成员中的任一服务器上，系统会根据在服务池上设置的算法来将客户请求的流量发送到服务池的成员上，而不是简单的发送到单一服务器上这样可以平衡后台服务器的流量负载分担，有效合理的利用这些服务器。

## 21.2 配置服务池

### 21.2.1 服务池新建

进入**服务器负载>服务池**，点击**新建**按钮。


**名称：**新建服务池的名称。

**健康检查方法选择：**选择已有的健康检查方法。

**有效性：**服务池中成员健康检查通过的有效条件，可以选择全部通过，或指定至少需要几个通过。

**健康检查失败动作：**流量到健康检查失败的服务池内的成员时的动作，可以选择无、拒绝或丢弃，无表示继续转发。

**负载均衡算法：**选择服务池内成员时的调度算法。

**低优先级组激活：** 选择是否激活低优先级组。

**服务成员：**服务池内的服务。

**地址：**服务器的 IP 地址。

**端口：**服务的端口。

**优先级组：**服务的优先级组别。

**温暖上线：**用于解决服务器维护完毕后、重新上线时，瞬时压力过大、容

易引起服务器异常的问题。

**恢复时间：**范围 0-3600 秒，在恢复时间段，设备不会把请求分配给刚上线的服务器。

**温暖时间：**范围 0-3600 秒，温暖时间段，设备会根据服务器的上线时间逐渐的把新的请求分配给新上线的服务器。

**过载保护：**通过健康检查的 tcp 被动检查方式，触发检查动作，执行指定的过载保护动作

**配置步骤：**

1. 输入服务池**名称。**
2. 选择**健康检查。**
3. 选择**有效性。**
4. 选择**健康检查失败动作。**
5. 选择**负载均衡算法。**
6. 选择**低优先组激活。**
7. 新建**成员。**
8. 点击**提交。**

## 21.3 配置服务成员

### 21.3.1 配置服务池中服务成员

进入**服务器负载>服务池>服务成员**，点击**新建**按钮。

**地址类型：**指定添加的服务成员地址是 IPV4 或者 IPV6 地址。

**地址：**指定服务池中服务成员的 ip 地址，可以新建也可以从服务器列表中选取。

**端口：**指定服务池中服务成员的端口。自己手动定义。

**权重：**指定服务成员的权重。

**优先级组：**指定服务成员的优先级组别。

**健康检查：**指定服务成员的健康检查类型，可以选择无、自定义、继承自服务池。


**权重：**指定服务成员的权重。

**优先级组：**指定服务成员的优先级组别。

**连接限制：**指定服务成员的连接限制。

**健康检查：**指定服务成员的健康检查类型，可以选择无、自定义、继承自服务池。

**HTTP 浪涌最大并发数：**到服务器的并发数，超过该值，则启用浪涌保护。

**HTTP 浪涌平均响应时间：**服务器响应请求的平均时间，超过该值，则启用浪涌保护。

**HTTP 连接确认最大并发数：**HTTP 连接并发数超过设置的最大值后，页面返回 HTTP 连接确认页面信息。

**HTTP 浪涌队列上限：**三个优先级队列可容纳的最大请求数。

**配置步骤：**

1. 选择服务成员地址为 IPV4 或者 IPV6。

2. 选择一个已有服务器节点地址或者使用新地址。
3. 输入**端口**。
4. 输入**权重**。
5. 输入**优先级组**。
6. 输入**连接限制**。默认为 0，表示无限制。
7. 点击**提交**。

### 21.3.2 编辑服务成员

点击服务成员，进入编辑状态。


**状态调整**：指定服务成员的状态：【可用】【不可用】【强制离线】三种状态。

## 21.4 监控与维护

### 21.4.1 查看服务池

1、进入**服务器负载>服务池**，可以查看到已经配置好的服务池列表，如下

图：


2、支持名称搜索，输入名称，搜索对应的服务池。

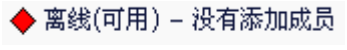

3、其状态栏表明当前服务池中的状态，具体的状态如下：


，服务池可用，表明服务池中有服务成员是可用的。


，服务池可用，表明服务池可用，但是有相关的成员是不可用的。


，服务池离线可用，表明服务池中有成员离线，服务池中服务成员不能进行调度。


，服务池未知可用，表明服务池中的服务成员健康状况未知，服务池中服务成员允许调度。




，服务池离线可用–没有添加成员，表明此服务池中无服务成员，是一个空的服务池。

### 21.4.2 查看服务池状态


### 21.4.3 查看服务成员状态

进入**服务器负载>服务池**，再点击其中某个服务池**>服务成员**，可以查看到这个服务池下配置好的服务成员列表，如下图：


其状态栏表明当前服务成员的状态，具体的状态如下：

有效(可用)，服务成员有效可用，表明服务成员健康良好，可以被调度。

有效(节点不可用)，服务成员有效（节点不可用），服务成员对应的服务器节点不可用，表示服务成员不允许调度。

有效(不可用)，服务成员有效（不可用），服务成员对应的服务器节点不可用，服务成员本身也不可用，表示服务成员不允许被调度。

离线(可用) – 成员有一个或多个健康检查失败，服务成员离线（可用），服务成员对应的节点可用，服务成员本身检查不健康，表示服务成员不允许被调度。

离线(节点不可用) – 节点离线，服务成员离线（节点不可用），服务成员对应的服务器节点不健康，服务成员本身可用，表示服务成员不允许被调度。

离线(节点不可用) – 成员有一个或多个健康检查失败，服务成员离线（节点不可用），服务成员对应的服务器节点不可用，服务成员本身不健康，表示服务成员不允许被调度。

离线(不可用) – 节点离线，服务成员离线（不可用），服务成员对应的服务器节点不可用，服务成员本身不可用，表示服务成员不允许被调度。

离线(不可用) – 成员有一个或多个健康检查失败，服务成员离线（不可用），服务成员本身检查不健康，表示服务成员不允许被调度。

未知(可用) – 成员没有配置健康检查，服务成员未知（可用），服务成员对应的服务器节点健康未知，服务成员健康未知，表示服务成员允许被调度。

未知(节点不可用) – 成员没有配置健康检查，服务成员未知（节点不可用），服务成员对应的服务器节点不可用，服务成员健康未知，表示服务成员不允许被调度。

■ 未知(不可用) – 成员没有配置健康检查，服务成员未知（不可用），服务成员对应的服务器节点不可用，服务成员不可用，表示服务成员不允许被调度。

◆ 离线(不可用) – 强制离线，服务成员离线（不可用），服务成员强制离线，服务成员不可用，表示服务成员不允许被调度。

■ 未知(可用) - 健康检查模板正在检测，服务成员未知（可用），服务成员的健康状态正在探测，结果未知，表示服务成员允许调度。

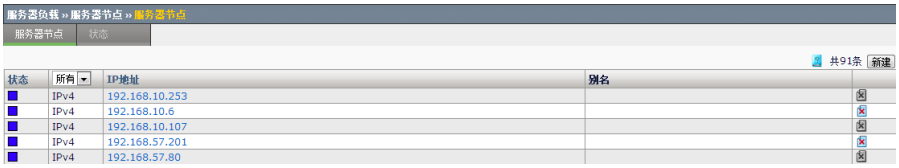
# 22 第22章 服务器节点

## 22.1 服务器节点概述

服务器节点是创建负载均衡服务池的基础，对于希望成为服务器负载服务池的服务成员的服务器，都必须首先创建一个服务器节点，即将该服务器指定为一个服务器节点，在将服务器指定为服务器节点之后，服务成员是由服务器节点加上某个端口组成，服务成员构成了服务池，所以服务器节点是服务池的基础。

## 22.2 配置服务器节点

### 22.2.1 服务器节点基本属性




**新建：** 新建一个服务池。

**删除：** 删除一个服务池。

**状态：** 显示服务池的状态。

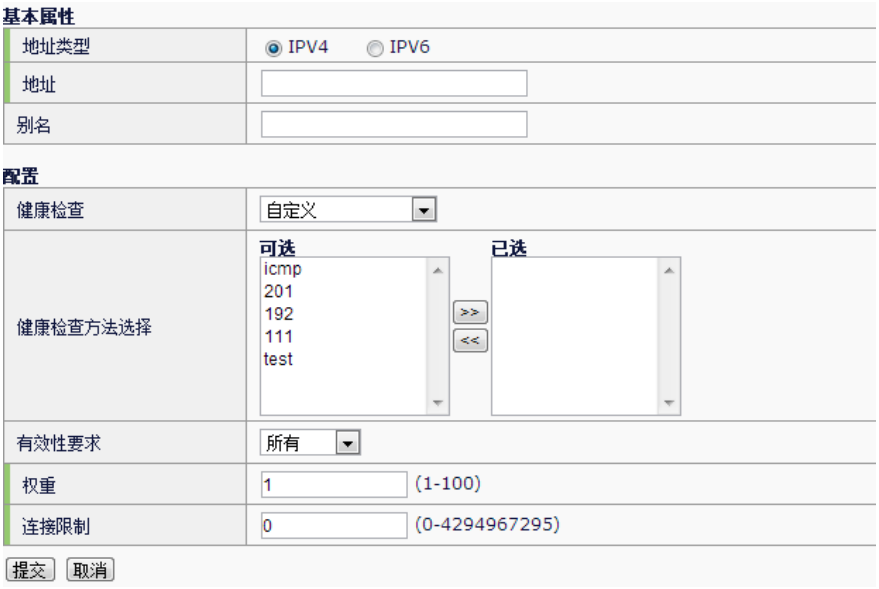
**所有：** 默认显示所有类型地址，可选择 IPV4 或者 IPV6

**IP 地址：** 显示服务器节点的 ip 地址。

**名称：** 显示服务器节点的名称。

### 22.2.2 服务器节点新建

进入**服务器负载>服务器节点**，点击**新建**按钮。




**地址类型：**选择新建服务节点的地址类型。

**地址：**指定服务器节点的 ip 地址 。

**名称：**新建服务器节点的名称。

**健康检查：**指定服务器节点健康检查类型，【无】【默认】【自定义】。默认为【无】

**权重：**指定该服务器节点的权重。默认为 1。

**连接限制：**指定该服务器节点的连接限制数量。默认为 0。

**配置步骤：**

1. 根据需要选择 IPV4 或者 IPV6。
2. 输入**地址**。
3. 输入**名称**。
4. 选择**健康检查方式**。
5. 选择**健康检查方法**。
6. 健康检查通过**个数限制**。
7. 输入**权重**。
8. 输入**连接数限制**。

### 22.2.3 编辑服务器节点

点击**服务器节点**，进入编辑状态。

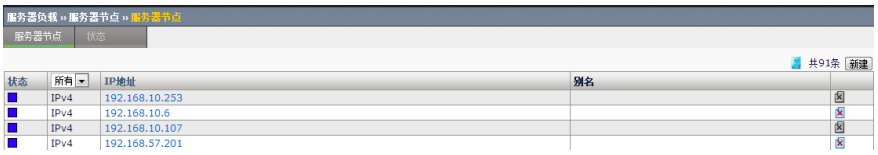

**地址类型：**显示地址类型为 IPV4 或者 IPV6。

**状态调整：**指定服务成员的状态：【可用】【不可用】【强制离线】三种状态。

## 22.3 监控与维护

### 22.3.1 查看服务器节点状态

进入**服务器负载>服务器节点**，可以查看到已经配置好的服务池列表，如下图：




：服务器节点有效，状态可用，表示服务器节点允许被调度。

：服务器节点有效，状态不可用，表示服务器节点不允许被调度。

：服务器节点离线，状态可用，表示服务器节点不允许被调度。

：服务器节点离线，状态不可用，表示服务器节点不允许被调度。

：服务器节点未知，状态可用，表示服务器节点允许被调度。

：服务器节点未知，状态不可用，表示服务器节点不允许被调度。

# 23 第23章 HTTP 模板

## 23.1 HTTP模板概述

HTTP 模板，可以帮助用户管理 HTTP 流量。用户可以根据实际需求，对进入到设备的 HTTP 流量进行全方位的管理，例如对 HTTP 头域进行各种处理。

其内容分为 HTTP 内容过滤功能、HTTP 改写功能、SSL 证书透传功能。

内容过滤功能让用户可以对 HTTP 流量内容进行检查、修改、过滤，从而实现对 HTTP 流量进行深层次管理。

改写功能基于对 http 流量的过滤匹配，让用户对 HTTP 报文头域、url、version 的内容进行改写，实现对 HTTP 报文功能的控制。

SSL 证书透传功能在 ssl 客户端卸载后，将证书信息加入 http 头域发送给服务端。SSL 透传你功能当前仅支持 HEADER 方式透传主题、序列号、有效期三个字段。

ssl 客户端卸载功能参考“第 31 章 SSL 加速”。

从功能上，可以分类为：合规检查、报文修改、重定向等。

从配置上，这部分功能属于 HTTP 模板的一部分，可以通过**服务器负载>模板>服务>HTTP** 进行配置。

## 23.2 配置HTTP模板

### 23.2.1 配置HTTP模板

**配置步骤：**

1. 进入**服务器负载>模板>服务>HTTP**，如下图：


点击名称，可以对已配置的 HTTP 模板内容进行编辑。

2. 点击**新建**,建立新的 HTTP 模板。


**名称：**设置新建模板的名称。

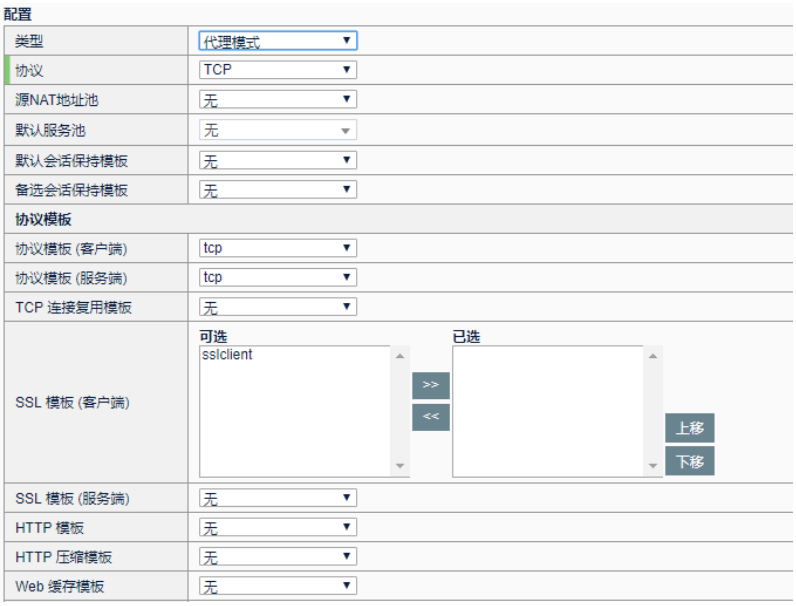
**继承模板：**下拉选择继承模板，把所选模板的配置继承下来。

例如，上图中创建了一个名称为 example_http1 的 HTTP 模板，其配置继承了系统预定义模板 http。

3. 虚拟服务中引用 HTTP 模板。

要使所配置的 HTTP 模板生效，需要在对应的虚拟服务中引用。

进入**服务器负载>虚拟服务**，在**新建**或**编辑**虚拟服务的界面中，从**HTTP 模板**的下拉列表中选择需要引用的 HTTP 模板，如下图。




提示

要使 HTTP 模板可以生效，需保证虚拟服务里的如下两项配置：类型必须为代理模式，协议必须为 TCP。

## 23.2.2 配置HTTP内容过滤功能

**配置步骤：**

1.点击**新建**或者编辑已存在 HTTP 模板，下述内容即是 HTTP 内容

过滤的配置。如下图：


**备用主机：**指定一个备用的主机地址。

没有选出可用的服务池或服务器回应错误码匹配备用主机启用条件错误码时，会使客户端转而访问该目标。


配置时，应注意带上协议类型，http 或者 https。完整的备用主机配置格式为：“http:// www.redirect.com”

**备用主机启用条件（错误码）：**指定服务器回应的错误码，当服务器回应的状态码与配置一致时，会使客户端转而访问上面配置的**备用主机**。


配置该项，必须同时配置备用主机。

这里的错误码，指的是服务器自身错误对应的状态码，一般是 5xx。

**请求头域擦除：**从请求的头域中擦除掉一个头域。输入想要擦除的头域名称，大小写不敏感。


提示

有些头域对服务器是有意义的，擦除会影响正常通信，例如 Host 等等。

有些头域对功能模块是有影响的，如压缩、缓存。

对压缩有影响的头域：User-Agent、Accept-Encoding

对缓存有影响的头域：Cache-Control、Authorization、Range、 Accept-Encoding、IF-Match、IF-None-Match、If-Modified-Since、If-Unmodified-Since、If-Range、User-Agent、Pragma 等

**请求头域插入：**向请求中插入一个头域。配置内容，必须为一个完整的头域，即是名值对的形式，如“InsertHdr: TestHeader”，注意中间要有冒号。


提示

可以与 LWS 最大列数、LWS 分隔符结合使用，可使头域的值按一定格式进行分割。

**响应头域过滤（放行）：**指定响应中允许通过的头域，其余头域将会被擦除。


提示

可配置多个，中间“,”隔开。

默认不会被擦除的头域包括：Connection、Content-Encoding、Content-Length、Content-Type、Set-Cookie、Set-Cookie2、Transfer-Encoding。

配置的头域名称是大小写不敏感的。

建议：为保证通信正常，一般应保留 Location 头域。

有些头域对功能模块是有影响的，如缓存。

对缓存有影响的头域：Cache-Control、 Authorization、Age、Date、Expires、Etag、Lase-Modified、Content-Location、Vary、Waring 等

**强制客户端 Keep-Alive：**可使客户端的连接为长连接。


提示

只针对 HTTP 1.0。

建议对应的虚拟服务启用 TCP 连接复用模板。

**重定向 HTTPS 重写：**将回应的 HTTP 重定向修改为 HTTPS 重定向。

应用场景：配置了一个 SSL 卸载的虚拟服务，此时客户端访问虚拟服务为 HTTPS 的方式，而其对应的服务器为 HTTP 方式的。当服务器回应一个重定向报文时，该重定

向肯定是 HTTP 方式的，就会导致客户端无法正确重定向，所以需要将其修改为 HTTPS 方式的。

具体配置，下拉列表项包括：

**无**：不做 HTTPS 重写

**所有**：所有重定向进行 HTTPS 重写

**与请求一致**：要求重定向的 host 与请求的 host 一致，才会重写

**IP 地址形式**：重定向为 IP 地址的形式，则重写为对应虚拟服务的地址


需要保证对应的虚拟服务启用了 SSL 卸载。

**Cookie 加密**：指定需要加密的 Cookie 名称

加密可以保证给客户端的 Cookie 不能被非法利用，而服务器看到的请求中的 Cookie 值仍然是明文

服务器回应时，对 Set-Cookie 头域中该名称的值进行加密。

客户端请求时，对 Cookie 头域中该名称的值进行解密。


配置的 Cookie 名称是大小写不敏感的。
配置多个，中间“,”隔开。
加密算法为 AES，采用编码为 Base64。

**Cookie 加密密码**：指定用来进行 Cookie 加密的密钥。

**Cookie 加密密码确认**：确认用来进行 Cookie 加密的密钥。

**最大请求头尺寸**：允许通过的一个 HTTP 请求头最大限制，包含请求行。超过该限制，会断开连接。

**Pipelining 启用**：启用 HTTP pipelining。默认开启。


HTTP pipelining 是 1.1 版本的特性，如果关闭此功能，客户端的 pipelining 请求会被设备进行流量整型，转化为非 pipelining 数据。

**X-Forwarded-For 插入：**在请求的头域中插入一个 X-Forwarded-For 头域，值为客户端的 IP 地址。

**LWS 最大列数：**插入请求头域时，所允许的最大列数。

**LWS 分隔符：**插入请求头域，当长度超过上面最大列数时，用来分隔的分隔符。可配的分隔符包括：lf cr sp，对应于换行、回车、空格。可配置多个，中间用逗号隔开。


提示

“LWS 最大列数”“LWS 分隔符”配置与请求头插入配合使用。

分隔符的不适当配置，可能会导致服务器无法正确解析。

更多 LWS 含义，可参照 RFC2616。

**长连接最大请求数：**一个 Keep-Alive 连接所允许的最大请求数，当客户端请求长连接数超过该值，会断开连接。

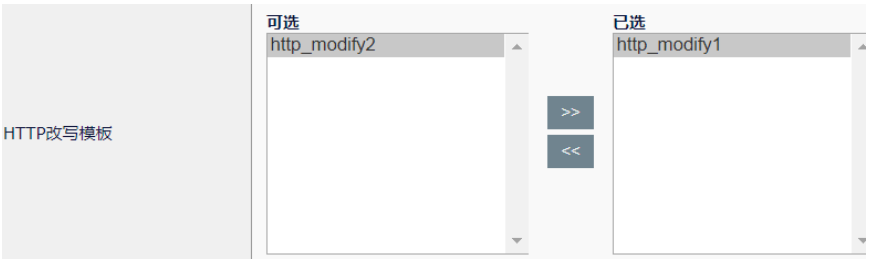
2.进入**服务器负载>虚拟服务**，将 HTTP 模板与虚拟服务关联。

具体配置方法见 HTTP 模板部分。

### 23.2.3 配置HTTP改写功能

**配置步骤：**

1.点击**新建**或者编辑已存在 HTTP 模板，下述即是 HTTP 改写的配置。从左侧栏中选择想要配置的 **HTTP 改写模板**，点击”>>”按钮，添加到右侧栏中。如下图：




2.进入**服务器负载>虚拟服务**，将 HTTP 模板与虚拟服务关联。

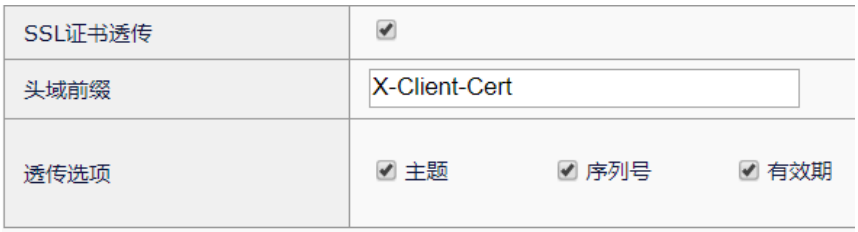
具体配置方法见 HTTP 模板部分。

HTTP 改写模板的配置见“第 27 章 HTTP 改写”。

### 23.2.4 配置SSL证书透传功能

**配置步骤：**

1.点击**新建**或者编辑已存在 HTTP 模板，将“**SSL 证书透传**”后面的选择框打勾（表示启用 SSL 透传功能）之后，系统展示展示“**头域前缀**”和“**透传选项**”如下图：



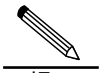

系统对于这两项分别有默认配置：**头域前缀**默认为”X-Client-Cert”，**透传选项**默认为全部勾选。

一旦 SSL 透传功能生效，在完成 SSL 卸载之后，传送给后端服务器的 HTTP 请求头体头体中将会增加用户启用的透传选项内容。默认情况下是 3 项：主题、序列号、有效期。

ssl 客户端卸载功能参考“第 31 章 SSL 加速”。

2.进入**服务器负载>虚拟服务**，将 HTTP 模板与虚拟服务关联。

具体配置方法见 HTTP 模板部分。


提示

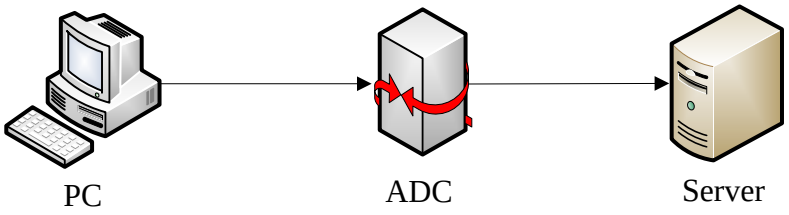
“SSL 证书透传”和“HTTP 改写”同时配置，先执行“HTTP 改写”。

## 23.3 配置案例

### 23.3.1 配置案例1：服务器返回错误码500，启用备用主机

**案例描述**

当服务器返回错误码 500 时，让客户端转而访问备用主机的地址，使得用户看到的不是错误页面。类似的拓扑如下：




**配置方法：**

1. 新建 http 模板“fallbackhost”。
2. 相关配置：

备用主机：http://www.redirect.com；

备用主机启用条件（错误码）：500

3. 虚拟服务引用该模板。

**配置步骤：**

1. 新建 http 模板，配置备用主机、备用主机启用条件（错误码）。

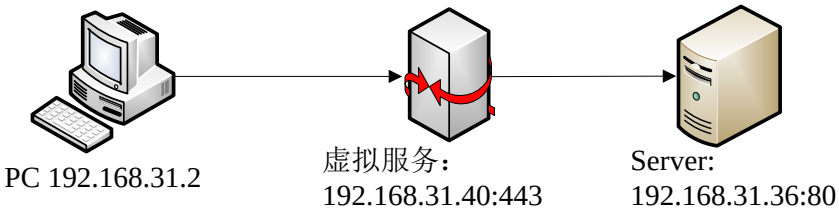

2. 在虚拟服务中引用该新建的 http 模板“fallbackhost”。


3. 浏览器访问该虚拟服务，同时使服务器回应 500 错误码。
   1. 浏览器转而访问 http://www.redirect.com。

## 23.3.2 配置案例2：以IP地址方式进行重写HTTPS重定向

**案例描述**

虚拟服务对应的目标地址为 192.168.31.40。服务器地址为 192.168.31.36，提供服务为 HTTP。通过重写 HTTPS 重定向，客户端可以正确进行重定向。拓扑如下：



**配置方法：**

1．新建 HTTP 模板“redirect”。

2．HTTP 模板相关配置：

重写 HTTPS 重定向：下拉选择“IP 地址形式”。

3．新建 ssl 客户端模板“SSL_Client”，具体配置参考对应章节。

4．虚拟服务配置：

目标地址：192.168.31.40

端口：443

服务池：Pool_Server36，对应的服务为 192.168.31.36:80

HTTP 模板：redirect

SSL 模板（客户端）：SSL_Client

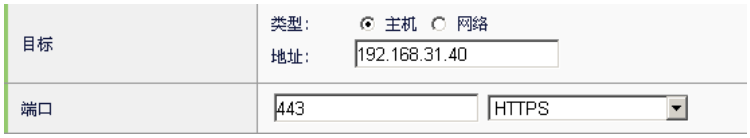
**配置步骤：**

1．新建 HTTP 模板 111，配置重写 HTTPS 重定向。


2．新建 ssl 客户端模板 123。

3．新建虚拟服务。

目标地址和端口




引用该 HTTP 模板


引用 SSL 模板（客户端）

引用服务池，需确认 Pool_Server36 包含服务 192.168.31.36:80


4．浏览器访问 https://192.168.31.40

5．后台服务器回应一个重定向报文，重定向地址类似为：
http://192.168.31.36/index.html

6．浏览器以 HTTPS 的方式正确重定向

## 23.4 常见故障分析

### 23.4.1 故障现象1：功能不正常

| | |
|---|---|
| | 配置了某些值，功能与想象中不一致，有的会导致压缩、缓存无法正常工作 |
| | 例如，配置了请求头擦除，而擦除的头域对压缩、缓存模块是有意义的。一旦擦除了，就会导致其他模块不能起作用。 |
| | 仔细查看各项配置里面的提示，重新配置。 |

# 24 第24章 快速 HTTP 模板

## 24.1 快速HTTP模板概述

快速 HTTP 模板，提供了一种可以对 HTTP 流量进行快速转发的方式。该模板，类似于 HTTP 模板，但为了流量能够更快速的转发，功能点比 HTTP 模板更为精简，用户可以根据自己的实际场景需求进行选择。

当虚拟服务启用了该模板，可以大大提高 HTTP 流量的转发效率。

## 24.2 配置快速HTTP模板

快速 HTTP，提供了快速转发 HTTP 流量的模式，同时提供了基础的 HTTP 操作功能点。

### 24.2.1 配置快速HTTP模板

1. **配置步骤：**进入**服务器负载>服务>快速 HTTP**，如下图：


**新建：**添加一个快速 HTTP 模板。

：删除掉该模板。

点击名称，可以对已配置的快速 HTTP 模板内容进行编辑。

2. 点击**新建。**


- **名称：**该模板的名称
- **继承模板：**下拉选择后，把所选模板的配置继承下来
- **配置->启用：**是否启用快速 HTTP 模板的基本配置
- **配置->最大请求头尺寸：**允许通过的一个 HTTP 请求头最大限制，包含请求行。超过该限制，会断开连接。
- **配置->长连接最大请求数：**一个 Keep-Alive 连接所允许的最大请求数，超过该值，会断开连接。
- **配置->X-Forwarded-For 插入：**在请求的头域中插入一个 X-Forwarded-For 头域，值为客户端的 IP 地址。
- **配置->请求头域插入：**向请求中插入一个头域。配置内容，必须为一个完整的头域，即是名值对的形式，如“InsertHdr: TestHeader”，注意中间要有冒号。

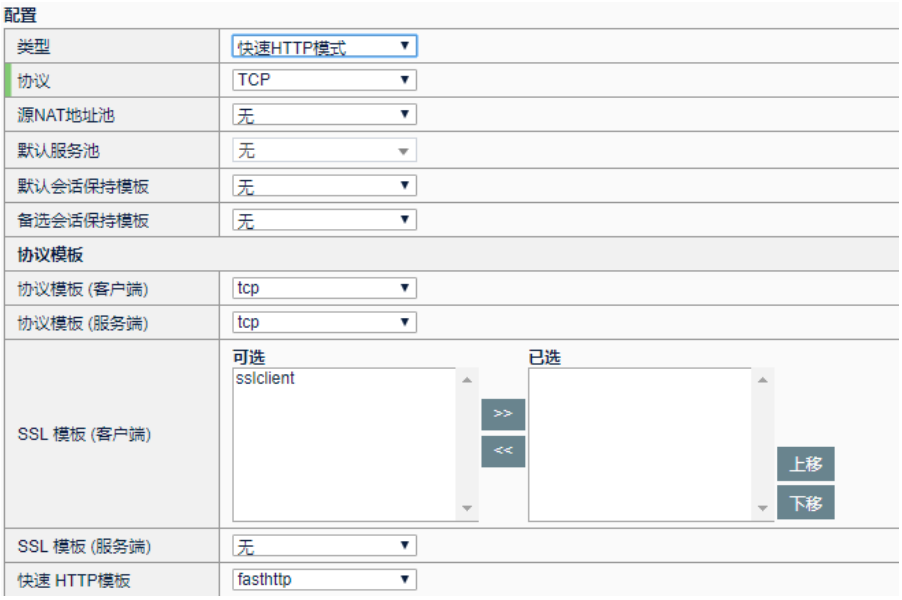

提示

插入的头放在头域的最后一行。

3. 点击**提交：**使**当前**配置生效
4. 虚拟服务中引用快速 HTTP 模板

进入**服务器负载>虚拟服务**，在**新建**或**编辑**虚拟服务的界面中，从**快速 HTTP 模板**的下拉列表中选择需要引用的快速 HTTP 模板，例如引用默认模板 fasthttp：

点击**更新**提交，这快速 HTTP 模板 fasthttp 就在虚拟服务中生效。




提示

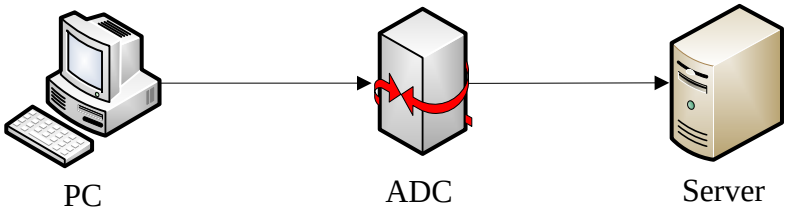
要使快速 HTTP 模板可以生效，需保证虚拟服务里的如下两项配置：类型必须为快速 HTTP 模式，协议必须为 TCP。

## 24.3 配置案例

### 24.3.1 配置案例1：最大请求头尺寸限制

**案例描述**

一般情况，服务器都要对头域做解析，如果头域超长，会增加服务器的负担。本案例设置最大请求头尺寸为 100，当请求的头域大小超过该限制时，会被断开连接。拓扑如下：




**配置方法：**

1. 新建快速 HTTP 模板 fast
2. 配置最大请求头尺寸为 100，并启用配置：
3. 虚拟服务引用该模板

**配置步骤：**

1. 新建快速 HTTP 模板，配置最大请求头尺寸，并启用。

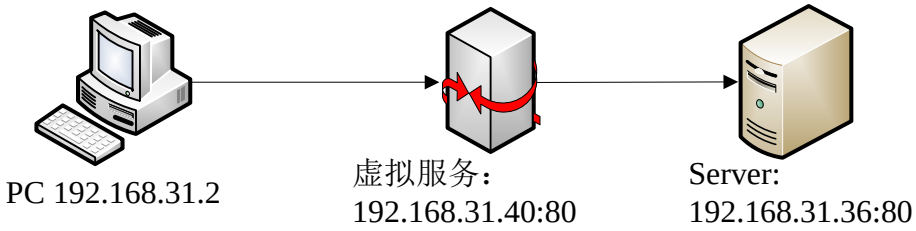

2. 在虚拟服务中引用该新建的快速 HTTP 模板 fast。


3. 浏览器发送请求，同时使请求头大于 100 字节。
4. 连接被断开。

### 24.3.2 配置案例2：插入X-Forwarded-For头域

**案例描述**

X-Forwarded-For 头域的值为客户端 IP 地址，很多服务器可以用这个值来做一些统计工作。本案例，在请求头中插入该头域，拓扑如下：



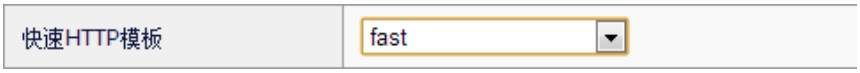

**配置方法：**

1. 新建快速 HTTP 模板 fast
2. 该模板启用 X-Forwarded-For 插入，并启用配置
3. 虚拟服务引用该模板
4. 客户端 IP 地址为：192.168.31.2

**配置步骤：**

1. 新建快速 HTTP 模板 fast，配置如下：

2. 在虚拟服务中引用该新建的快速 HTTP 模板 fast。




3. 浏览器发送请求到虚拟服务。
4. 服务器侧抓包查看，存在该头域：

   X-Forwarded-For: 192.168.31.2

## 24.4 常见故障分析

### 24.4.1 故障现象1：效率感觉没有明显提升

| | |
|---|---|
| 现象 | 虚拟服务中引用了快速HTTP模板，但是感觉转发效率没有明显提升 |
| 分析 | 首先应查看，是否启用了两个插入头域的操作，这会影响到转发效率。<br>另外，大并发量的情形下，可以通过不勾选“配置启用”来提升效率。 |
| 解决 | 仔细查看各项配置里面的提示，重新配置。 |

# 25 第25章 DNS 服务器负载均衡

## 25.1 DNS服务器负载均衡

为了均衡 DNS 服务器集群的负载，达到优化集群系统性能的目的，ADC 设备提供了 DNS 服务器负载均衡的功能，通过在虚拟服务中启用 DNS 模板，可以把对不同域名的请求分散到不同的 DNS 服务器节点上进行处理。

## 25.2 配置DNS服务器负载均衡模板

**配置步骤：**

1. 进入**服务器负载>模板>服务>DNS**，点击**新建**：


**参数说明：**

**名称：**DNS 服务器负载均衡模板名称，可以是中文。

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

**请求域名：**DNS 报文请求的域名。

**服务池：**DNS 服务池，当 DNS 请求报文同时匹配请求源地址名和请求域名时，该请求报文将被分配到指定的 DNS 服务池中。

注意

DNS 服务器负载均衡模板必须在虚拟服务中被引用，才能生效。

## 25.3 配置案例

### 25.3.1 配置DNS服务器负载均衡

**案例描述**

将域名中包含 test_a 的 DNS 请求全都分配到服务池 dns_server 中。

**配置步骤：**

1. 配置 DNS 服务器负载均衡模板 dns_balance。

进入**服务器负载>模板>服务>DNS**，点击**新建**：

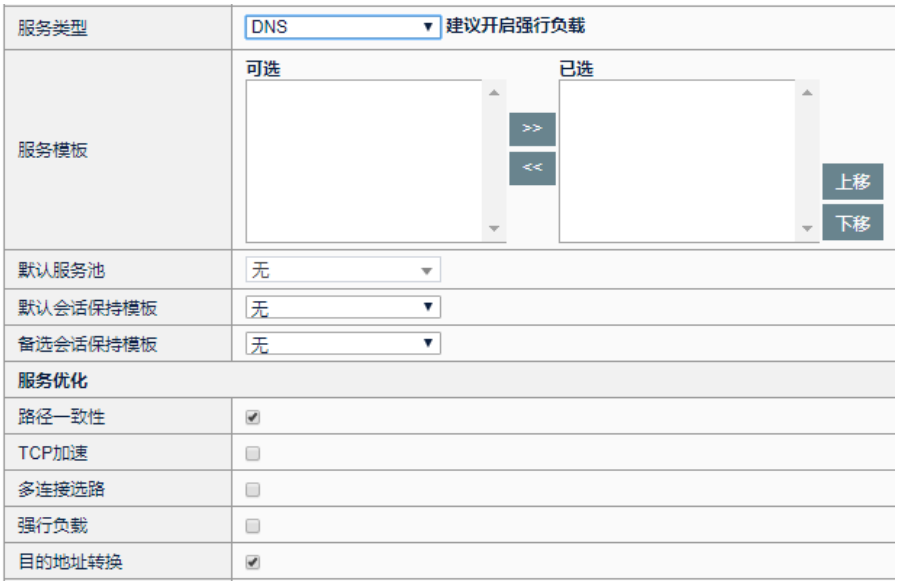

点击**提交**。

2. 在虚拟服务中引用 DNS 模板。

进入**服务器负载>虚拟服务>虚拟服务**，点击**新建**。虚拟服务配置参见相关章节。

虚拟服务的类型配置为高性能模式，协议配置为 UDP，如下图所示：


配置服务类型为 DNS，选择 DNS 模板 dns_balance，同时启用强行负载，如下图所示：




点击**提交**。

注意

DNS 服务器负载均衡模板，仅在虚拟服务的类型配置为高性能模式，协议配置为 UDP，服务类型配置为 DNS 时才能被引用。

为了保证源和目的完全相同、但请求域名不同的 DNS 请求报文可以被负载均衡到不同的 DNS 服务器，建议用户同时启用强行负载功能。

# 26 第26章 SIP

## 26.1 SIP服务器负载均衡

为了均衡 SIP 服务器集群的负载，达到优化集群系统性能的目的，ADC 设备通过指定目的端口的虚拟服务就可以提供 SIP 服务器负载均衡的功能，但在一些特殊场景下，还需要维持 SIP 请求包的源端口保持不变，或者在 SIP 数据包的消息头域中插入 VIA 字段来记录数据包经过的路径。ADC 设备通过配置 SIP 服务模板来满足这类需求。

## 26.2 配置SIP服务器负载均衡模板

**配置步骤：**

1. 进入**服务器负载>模板>服务>SIP**，点击新建：


**参数说明：**

**名称：**SIP 服务器负载均衡模板名称，可以是中文。

**插入 VIA：**在 SIP 数据包消息头域中插入 VIA 字段。当 SIP 请求包经过 ADC 设备时，在消息头域中插入形如：Via: SIP/2.0/TCP uunet.com 的 VIA 字段，用于记录请求包经过的路径，当 SIP 响应包经过 ADC 设备时，删除该字段。

**源端口保持：**SIP 数据包源端口保持。SIP 请求包经过 ADC 设备时，可能需要经过 NAT 处理，要求 NAT 转换后数据包的源端口保持不变。

2. 点击**提交**


提示

配置>Cookie，指的是 cookie 名称

配置规则时，Host 和 URI 路径是大小写敏感的，而 Cookie 名称则是大小写不敏感的。

SIP 服务器负载均衡模板必须在虚拟服务中被引用，才能生效。

# 27 第27章 TCP 协议模板

## 27.1 TCP协议模板概述

协议模板是用来配置各种协议使用的配置参数的，用户可以通过配置这些参数改变协议的行为，控制传输性能，开启或者关闭特性等。

TCP 协议模板配置主要分为三类：

1. TCP 协议各状态的超时时间配置

2. TCP 传输性能参数

3. TCP 协议特性功能开关

TCP 是一个有状态协议，为了合理利用系统资源，用户需要按照特定的情况制定各种状态的超时时间，以避免 TCP 连接长时间的占用系统资源或者过早的释放系统资源。例如：finwait 状态超时，timewait 状态超时等。

为了提高或者控制连接的数据传输效率，用户可以根据需要配置 TCP 的传输窗口，数据缓冲区等参数，以此达到控制数据传输效率的目的。例如：接收窗口，发送缓冲区等。

为了防止一些特定攻击对系统造成影响，或者在一些特定场景下提高连接的带宽利用率，TCP 协议模板提供了一些功能开关以启用或者关闭这些特定功能和特性。例如：nagle 算法，延时确认，连接延时接受等。

## 27.2 配置模板

**配置步骤：**

1.进入**服务器负载>模板>协议>TCP**，点击**新建**


**参数说明：**

**名称：**TCP 模板的名称

**继承模板：**当前模板的继承模板名称，用户可以选择从某个已存在的模板继承配置参数。

**连接空闲重置：**开启此项，允许协议栈按照配置的空闲超时时间对空闲的连接进行重置，防止出现无数据交互的连接占用资源。此功能推荐使用默认配置，默认开启。

**TIMEWAIT 连接回收：**开启此项，允许协议栈在新建连接的时候回收 TIMEWAIT 状态的连接。这样可以防止 TIMEWAIT 连接占用资源，同时可以在一定程度上提高建立连接的效率。此功能推荐使用默认配置，默认开启。

**延时确认：**开启此项，TCP 协议栈对收到的报文执行延时确认。这样可以减少网络中的 ack 报文，提高网络带宽利用率。此功能推荐使用默认配置，默认开启。

**透传最大段长度：**开启此项，服务器在建立连接的时候使用和客户端连接相同的最大段长度，默认不开启。

**透传选项：**开启此项，服务器在建立连接的时候使用和客户端连接相同的 TCP 选项，默认不开启。

**代理缓冲区低水位线：**配置代理缓冲区的低水位线，当连接接收数据低于该水位线的时候，如果连接的接收窗口被关闭，则开启接收窗口。

**代理缓冲区高水位线：**配置代理缓冲区的高水位线，当连接接收数据高于该水位线的时候，强行关闭连接的接收窗口。这样可以防止由于客户端和服务器两端传输速度不一致而导致的大量数据被缓存在接收端。

**空闲超时时间：**配置 TCP 连接的空闲超时时间。可以指定超时时间，单位为秒或者指定为无限，无限表示不超时。

**TIMEWAIT 状态超时时间：**配置 TCP 连接的 TIMEWAIT 状态超时时间。可以指定具体时间，单位为毫秒，或者指定为立即或者指定为无限。

**FINWAIT 状态超时时间：**配置 TCP 连接的 FINWAIT 状态超时时间。可以指定具体时间，单位为秒，或者指定为立即或者指定为无限。

**CLOSEWAIT 状态超时时间：**配置 TCP 连接的 CLOSEWAIT 状态超时时间。可以指定具体时间，单位为秒，或者指定为立即或者指定为无限。

**发送缓冲区：**配置 TCP 连接的发送缓冲区，发送缓冲区至少是一个最大段长度。

**接收窗口：**配置 TCP 连接的接收窗口。

**保活间隔：**配置 TCP 连接的保活时间间隔。该项控制当连接处于空闲状态时发送保活报文的时间间隔。配置可以指定为具体时间，单位是秒，也可以指定为无限，当指定为无限的时候表示不需要发送保活报文。

**SYN 报文最大重传次数：**配置 TCP 发送 SYN 报文失败时的最大重传次数。当 SYN 报文达到最大重传次数并且仍然没有收到回应，则本次连接建立失败。

**报文最大重传次数：**配置 TCP 发送除了 SYN 报文失败时的最大重传次数。当报文达到最大重传次数并且仍然没有收到回应，则认为连接已经断开，连接应该结束。

**连接延时接受：**配置该项以后当建立连接三次握手完成以后不立刻创建连接句柄，直到收到数据的时候才创建连接句柄。这样可以有效的防止“空连接”攻击，消耗系统资源。

**Nagle 算法：**配置该项以后连接启用 Nagle 算法。启用该算法会对需要发送的小数据报文进行延时发送，这样可以提高 TCP 连接的带宽占用率，但是也会导致某些场景下的数据延迟，对于实时交互式的连接不建议启用该算法。

1. 在名称一栏填写 TCP 模板的**名称**
2. 选择需要继承的 **TCP 模板名称**
3. 修改需要配置的参数
4. 点击**提交。**

## 27.3 配置案例

### 27.3.1 案例1：大数据通信场景使用的TCP模板

**案例描述**

配置一个模板，要求最大限度的保证传输速度，防止“空连接”攻击。该应用场景全部是短连接，传输数据量大，但是没有实时交互应用。

此案例主要通过增大 TCP 的窗口和缓冲区大小来尽量加快传输速度，通过改短空闲超时时间来加速不正常断开的短连接的老化时间，加速资源回收。此配置较适合大数据传输的短连接，普通的传输场景请使用默认的 TCP 模板。

**配置步骤：**

1．进入**服务器负载>模板>协议>TCP**，点击新建

2．配置参数。


3．点击提交。

提交成功后就可以在虚拟服务中引用即可。

# 28 第28章 HTTP 内容交换

## 28.1 HTTP内容交换概述

HTTP 内容交换功能，为用户提供了分发 HTTP 流量的方法。通过配置基于 HTTP 报文内容的匹配规则，可以将不同的 HTTP 数据分发到对应的服务池中。由于是基于应用层的分类方法，与 4 层的流量分发相比，可以更加细化、准确，所以更能贴近用户的实际需求。

HTTP 内容交换的匹配规则包括：

**源 IP**

**Host**

**URI 路径**

**头域**

**Cookie 名称**

匹配规则可以是完整匹配的字符串或是正则表达式匹配。

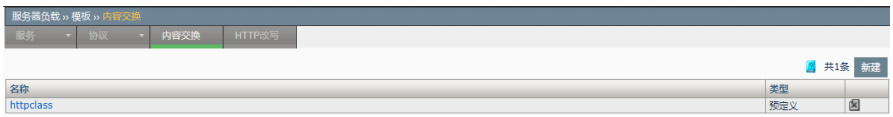
## 28.2 HTTP内容交换配置

### 28.2.1 HTTP内容交换配置

HTTP 内容交换的匹配规则是流量分发的判断依据，包括 Host、URI 路径、头域名称、cookie 名称，配置的方法类似，下面以 Host 为例。

**配置步骤：**

1. 进入**服务器负载>模板>内容交换**，如下图：




**新建：**添加一个内容交换模板。

：删除掉该模板。

点击对应的名称，可对原有的配置进行编辑。

2. 点击**新建**


**名称：**新建模板的名称

**继承模板：**选择一个已配置模板，会把已配好模板的所有配置都继承下来

**配置>源 IP：**对源 IP 进行匹配。类型包括：

**IP：**输入的可以是单个 IP，也可以是子网。支持 IPv4 和 IPv6

**地址对象：**下拉选择已经配置的地址对象。关于地址对象的配置，可以参照“地址对象”相关章节。

**配置>Host：**可选任意匹配、条件匹配

**任意匹配：**默认项，表示该项匹配是成功的，即不做处理

**条件匹配：**编辑框中输入要配置字符串内容。规则类型包括完整字符串匹配、正则匹配。

**完整字符串：**将协议解析后的内容与输入的内容进行字符串完全匹配

**包含匹配：**将协议解析后的内容与输入的内容进行字符串匹配，输入的字符串是协议解析后内容的子串，也可与之相等

**正则：**输入的内容为正则表达式，匹配时按正则的方式进行匹配。最常见的正则配置方式为后缀名，如 html、jpg 等。

输入字符串，选择规则类型后，点击添加。即在 **Host 列表**中会显示配置内容，列表中带有(regex)前缀表示当前规则为正则方式。

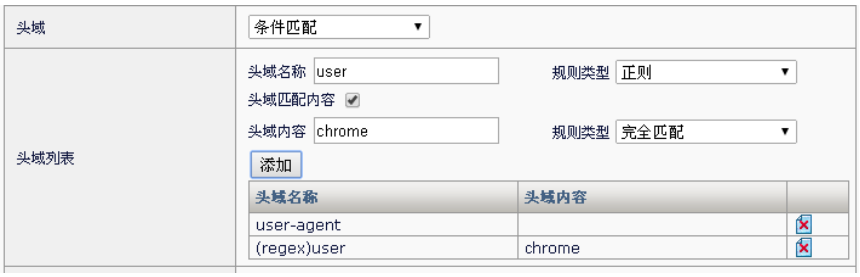
**配置>URI 路径、Cookie：**配置方式与 Host 相同

提示

配置>Cookie，指的是 cookie 名称

配置规则时，Host 和 URI 路径是大小写敏感的，而 Cookie 名称则是大小写不敏感的。

**配置>头域：**支持头域名称和头域内容的匹配。




提示

配置时，可以只配置头域名称，也可以同时配置名称和内容。

配置规则时，头域名称、头域内容是大小写不敏感的。

**动作>发送到：**包括无、发送到服务池、服务器重定向。

**动作>发送到服务池：**选中“发送到服务池”后，可在已配置的服务池列表中下拉选择

**动作>服务器重定向：**选中“服务器重定向”，可在下面的编辑框中输入服务器地址。可以将请求重定向到配置的服务器上。

**动作>服务池重定向：**选中“服务池重定向”，可在下面的下拉框选择 HTTP 和 HTTPS 协议进行重定向。可以将请求重定向到配置的服务池上。

3. 点击**提交：**使当前配置生效。

注意

Host、URI 路径、头域、Cookie，按该顺序进行匹配的。

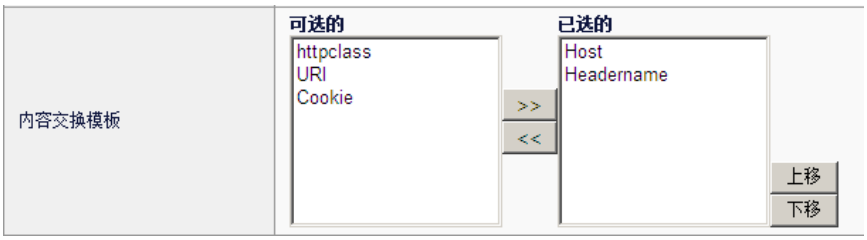
Host 规则匹配成功，才会匹配 URI 路径。URI 路径匹配成功，才会匹配头域名称。头域名称匹配成功，才会匹配 Cookie。

只要有一项匹配失败（如 Host），则该模板匹配失败。未配置服务池，该模板会匹配失败。

各项的条件匹配，其对应列表中的各条规则，只要有一条匹配成功，即该项匹配成功。

4. 虚拟服务中引用内容交换模板

进入**服务器负载>虚拟服务**，新建或编辑虚拟服务时，在**资源**中的**内容交换模板**选择即可，如下：




提示

如要该配置生效，需保证虚拟服务中同时配置了 http 模板。

一条虚拟服务中可以配置多个内容交换模板，其匹配顺序为“已选的”列表框中的自上而下的顺序。

若一个请求与某个模板匹配成功，就不会继续匹配下一个。若匹配成功，该请求会被发送到对应模板的服务池中。若对应的模板中没有配置服务池，则作为匹配失败。

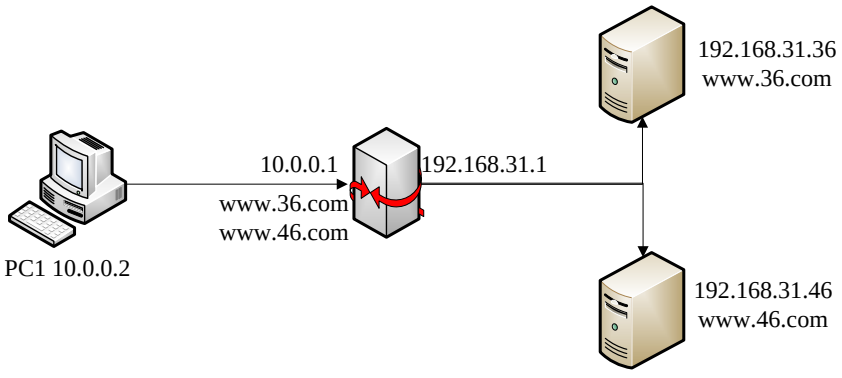
若所有的模板都匹配失败，虚拟服务则按默认服务池转发请求。

## 28.3 配置案例

### 28.3.1 配置案例1：通过Host进行流量分发

**案例描述**

通过 Host 来进行流量分发。拓扑如下：




**配置方法：**

1. 前提条件：配置一个虚拟服务，其地址为 10.0.0.1，对应两个域名 www.36.com 和 www.46.com。即访问这两个域名，都可以访问到该虚拟

服务。

2. 配置两个服务池 36、46。36 对应的服务 192.168.31.36:80,46 对应的服务 192.168.31.46:80

3. 配置两个内容交换模板，分别配置 Host 完全匹配为 www.36.com 和 www.46.com，配置对应的服务池为 36 和 46。

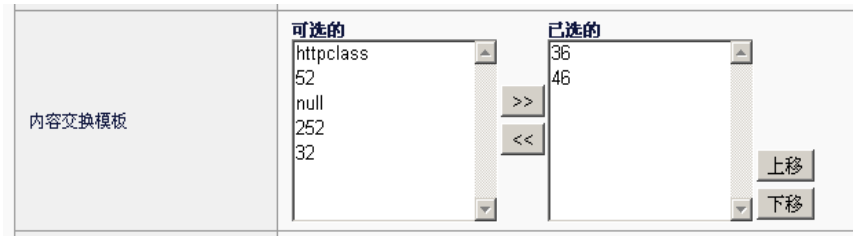
4. 在使用的虚拟服务中引用这两个内容交换模板，同时需引用 http 模板。

**配置步骤：**

1. 进入**模板>内容交换**，新建 36，如下图：


2. 进入**模板>内容交换**，新建 46，如下图：


3. 所使用的虚拟服务中引用：




4. 注意此虚拟服务必须引用了一个 HTTP 模板。

5. 通过浏览器访问 www.36.com，通过设备后可将流量定向 192.168.31.36。访问 www.46.com，可定向到 192.168.31.46。

## 28.4 常见故障分析

### 28.4.1 故障现象1：配置规则，但不能正确分发流量

| | |
|---|---|
| 现象 | 配置了对应的内容交换模板，但是无法正确访问到目标服务器 |

| | | |
|---|---|---|
| 分析 | | 有可能是以下几种情况导致的：<br>1.对应的虚拟服务中是否引用了该模板，以及是否引用了http模板<br>2.所配置的规则，完整字符串、正则的配置是否合适，同时是否配置了服务池3.http请求中是否与匹配的规则一致 |
| 解决 | | 应在虚拟服务中引用该模板，并且需同时引用了某个http模板才能生效。<br>检查配置的规则是否正确。 |

# 29 第29章 HTTP 改写

## 29.1 HTTP 改写概述

在实际的应用中，用户需要对 http 报文的头域进行修改。例如：更改报文中某个头域名称；或者对某个空白头域进行删除；再或者需要插入新的头域等等。

HTTP 改写模块用来完成上述功能。该模块实现的原理是：先根据 HTTP 改写模版配置部分的源 IP、Host、Cookie 等参数配置对流量进行过滤筛选，然后对满足这些配置的流量进行模版中动作部分的修改动作。

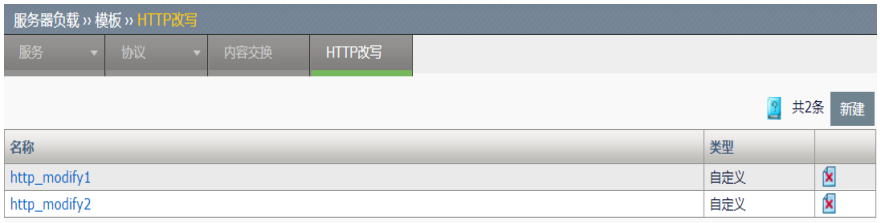
改写的类型分为请求改写和应答改写。改写类型可以在新建 HTTP 改写模版的时候进行选择，一旦对 HTTP 改写模版进行配置提交之后则不能对改写类型进行修改。

## 29.2 配置HTTP改写模板

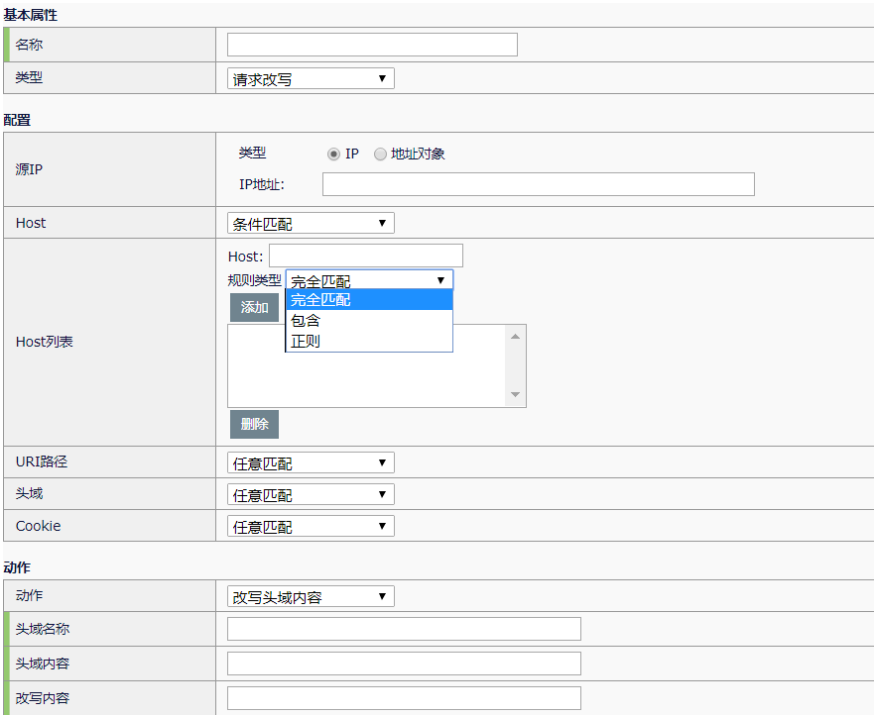
### 29.2.1 弹出新建HTTP改写模版界面

**配置步骤：**

1.进入**服务器负载>模板>HTTP 改写**。如下图所示：




2.点击**新建**,弹出 HTTP 改写模板界面。如下图所示：




**名称：**新建 HTTP 改写模板的名称，必填项。

**类型：**HTTP 改写模版的类型，分为请求改写和应答改写两种类型

**配置>源 IP：**对源 IP 进行匹配。类型分为 IP 和地址对象两种，对这两种类型的选择是互斥的。

**IP：**输入的可以是单个 IP，也可以是子网。支持 IPv4 和 IPv6。

**地址对象：**下拉选择已经配置的地址对象。当前 HTTP 改写模块仅支持对于地址节点的引用，不支持地址组对象引用。关于地址对象的配置，可以参照“地址对象”相关章节。

**配置>Host：**过滤 HTTP 报文时对报文 Host 字段的规则设定。可选项有任意匹配和条件匹配。

**任意匹配：**默认项，表示不论报文中 Host 字段是什么内容都会匹配。

**条件匹配：**编辑框中输入要配置的字符串。规则类型包括完全匹配、包含、正则。

**完全匹配：**将协议解析后的内容与输入的内容进行字符串完全匹配。

**包含匹配：**将协议解析后的内容与输入的内容进行字符串匹配，输入的字符串是协议解析后内容的子串，也可与之相等。

**正则：**输入的内容为正则表达式，匹配时按正则的方式进行匹配。最常见的正则配置方式为后缀名，如 html、jpg 等。

输入字符串，选择规则类型后，点击添加。即在 **Host 列表**中会显示配置内

容，列表中带有(regex)前缀表示当前规则为正则方式。

**配置>URI 路径、Cookie：**配置方式与 Host 相同

| | |
|---|---|
| 提示 | 配置>Cookie，指的是 cookie 名称<br>配置规则时，Host 和 URI 路径是大小写敏感的，而<br>Cookie 名称则是大小写不敏感的。 |

**配置>头域：**支持头域名称和头域内容的匹配。


| | |
|---|---|
| 提示 | 配置时，可只配置头域名称，也可同时配置名称和内容。<br>配置规则时，头域名称、头域内容是大小写不敏感的。 |

**动作：**上述**配置**中匹配成功后会执行相应的动作，详见下述章节。

| | |
|---|---|
| 注意 | Host、URI 路径、头域、Cookie，按该顺序进行匹配的。<br>Host 规则匹配成功，才会匹配 URI 路径。<br>URI 路径匹配成功，才会匹配头域名称。<br>头域名称匹配成功，才会匹配 Cookie。<br>只要有一项匹配失败（如 Host），则该模板匹配失败。<br>各项的条件匹配，其对应列表中的各条规则，只要有一条匹配<br>成功，即该项匹配成功。 |

### 29.2.2 改写头域内容

**配置步骤：**

进入**服务器负载>模板>HTTP 改写>动作**，如下图：


**头域名称：**http 报文头域的名称。

**头域内容：**http 报文改写前头域的内容。

**改写内容：**http 报文改写后头域的内容。

### 29.2.3 改写头域名称

**配置步骤：**

进入**服务器负载>模板>HTTP 改写>动作**，如下图：


**头域名称：**http 报文改写前头域的名称。

**改写名称：**http 报文改写后头域的名称。

### 29.2.4 改写完整头域

**配置步骤：**

1.改写内容部分替换

进入**服务器负载>模板>HTTP 改写>动作**，如下图：


**头域名称：**http 报文改写前头域的名称。

**改写名称：**http 报文改写后头域的名称。

**头域内容：**http 报文改写前头域的内容。

**改写内容：**http 报文改写后头域的内容。

2.改写内容全部替换

进入**服务器负载>模板>HTTP 改写>动作**，如下图：


**头域名称：**http 报文改写前头域的名称。

**改写名称：**http 报文改写后头域的名称。

**头域内容：**http 报文改写前头域的内容。

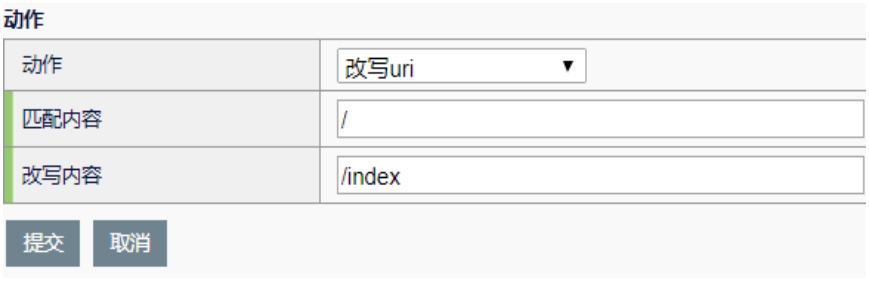
**改写内容：**http 报文改写后头域的内容。


用于匹配的头域名称和头域内容对大小写不敏感。

### 29.2.5 改写uri

**配置步骤：**

进入**服务器负载>模板>HTTP 改写>动作**，如下图：




**匹配内容：**http 报文改写前 uri 的内容。

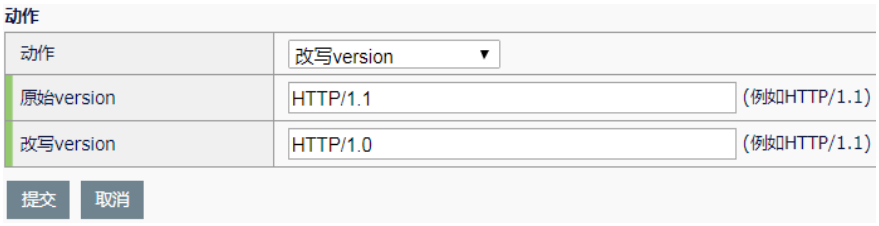
**改写内容：**http 报文改写后 uri 的内容。

| | |
|---|---|
| 注意 | 只有请求类型的 HTTP 改写模版有改写 uri 动作，因为按照 http 应答报文的格式是不存在 uri 的。 |

### 29.2.6 改写version

**配置步骤：**

进入**服务器负载>模板>HTTP 改写>动作**，如下图：




**原始 version：**http 报文改写前 HTTP 协议版本，当前支持 1.0、1.1 两个版本。

**改写 version：**http 报文改写后 HTTP 协议版本，当前支持 1.0、1.1 两个版本。

### 29.2.7 插入头域

**配置步骤：**

进入**服务器负载>模板>HTTP 改写>动作**，如下图：


**头域名称：**新插入的 http 头域名称。

**头域内容：**新插入的 http 头域内容。

### 29.2.8 删除头域

1.只配置头域名称

**配置步骤：**

进入**服务器负载>模板>HTTP 改写>动作**，如下图：


**头域名称：**要删除的 http 头域名称。

**头域内容：**配置为空。

2.配置头域名称和头域内容

**配置步骤：**

进入**服务器负载>模板>HTTP 改写>动作**，如下图：


**头域名称：**要删除的 http 头域名称。

**头域内容：**要匹配的 http 头域内容。

### 29.2.9 删除空白头域

**1.基于头域名称匹配**

**配置步骤：**

进入**服务器负载>模板>HTTP 改写>动作**，如下图：


**头域名称：**要匹配的 http 头域名称。

**2.基于全部头域名称匹配**

**配置步骤：**

进入**服务器负载>模板>HTTP 改写>动作**，如下图：

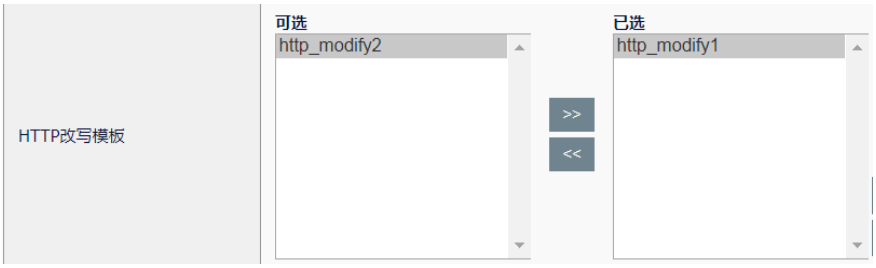


用于匹配的头域名称和头域内容对大小写不敏感。

## 29.3 HTTP模版引用HTTP改写模版

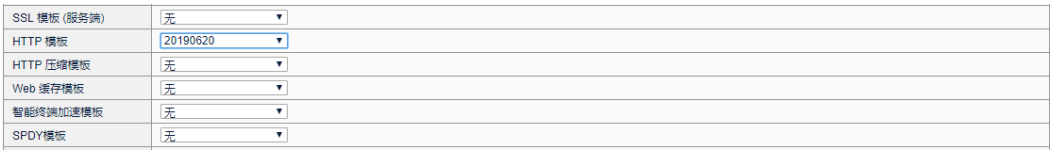
要使所配置的 HTTP 改写模板生效，需要在对应的 HTTP 服务中引用。

进入**服务器负载>模板>服务>HTTP**，在**新建**或**编辑** HTTP 服务的界面中，从左侧栏中选择想要配置的 **HTTP 改写模板**，点击”>>”按钮，添加到右侧栏中。如下图：




## 29.4 VS中引用HTTP模版

经过 29.2 小节配置 HTTP 改写模版和 29.3 小节 HTTP 模版引用之后，最终在代理模式 VS 中 **HTTP 模版**配置处对 HTTP 模版加以引用。当 HTTP 流量流经设备的时候就会按照 HTTP 改写模版的配置对报文进行处理。



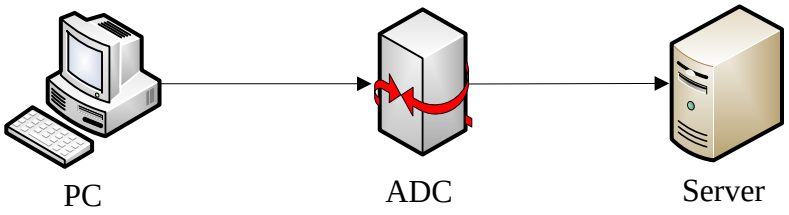

## 29.5 配置案例

### 29.5.1 配置案例1：同时修改选定头域的名称和内容

**案例描述**

用户想要删除 Cache-Control: max-age=0 头域，并新添加一条头域为 X-cache: min-time=0。

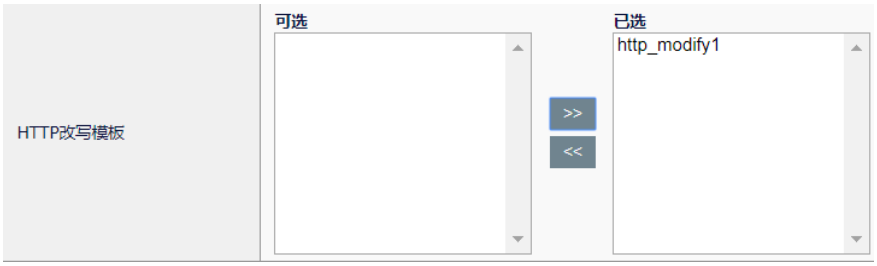
拓扑如下：



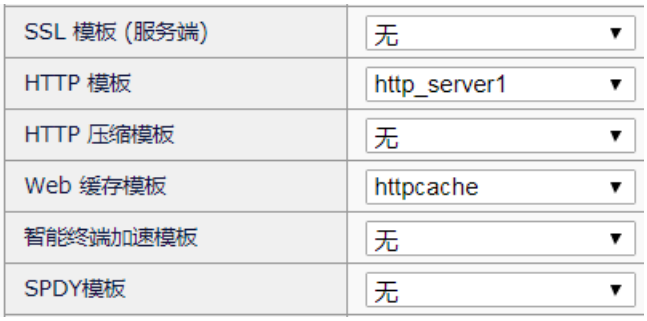

**配置方法：**

1.新建 http 改写模板“http_modify1”，如下图。


2.将 http 改写模板加入对应的 http 服务模板 http_server1。




3.在虚拟服务中引用该 http 服务模板 http_server1。



# 30 第30章 TCP 连接复用

## 30.1 TCP连接复用概述

TCP 连接复用，利用了 HTTP 的 keepalive 特性，使得来自不同客户端的 HTTP 请求，在服务器侧通过同一条 TCP 连接进行传递和响应。通过这种方式，能够减少服务器的 TCP 连接数量，降低服务器的负载，缩短 HTTP 请求的响应延迟。

应用交付控制器中，典型的 TCP 连接复用的步骤是：

1．客户端 A 和 ADC 设备建立 TCP 连接 a，并发起 HTTP 请求。

2．ADC 设备和服务器建立 TCP 连接 b，转发客户端 A 的 HTTP 请求。

3．ADC 设备将服务器的 HTTP 响应转发给客户端 A，并将连接 b 回收(detach)。

4．客户端 B 和 ADC 设备建立 TCP 连接 c，并发起 HTTP 请求。

5．ADC 设备重新使用连接 b(reuse)，转发客户端 B 的 HTTP 请求。

6．ADC 设备将服务器的 HTTP 响应转发给客户端 B，并将连接 b 回收(detach)。

ADC 设备和服务器之间能否正常进行 TCP 的连接复用，需要服务器提供的 HTTP 服务具备两个基本功能：

1．支持 HTTP 的 Keepalive，即同一条 TCP 连接可以支持多个 HTTP 访问。

2．TCP 连接保持一定的活跃时间，能够在一定的生命周期内提供 HTTP 服务。

## 30.2 配置TCP连接复用

进行一次 TCP 连接复用的完整配置，需要两个步骤：

1．建立 TCP 连接复用的模板（如果已存在符合要求的模板，也可跳过该步骤）。

2．在“虚拟服务”中引用步骤 1 建立好的模板。

### 30.2.2 建立并配置TCP连接复用模版

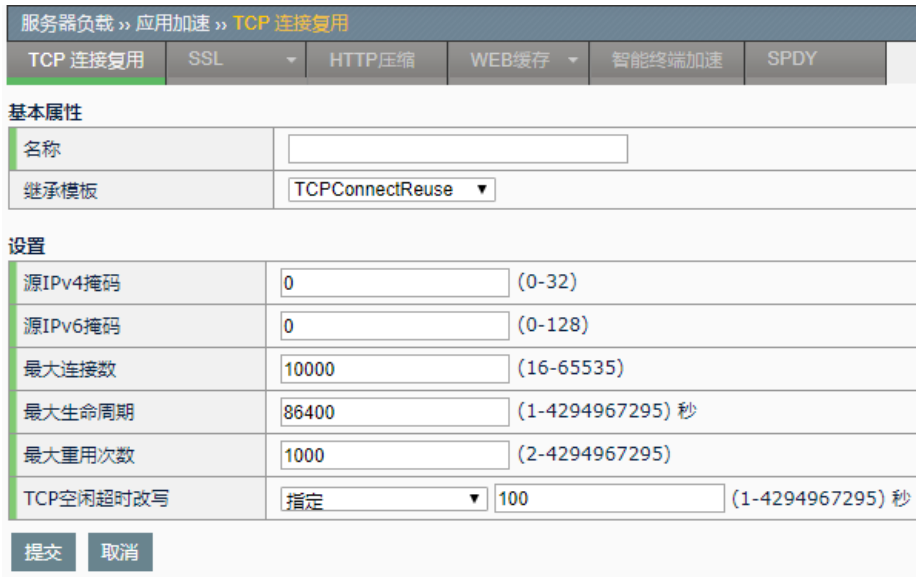
**配置步骤：**

1. 进入**服务器负载>应用加速>TCP 连接复用**，如下图：


**新建：**添加一个 TCP 连接复用模板。

：删除掉该模板。

2. 点击**新建,**添加一个 TCP 连接复用模板。




**参数说明：**

**名称：**TCP 连接复用模版的名称。

**继承模版：**创建模板时可以选择一个已经存在模版作为初始状态，以它的配置作为初始值开始配置。

**源 IPv4 掩码：**用掩码来控制什么样的客户端可以复用一条服务器侧的连接。如果配置成 0，则代表不控制，任意两个 ip 地址的客户端都可以复用一条服务器侧的连接；如果配置成为 32，则表示同一个 ip 地址的客户端才允许重复使用同一条服务器侧的连接。中间状态以此类推。

**源 IPv6 掩码：**用掩码来控制什么样的客户端可以复用一条服务器侧的连接。如果配置成 0，则代表不控制，任意两个 ip 地址的客户端都可以复用一条服务器侧的连接；如果配置成为 128，则表示同一个 ip 地址的客户端才允许重复使用同一条服务器侧的连接。中间状态以此类推。

**最大连接数量：**当一个 TCP 连接复用模板在一个虚拟服务中生效时，系统会维护一个服务器连接空闲池，服务器侧建立好的 TCP 连接都存储在空闲池中，当客户端发起访问时，系统会首先从该空闲池中挑选可用连接；当客户端访问完成之后，系统会将服务器侧的连接回收到空闲池中。这个参数限定了空闲池中的最大连接数量。

**最大生命周期：**这个参数规定了空闲池中 TCP 连接的生命周期，达到这个

时间之后，系统会主动关闭这条 TCP 连接。

**最大重用次数：**这个参数规定了一条服务器侧 TCP 连接被复用的最大次数。达到这个次数之后，系统会主动关闭这条 TCP 连接。

**TCP 空闲超时改写：**TCP 连接有空闲超时的参数(具体含义及原始配置途径请参考 TCP 协议模板相关章节)，这个参数对 TCP 连接复用模块有比较大的影响，因为如果空闲超时参数配置不合理，会导致服务器侧的连接过早老化，影响 TCP 连接复用的效率。因此本模版可以提供一个配置参数，在创建服务器侧 TCP 连接时，改写 TCP 空闲超时。参数配置含义如下：

**指定：**指定改写 TCP 空闲超时的值；

**不可用：**不改写 TCP 空闲超时。TCP 空闲超时按照 TCP 协议模板生效

**无限：**TCP 空闲超时改写为无限。

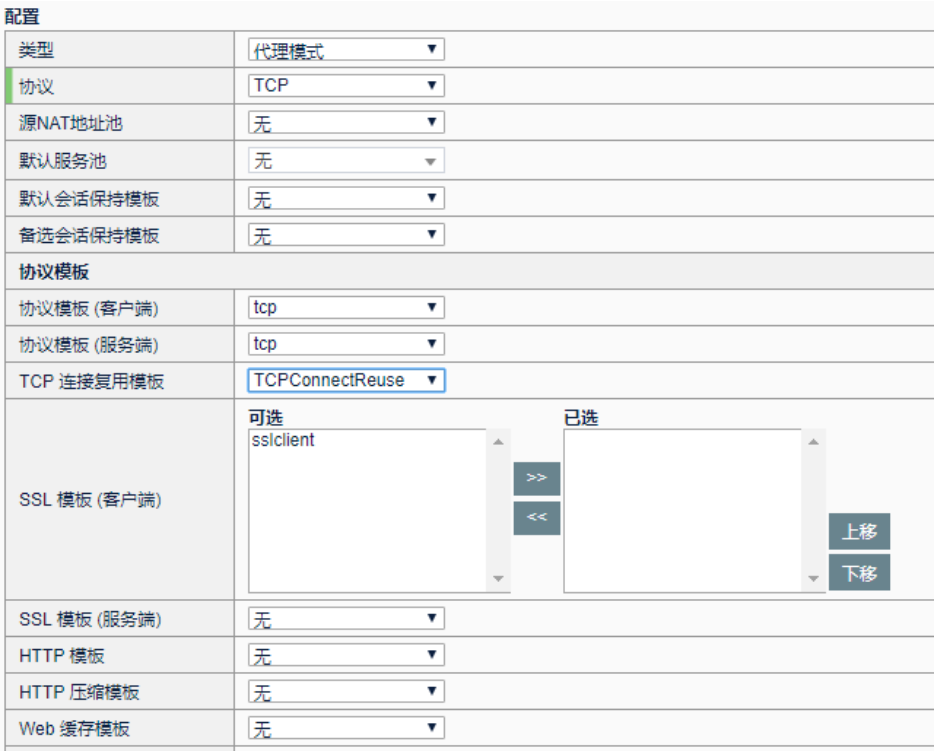
3. 点击**提交：**使当前配置生效。

### 30.2.3 在虚拟服务中引用TCP连接复用模板

**配置步骤：**

1. 进入**服务器负载>虚拟服务>虚拟服务**，如下图：


2. 选择需要引用 TCP 连接复用模板的虚 拟服务。在“TCP 连接复用模板”选项中选择建立好的 TCP 连接复用模板。




注意

1.只有类型为“代理模式”的虚拟服务才允许引用 TCP 连接复用模板；

2. 配置了“SSL 模板(服务端)”的虚拟服务不允许引用 TCP 连接复用模板；

3. 点击**提交**：使当前配置生效。

## 30.3 配置案例

### 30.3.1 配置案例：标准的TCP连接复用配置

**案例描述：**

1. 在服务器前部署 ADC 设备，为 HTTP 服务提供负载均衡业务。
2. 假设服务器群规模为 10 台，每台设计连接数量为 1000，则 TCP 连接复用空闲池上限为 10000。
3. 假设 HTTP 服务器使用 apache，其 HTTP keepAlive 参数设置为：

   MaxKeepAliveRequests 100KeepAliveTimeout 30

   那么我们的“最大生命周期”和“最大重用次数”也做相应设置。同时 TCP 空闲超时参数也做相应配置。

4. 将客户端限制为同一 24 位掩码子网才能够复用服务器侧连接。“源 IP 掩码”设置为 24。

配置如下图：

# 31 第31章 SSL 加速

## 31.1 SSL加速概述

SSL(Secure Sockets Layer 安全套接层),及其继任者传输层安全（Transport Layer Security，TLS）是为网络通信提供安全及数据完整性的一种安全协议。TLS 与 SSL 在传输层对网络连接进行加密。SSL 的加解密算法需要消耗大量的 CPU 运算，会严重影响服务器的性能。启用 SSL 加速，将 SSL 加解密的运算压力转移到负载均衡设备上，会大大减轻服务器的负担。

SSL 加速包括客户端卸载和服务器端加密功能。

SSL 客户端卸载，是指负载均衡设备充当服务器完成与客户端的 SSL 握手，并且在完成握手以后对客户端的 SSL 加密连接进行卸载，最终以明文的方式与后端服务器通信。

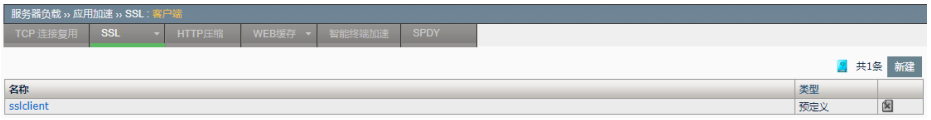
SSL 服务器端加密，是指负载均衡设备接收到客户端发送的明文后，在后端与服务器建立 SSL 连接，将客户端的明文数据加密传递给服务器端，负载均衡设备和服务器之间进行 SSL 加密通信。

SSL 客户端卸载能减轻服务器的负担，而 SSL 服务器端加密能减少 SSL 加速功能对服务器配置的影响。

## 31.2 配置SSL客户端卸载模板

**新建 SSL 客户端模版：**

进入**服务器负载>应用加速>SSL>客户端**，如下图：




**点击新建**添加一个 SSL 客户端卸载模板，


**参数说明：**

**名称：**该模板的名称。

**继承模板：**通过下拉菜单的方式选择系统已经存在的卸载模版，这个操作会把选中卸载模版的所有配置继承下来。

**证书：**必选项，下拉菜单，从证书管理中已上传的本地证书中选择一个应用于本模板的 SSL 数字证书。

**证书密码：**可选项，已选数字证书的密码，如果没有密码就保持该字段字段为空。

**证书链：**可选项，下拉菜单，从证书管理中已上传的本地证书链中选择一个应用于本模板的 SSL 数字证书链。数字证书链将作为额外证书在握手时传到对端。

**受信任的 CA：**可选项，下拉菜单，从证书管理中已上传的 CA 证书中选择一个应用于本模板的 SSL 受信任 CA。受信任 CA 将用于验证对端发送过来的数字证书。

**加密套件：**必选项，可选框表示设备支持的加密算法套件，已选框表示当前使用的加密算法套件。选择算法然后点击 >>，<< 可以将算法加入使用或者取消使用；选择算法然后点击 上移，下移 可以调整使用算法的优先级。加密套机必须选择至少一种。

**OPENSSL 选项：**设置 OPENSSL 可选项，可选项定义在下面的**使用选项列表**中，选择使用选项列表将开启**使用选项列表**中定义的可选项，选择**禁止所有选项**将禁止所有 openssl 可选项。

**使用选项列表：**设置一个 OPENSSL 选项列表，用于 **OPENSSL 选项**，可用的选项为设备支持的 OPENSSL 可选项，启用的选项为模板启用的 OPENSSL 可选项。在可用的列表中选择一项可选项点击启用把该可选项添加到使用选项列表中，在启用的列表中选择一项可选项点击不可用把该可选项从使用选项列表中删除。

部分 OPENSSL 可选项之间存在互斥关系，如果同时配置会导致连接不通。

**会话缓存大小：**设置 SSL 会话缓存的大小，大于 0 表示该模版的会话缓存功能启用，且会话缓存的总数为设置的值，0 表示该模板会话缓存功能关闭，不缓存 SSL 会话。

**会话缓存超时时间：**设置 SSL 会话缓存的超时时间。下拉菜单无限表示不限制 ssl 会话超时时间，指定表示指定超时时间，超时时间设置在选择指定以后出现的输入框中，默认为 3600 秒。

会话缓存超时时间不宜设置过长，否则会存在安全风险，推荐的超时时间为不超过 3600 秒。

**警告超时时间：**设置 SSL 告警的超时时间，SSL 告警信息发送后如果指定时间后仍没有收到对端回应，负载均衡设备将中断 TCP 连接。下拉菜单无限表示不限制 SSL 警告超时时间，指定表示指定超时时间，超时时间设置在选择指定以后出现的输入框中，默认为 60 秒。

**握手超时时间：**设置 SSL 握手的超时时间，SSL 握手开始后如果指定时间仍没有完成握手，负载均衡设备将中断 TCP 连接。下拉菜单无限表示不限制 SSL 握手超时时间，指定表示指定超时时间，超时时间设置在选择指定以后出现的输入框中，默认为 60 秒。

**允许对端重协商：**设置 SSL 会话是否允许对端发起重协商。勾选启用允许对端发起重协商，否则将在对端发起重协商时断开连接。

目前存在 SSL 重协商攻击，推荐关闭允许对端重协商。

**触发重协商时间：**设置 SSL 连接建立后，负载均衡设备主动发起重协商请求的超时时间值，当 SSL 会话持续时间超过设定值时，负载均衡设备将尝试发起重协商请求。下拉菜单无限表示不限制 ssl 触发重协商超时时间，指定表示指定超时时间，超时时间设置在选择指定以后出现的输入框中。

**触发重协商流量：**设置 SSL 连接建立后，负载均衡设备主动发起重协商请求的流量值，当 SSL 会话数据流量超过设定值时，负载均衡设备将尝试发起重协商请求。下拉菜单无限表示不限制 SSL 触发重协商流量，指定表示指定流量，流量设置在选择指定以后出现的输入框中。

**最大重协商延迟记录：**设置 SSL 连接中负载均衡设备发起重协商请求后等待对方回应前收到的 SSL 记录最大值，当对端回应记录数超过设定值而没有回应重协商请求时，负载均衡设备将关闭连接。下拉菜单选择**无限**表示不限制 SSL 的等待最大记录数，指定表示指定等待最大记录数，最大记录数设置在选择指定以后出现的输入框中。

重协商功能需要对端支持，部分客户端和服务器会关闭 SSL 重协商功能，配置 SSL 重协商可能会导致 SSL 连接中断。

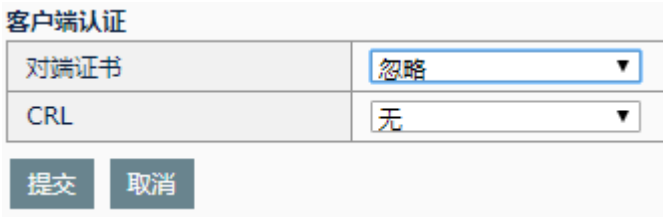
**允许 SSL 不完全关闭：**设置是否允许负载均衡设备不发送 SSL 关闭告警来关闭 SSL 连接。勾选启用允许负载均衡设备不发送 SSL 关闭告警关闭 SSL 连接，否则负载均衡设备在关闭 SSL 连接时都会主动向对端发送 SSL 关闭告警。

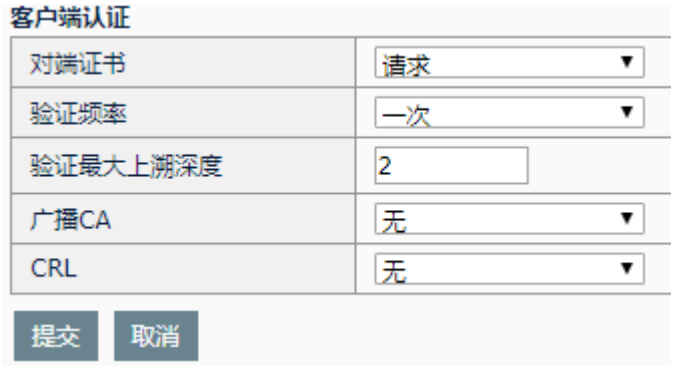
| | |
|---|---|
| 提示 | 不同版本的客户端或者服务器配置会对 SSL 连接关闭做出不同的应答。某些版本的客户端或者服务器会要求完整的 SSL 连接关闭流程，关闭该选项能防止特殊条件下连接不通的情况。 |

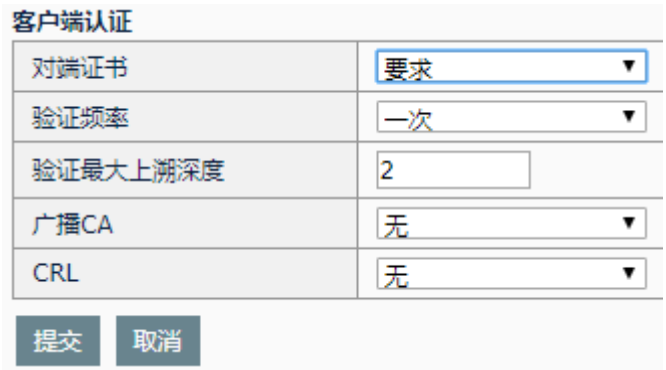
**严格会话重用：**在关闭**允许 SSL 不完全关闭**选项的情况下，启用严格会话重用将不会重用不完全关闭的 SSL 会话，否则将允许重用这些会话。

**兼容非 SSL 连接：**启用兼容非 SSL 连接将允许匹配了 VS 但非 SSL 流量通过配置了 SSL 模板的虚拟服务，SSL 模板将不对这些流量进行操作。禁用则禁止匹配了 VS 但非 SSL 流量通过。

**客户端认证：**负载均衡设备认证客户端身份配置，SSL 模板验证对端证书的方式，通过**对端证书**下拉菜单选择不同的对端认证方式。忽略代表不要求对端证书，请求代表请求但不强制要求对端发送证书，要求代表强制要求对端证书发送并验证。




**验证频率：**设置客户端认证频率，下拉菜单选择一次表示会话只验证一次，选择总是表示会话每次都需要验证。

**验证最大上溯深度：**设置客户端认证证书时上溯的最大深度，选择 0 到 9 作为最大深度，当超过设置的深度仍没有找到可信任的 CA 时将验证失败。

**广播 CA：**设置请求客户端认证时负载均衡设备附带发送的广播 CA，用于提示对端发送对应广播 CA 所签发的证书，下拉菜单，从证书管理中已上传的 CA 证书中选择一个证书作为广播 CA。

---

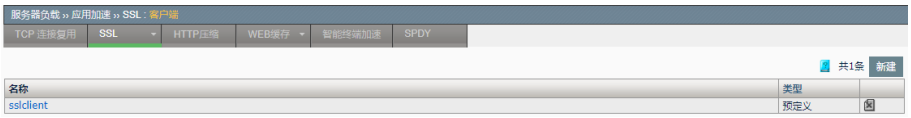
如果广播 CA 和受信任的 CA 不一致，会导致 SSL 验证对端证书失败。

---

**CRL：**设置作废证书列表，用于验证过期证书，下拉菜单，从证书管理中 CRL 证书中选择一个作废证书列表作为模板的 CRL。

**修改 SSL 客户端模版：**

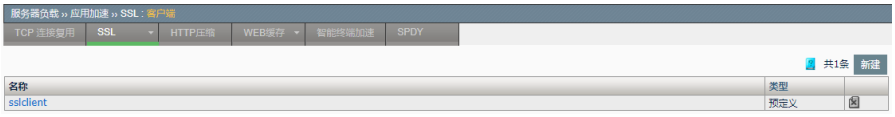
进入**服务器负载>应用加速>SSL>客户端**，如下图：




点击 ssl 客户端模版的名称，在打开的界面中修改相应的参数后更新即可。

**删除 SSL 客户端模版：**

进入**服务器负载>应用加速>SSL>客户端**，如下图：

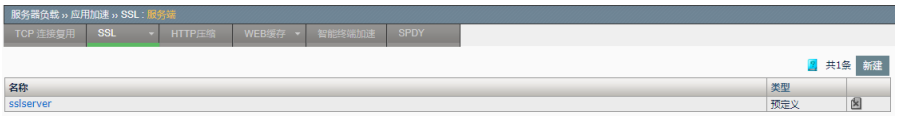



：点击即可删除，如果是，则表示 ssl 客户端模版已经被引用或者为默认的 ssl 客户端模版，不允许删除。

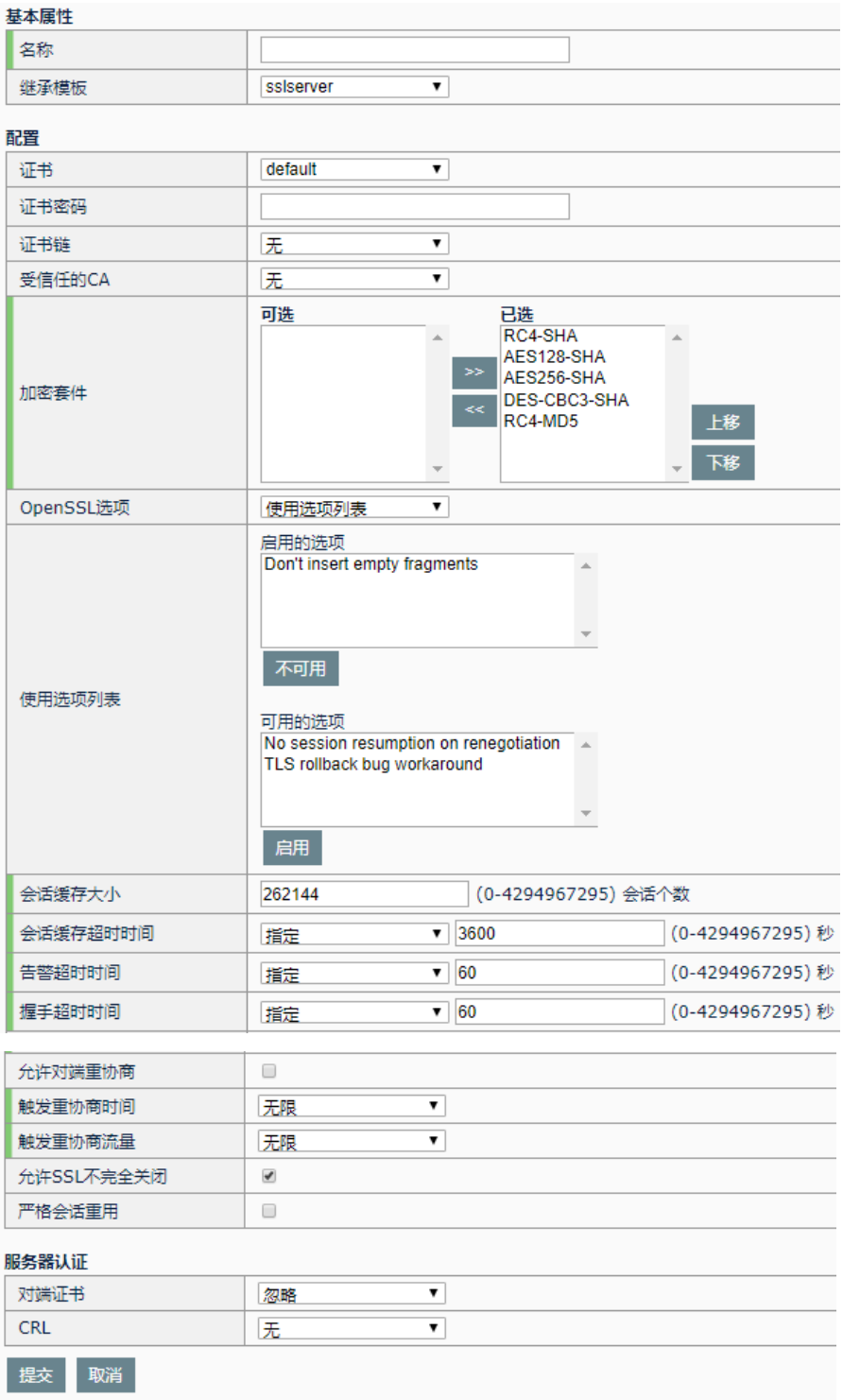
## 31.3 配置SSL服务器端加密模板

**新建 SSL 服务器端模版：**

进入**服务器负载>应用加速>SSL>服务端**，如下图：



**点击新建：**添加一个 SSL 服务端加密模板。




**参数说明：**

**名称：**该模板的名称。

**继承模板：**下拉选择后，会把已配好模板的所有配置都继承下来。

**证书：**必选项，下拉菜单，从证书管理中已上传的本地证书中选择一个应

用于本模板的 SSL 数字证书。

**证书密码：**可选项，已选数字证书的密码，如果没有密码留空。

**确认证书密码：**可选项，确认数字证书的密码，如果没有密码留空。

**证书链：**可选项，下拉菜单，从证书管理中已上传的本地证书链中选择一个应用于本模板的 SSL 数字证书链。数字证书链将作为额外证书在握手时传到对端。

**受信任的 CA：**可选项，下拉菜单，从证书管理中已上传的 CA 证书中选择一个应用于本模板的 SSL 受信任 CA。受信任 CA 将用于验证对端发送过来的数字证书。

**加密套件：**必选项，可选框表示设备支持的加密算法套件，已选框表示当前使用的加密算法套件。选择算法然后点击 >>，<< 可以将算法加入使用或者取消使用；选择算法然后点击 上移，下移 可以调整使用算法的优先级。加密套机必须选择至少一种。

**OPENSSL 选项：**设置 OPENSSL 可选项，可选项定义在下面的**使用选项列表**中，选择使用选项列表将开启**使用选项列表**中定义的可选项，选择禁止所有选项将禁止所有 OPENSSL 可选项。

**使用选项列表：**设置一个 OPENSSL 选项列表，用于 **OPENSSL 选项**，可用的选项为设备支持的 OPENSSL 可选项，启用的选项为模板启用的 OPENSSL 可选项。在可用的列表中选择一项可选项点击启用把该可选项添加到使用选项列表中，在启用的列表中选择一项可选项点击不可用把该可选项从使用选项列表中删除。

---

部分 OPENSSL 可选项之间存在互斥关系，如果同时配置会导致连接不通。

---

**会话缓存大小：**设置 SSL 会话缓存的大小，大于 0 表示该模版的会话缓存功能启用，且会话缓存的总数为设置的值，0 表示该模板会话缓存功能关闭，不缓存 SSL 会话。

**会话缓存超时时间：**设置 SSL 会话缓存的超时时间。下拉菜单无限表示不限制 ssl 会话超时时间，指定表示指定超时时间，超时时间设置在选择指定以后出现的输入框中，默认为 3600 秒。

---

会话缓存超时时间不宜设置过长，否则会存在安全风险，推荐的超时时间为不超过 3600 秒。

---

**警告超时时间：**设置 SSL 告警的超时时间，SSL 告警信息发送后如果指定时间仍没有收到对端回应，负载均衡设备将中断 TCP 连接。下拉菜单无限表示不限制 SSL 警告超时时间，指定表示指定超时时间，超时时间设置在选择指定以后出现的输入框中，默认为 60 秒。

**握手超时时间：**设置 SSL 握手的超时时间，SSL 握手开始后如果指定时间仍没有完成握手，负载均衡设备将中断 TCP 连接。下拉菜单无限表示不限制 SSL 握手超时时间，指定表示指定超时时间，超时时间设置在选择指定以后出现的输入框中，默认为 60 秒。

**允许对端重协商：**设置 SSL 会话是否允许对端发起重协商。勾选启用允许对端发起重协商，否则将在对端发起重协商时断开连接。

目前存在 SSL 重协商攻击，推荐关闭允许对端重协商。

**触发重协商时间：**设置 SSL 连接建立后，负载均衡设备主动发起重协商请求的超时时间值，当 SSL 会话持续时间超过设定值时，负载均衡设备将尝试发起重协商请求。下拉菜单无限表示不限制 ssl 触发重协商超时时间，指定表示指定超时时间，超时时间设置在选择指定以后出现的输入框中。

**触发重协商流量：**设置 SSL 连接建立后，负载均衡设备主动发起重协商请求的流量值，当 SSL 会话数据流量超过设定值时，负载均衡设备将尝试发起重协商请求。下拉菜单无限表示不限制 SSL 触发重协商流量，指定表示指定流量，流量设置在选择指定以后出现的输入框中。

重协商功能需要对端支持，部分客户端和服务器会关闭 SSL 重协商功能，配置 SSL 重协商可能会导致 SSL 连接中断。

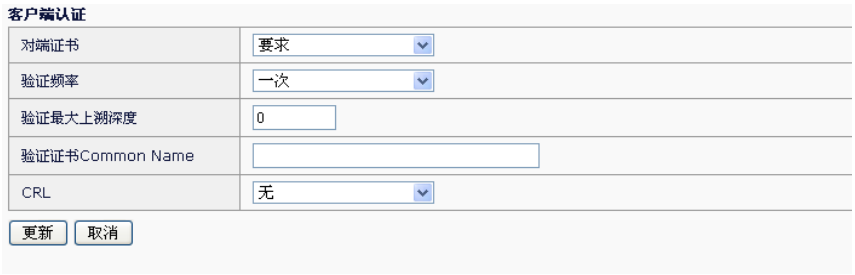
**允许 SSL 不完全关闭：**设置是否允许负载均衡设备不发送 SSL 关闭告警来关闭 SSL 连接。勾选启用允许负载均衡设备不发送 SSL 关闭告警关闭 SSL 连接，否则负载均衡设备在关闭 SSL 连接时都会主动向对端发送 SSL 关闭告警。


不通版本的客户端或者服务器配置会对 SSL 连接关闭做出不同的应答。某些版本的客户端或者服务器会要求完整的 SSL 连接关闭流程，关闭该选项能防止特殊条件下连接不通的情况。

**严格会话重用：**在关闭**允许 SSL 不完全关闭**选项的情况下，启用严格会话

重用将不会重用不完全关闭的 SSL 会话，否则将允许重用这些会话。

**客户端认证：**负载均衡设备作为客户端是被认证部分，SSL 加密模板验证对端证书的方式，通过**对端证书**下拉菜单选择不同的对端认证方式。忽略代表不要求对端证书，要求代表强制要求对端证书发送并验证。


**验证频率：**设置客户端认证频率，下拉菜单选择一次表示会话只验证一次，选择总是表示会话每次都需要验证。

**验证最大上溯深度：**设置客户端认证证书时上溯的最大深度，选择 0 到 9 作为最大深度，当超过设置的深度仍没有找到可信任的 CA 时将验证失败。

**验证证书 Common Name：**设置验证对端证书的 CN 字段，对端证书的 CN 字段与设置值不同时验证失败。

**CRL：**设置作废证书列表，用于验证过期证书，下拉菜单，从证书管理中 CRL 证书中选择一个作废证书列表作为模板的 CRL。

**修改 SSL 服务器端模版：**

进入**服务器负载>应用加速>SSL>服务端**，如下图：


点击 ssl 服务端模版的名称，在打开的界面中修改相应的参数后更新即可。

**删除 SSL 服务器端模版：**

进入**服务器负载>应用加速>SSL>服务端**，如下图：

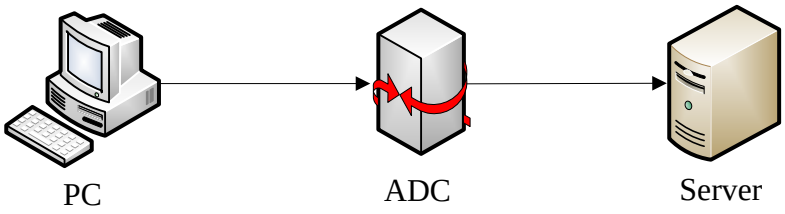
：点击即可删除，如果是，则表示 ssl 服务器端模版已经被引用或者为默认的 ssl 服务器端模版，不允许删除。

## 31.4 配置案例

### 31.4.1 配置案例：配置SSL卸载与SSL服务端加密

**案例描述**

配置 SSL 客户端卸载和 SSL 服务端加密。案例组网图如下：




**配置步骤：**

1. 新建 SSL 客户端模板。

   进入**服务器负载>应用加速>SSL>客户端**，点击**新建**，配置如下图：


2. 新建 SSL 服务端模板。

进入**服务器负载>应用加速>SSL>服务端**，点击**新建**，配置如下图：


3. 新建虚拟服务。

进入**服务器负载>虚拟服务>虚拟服务列表**，点击**新建。**


在 SSL 模板（客户端）中选择 SSL 模板 sslclient，在 SSL 模板（服务端）下拉菜单中选择 SSL 模板 server。选择一组 HTTPS 服务器作为 pool。**源 NAT 地址池**设置为自动映射。

4. 访问虚拟服务。

通过浏览器访问 https://192.168.31.49，HTTPS 流量通过设备后先被卸载，然后被加密并转发到 pool 中的各个 HTTPS 服务器。

## 31.5 常见故障分析

### 31.5.1 故障现象1：SSL认证证书失败

| | |
|---|---|
| 现象 | SSL认证对端证书失败 |
| 分析 | （1） 客户端发送的证书与负载均衡设备设置的CA不匹配。<br>（2） 客户端证书存在于负载均衡设备配置的CRL列表里。<br>负载均衡设备配置的CRL列表过期。 |
| 解决 | （1）客户端使用负载均衡设备所配置的CA颁发的有效证书。<br>（2）客户端获取新的数字证书。 |

| | |
|---|---|
| | 更新负载均衡设备配置的CRL列表。 |

# 32 第32章 HTTP 压缩

## 32.1 HTTP压缩概述

HTTP 压缩作为一种应用加速方法，主要适用于窄带宽或时延较高的网络环境。若在这种网络环境中传输大量的数据，势必会阻塞带宽导致最终用户浏览体验不佳，而 HTTP 压缩能够对数据流进行精细化的判断，压缩其中适宜压缩的数据，减少 50%到 80%的数据量，从而最大程度节省流量、加快传输速率、提升用户访问体验。

HTTP 压缩将耗费资源的压缩操作从服务器卸载到设备，实现了更加灵活的压缩选项设置，加速了服务器的业务处理能力。

HTTP 压缩如果与 HTTP 高速缓存结合使用，可以缓存压缩副本，避免了对同一请求重复性的压缩操作，进一步提高了 HTTP 压缩的效率。

从功能上，HTTP 压缩把报文的可接受压缩算法、请求 URI、客户端类型、回复体数据类型、回复体长度等信息和用户配置的策略匹配，决定是否压缩这条数据流。

从配置上，这部分功能属于 HTTP 模板的一部分，可以通过**服务器负载>应用加速>HTTP 压缩**进行配置，然后在**虚拟服务**中引用，最后在 **HTTP 压缩统计**中查看实时状态。

## 32.2 配置HTTP压缩

### 32.2.1 配置HTTP压缩

配置 HTTP 压缩

**配置步骤：**

1. 进入**服务器负载>应用加速>HTTP 压缩**：
2. 点击**新建**或者编辑已存在 HTTP 模板，其中**“压缩”**部分即是 HTTP 压缩功能的配置

HTTP 压缩的配置如下图：


- **压缩：**是否启用压缩功能，默认不启用压缩功能。

- **URI 过滤：**对 HTTP 请求的 URI 做匹配过滤，默认为“未配置”。


- **未配置**：不指定 URI 过滤。
- **URI 列表...**：列表分为“包含列表”和“排除列表”。
- **URI**：输入要包含或排除的 URI（通用资源标识符，Uniform Resource Identifier，简称"URI"）。
- **包含列表**：需要压缩的 URI 列表，如可配置压缩 txt 文件为“.*\.txt”。
- **排除列表**：不需要压缩的 URI 列表，如可配置不压缩的图片文件为“.*\.(jpg|bmp|gif|png)”。

提示

匹配使用正则匹配算法，输入的字符串请严格符合正则语法。

只有包含列表命中该 URI，排除列表未命中时才会压缩该 URI 对应的回复内容。

**URI 过滤**功能启用后，至少需要配置一项 **URI** 到**包含列表**或**排除列表**。

➢ **类型过滤**：对 HTTP 回复内容的类型做匹配过滤。默认配置“text/.*”“application/(xml|x-javascript)”到包含列表，即默认压缩文本类的回复内容。


- **未配置**：不指定类型过滤。
- **类型列表...**：列表分为“包含列表”和“排除列表”。

- **类型**：输入要包含或排除的类型。
- **包含列表**：需要压缩的类型列表，如可配置压缩文本类内容为“text/.*”
- **排除列表**：不需要压缩的类型列表，如可配置不压缩的图片文件为“image/.*”。


提示

HTTP 回复内容的类型是根据 HTTP 回复头中“Content-Type”头域判断的。

匹配使用正则匹配算法，输入的字符串请严格符合正则语法。

只有包含列表命中该类型，排除列表未命中时才会压缩该类型对应的回复内容。

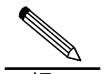
**类型过滤**功能启用后，至少需要配置一项**类型**到**包含列表**或**排除列表**。

- **压缩算法**：压缩使用的算法，支持 deflate 和 gzip 两种主流算法，默认为 gzip。


提示

按照配置优先选择压缩算法，若客户端压缩算法两种算法都不支持，则不压缩该流。

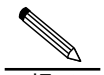
- **最小长度过滤**：http 回复体长度低于此值则不压缩。默认 1024。


提示

回复体长度是根据回复头中的“Content-Length”头域进行判断的，若回复头中无此头域，则忽略该项过滤。

压缩数据太少时压缩效果不理想，建议此值不要设置过低。

- **最大压缩缓存**：此值决定了压缩后数据的传输方式。默认 4096。


提示

若压缩后的数据长度小于该值，则通过 Content-Length 方式传输压缩后数据，否则使用 chunked 方式传输压缩后数据。

若设置过大会造成设备端缓存大量压缩后的数据，客户端可能会超时，所以此值不建议设置太高。

- **插入 Vary 头域**：是否在回复头内插入“Vary”头域。默认插入。


提示

插入该头域可使下游缓存服务器缓存压缩后数据。
若原始的 HTTP 回复头内已经有 Vary 头域并且包含“Accept-Encoding”，则不再插入该头域。

- **支持 HTTP1.0 请求压缩：**是否支持 HTTP1.0 的压缩请求。默认不支持。


提示

支持使用“Content-Length”方式的回复数据、并且该长度小于**最大压缩缓存**的 HTTP1.0 数据，可以进行压缩。

- **服务器优先压缩：**让服务器优先进行压缩，默认不启用该功能。


提示

该功能是不修改“Accept-Encoding”头域，将该头域暴露给服务器让其优先压缩，若服务器端未压缩则设备再根据配置决定是否压缩，若服务器端已经压缩则设备不再做压缩处理。

- **规避浏览器错误：**为避免触发已知的某些浏览器解压错误，不压缩这些浏览器请求对应的 HTTP 响应。默认不开启。


提示

已知的浏览器解压错误如下所示：

1. 客户端浏览器版本是 Netscape version 4.0x
2. 客户端浏览器版本是 Netscape version 4.x(4.10 版或更高)，服务器回复的 http 回复头中 Content-Type 头域未被设为 text/html 或 text/plain
3. 客户端浏览器版本是微软 IE 浏览器(任意版本)，服务器回复的 http 回复头中 Content-Type 头域被设为 text/css 或 application/x-javascript，Cache-Control 头域被设为 no-cache

- **CPU 节约：**压缩会消耗大量 CPU，设置高低阈值可以避免其占用过多 cpu 资源。默认启用。
- **CPU 节约高阈值：**当 cpu 利用率到达高阈值时不再压缩，默认 90。
- **CPU 节约低阈值：**当 cpu 利用率到达低阈值时恢复压缩，默认 75。


提示

设置高低阈值时请尽量使二者有些差距，避免发生振荡。

3. 进入**服务器负载>虚拟服务**，将 HTTP 模板与虚拟服务关联

具体配置方法见 HTTP 模板部分。

## 32.3 查看HTTP压缩实时状态

进入**系统信息>统计信息>压缩统计**，选取**统计间隔**和生效的 HTTP 模版，就可以查看实时的压缩统计信息。


## 32.4 配置案例

### 32.4.1 配置案例1：使用HTTP压缩功能

**案例描述**

使用 HTTP 压缩功能。

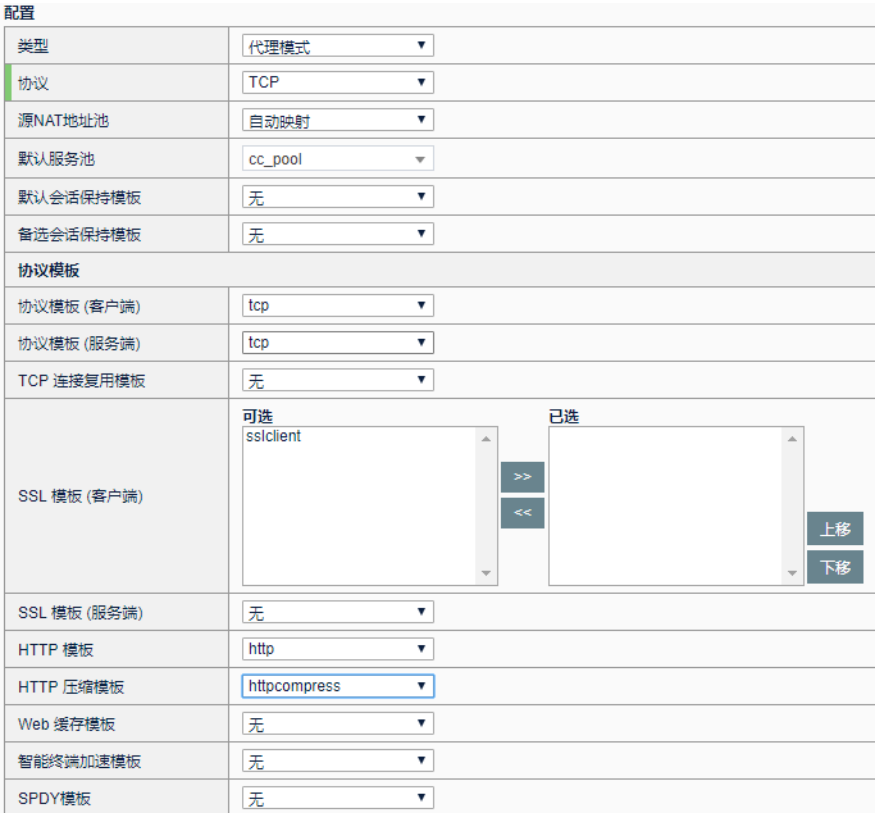
**配置方法：**

1. 新建 http 压缩模板。
2. 相关配置。

**配置步骤：**

1. 新建 http 模板，压缩配置如下图所示：


2. 在虚拟服务中引用 HTTP 模版和该新建的 http 压缩模板




## 32.5 常见故障分析

### 32.5.1 故障现象1：配置HTTP压缩后，某条流没有压缩

| | |
|---|---|
| 现象 | 配置了HTTP压缩模版并后，某条流没有压缩 |
| 分析 | 有可能是以下几种情况导致的：<br>1. 虚拟服务无法访问，或者虚拟服务没有引用该 http 模版<br>2. CPU 节约功能开启了，当前 CPU 利用率高于 CPU 节约高阈值，或者高于 CPU 节约高阈值后没有降到 CPU 节约低阈值之下<br>3. URI 匹配命中导致不压缩<br>4. 类型匹配命中导致不压缩<br>5. 回复体长度小于设置的**最小长度过滤**<br>6. 开启了规避浏览器错误选项，命中了浏览器错误<br>7. 该 http 模版**基本配置**部分配置了擦除 Accept-Encoding 头域，导致压缩算法无法识别<br>8. 请求头 Accept-Encoding 支持的算法不是配置的**压缩算法**<br>9. 压缩并发数到达上限 |

| | |
|---|---|
| | 10. 当前内存利用率已到 80%，或内存页较少<br>11. 回复头状态码不是 200，403，404<br>12. 回复是 http1.0 |
| 解决 | 1. 检查虚拟服务配置，引用该 http 模版<br>2. 等待 CPU 利用率下降，或者关闭 CPU 节约功能<br>3. 检查 URI 过滤配置<br>4. 检查类型过滤配置<br>5. 检查**最小长度过滤**配置，决定是否调低该值<br>6. 确认规避浏览器错误是否启用<br>7. 若使用 HTTP 压缩功能，请勿擦除 Accept-Encoding 头域<br>8. 修改**压缩算法**<br>9. 建议使用多台设备分流，或使用高端型号的设备<br>10. 当内存利用率下降，可用内存页增多时会压缩<br>11. 只有回复头状态码为 200 或 403 或 404 时才会压缩<br>12. 不压缩回复是 http1.0 的情况 |

# 33 第33章 Web 缓存-缓存模板

## 33.1 Web缓存概述

Web 缓存，将频繁访问的 HTTP 对象副本存储在本地内存中，当下一次相同 URI 的请求到达时，直接从内存返回用户请求的数据，从而降低服务器的请求压力和流量负载，提高服务器性能。

Web 缓存基于内存缓存，可以提高响应效率。

Web 缓存主要适用于以下场景：

- 频繁用到的对象: 站点上特定的内容在一定时期内被频繁的访问。
- 静态内容: 站点由大量静态内容组成，例如 CSS、javascript、图像或徽标。
- 压缩模块开启压缩特性: Web 缓存与压缩联合启用,减轻本系统和内容服务器的压力。

**基础模式**：Web 缓存模块判断应答是否可以被缓存基于以下条件：

- 该请求必须是一个 HTTP GET 请求
- 应答必须具有如下 HTTP 状态码：200, 203, 300, 301, 410
- 符合 RFC 缓存相关的规范

**高级模式**：Web 缓存模块判断应答是否可以被缓存基于以下条件：

- 该请求必须是一个 HTTP GET 请求。
- 符合模板引用的策略树规则。

Web 缓存会缓存服务器的原始回应体数据，但是对头数据做如下的修改：

- 删除：删除所有 cookie 头域。
- 修改：提供服务时，会根据实际情况修改部分头域，包括 Connection、Keep-Alive 和 Transfer Encoding 等
- 添加：基础模式，根据配置，添加 Date 头域和 Age 头域。

Web 缓存所有缓存对象在设备重启后清空。

可以通过**服务器负载>应用加速>Web 缓存>缓存模板**进入配置界面，Web 缓存有两种配置模式，基础模式和高级模式，详见配置 Web 缓存章节。

## 33.2 配置缓存模板

### 33.2.1 配置基础模式

**配置步骤：**

1. 进入**服务器负载>应用加速>Web 缓存>缓存模板**

点击**新建**或者编辑已存在缓存模板。

配置 Web 缓存基本参数，如下图：


- **名称:** 指定缓存模板的名称，在新建的时候指定，可接受最大 63 个字符。
- **配置模式：**指定缓存个工作模式，基础模式如果不开启 uri 强制缓存则所有缓存依据 rfc 标准执行。

**基础模式各项参数说明：**

- **最大可用内存:**指定 Web 缓存数据的可用内存最大值。缺省值为 100 兆字节。

注意

**最大可用内存**是当前缓存模板中可以用于存储 http 对象的内存大小。当高速缓存内存使用达到最大值时，系统将开始删除最早未被使用的对象。最大可用内存直接影响缓存功能的有效性，用户应该根据服务器可缓存内容大小和系统自身的内存配置一个合理的最大可用内存值。

- **最大缓存对象数量**：指定 Web 缓存中可以存在的最大条目数。缺省值

为 0，表示该模板不限制最大条目数。

- **最大生存期**：默认在多长时间内，缓存的对象视为有效。缺省值为 3600 秒。


当无法根据响应的头域计算缓存对象的过期时间时,**最大生存期**才生效。否则使用响应头域自带的生存期值。

- **缓存对象最小字节**: 指定该模板认为可以进行缓存的最小对象,缺省为 500 字节。


如果 GET 请求的 uri 配置在”永久缓存列表”或者”包含列表”中,不受此过滤条件限制。

- **缓存对象最大字节**: 指定该模板可以缓存的最大对象,缺省为 50000 字节.


如果 GET 请求的 uri 配置在”永久缓存列表”或者”包含列表”中,不受此过滤条件限制。

- **URI 过滤**：指定该模板保留或排除 Web 缓存中的特定 URI。
  - ✓ 未配置不指定特殊 URI 过滤
  - ✓ URI 列表取用 URI 列表,需要将特定的 URI 配置到指定列表中，具体配置方法见步骤 3 的 URI 过滤配置。

  缺省为“**未配置**”。

  **配置 uri 过滤**

URI 过滤可以更加灵活的控制本系统的缓存机制。在**下图**的 URI 过滤下拉选项中选 URI 列表,则出现如下图的 uri 列表配置:


在“URI”编辑框中输入想要特殊处理的 uri 字串规则（支持正则语法）,例如: www.Sina.com.cn/,然后点击”永久缓存”,”包含”,”排除”三个按钮其中的一个,将编辑框中的字串添加到相应的列表中。

- ✓ **永久缓存列表:** 如果请求的 uri 匹配该列表中的字串之一,那么该请求的响应会被强制缓存到 HTTP 高速缓存中,并且该条缓存默认是永不过期的,后续的请求命中该条缓存,则不必进行新鲜度判断,直接取用缓存中的内容做响应。

- ✓ **包含列表**: 如果用户想缓存一些通常不能被本系统缓存的 uri,用户可以将该 uri 配置到本列表中。

- ✓ **排除列表**: 通常可以被缓存，但用户不想缓存住的 URI 字串添加到本列表中,则 Web 缓存不会保存这些 URI 的响应。

注意

URI 过滤是为了强迫系统对通常不能缓存的 URI 进行缓存，或者对通常可以缓存的 URI 不进行缓存。配置了 URI 列表会降低 Web 缓存的性能,除非有特殊需要,否则不建议用户配置。

- ➢ **忽略请求的 cache-control 值**：指定启用 HTTP 缓存时，系统如何处理客户机端的 Cache-Control 头域。方法有以下三种：
  - ✓ **所有**指定系统忽略所有 Cache-Control 头域。
  - ✓ Cache-Control：max-age 指定系统仅忽略 Cache-Control：max-age
  - ✓ **无**指定系统处理所有 Cache-Control 头域。

  缺省为“**所有**”。
- ➢ **插入 Age 头域**：启用此设置时，将在缓存对象中插入 Date 和 Age 头域。Date 头域包含负载均衡系统上的当前日期和时间。Age 头域包含

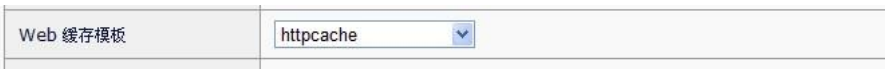
内容在高速缓存中已存在的时间长度。缺省值为启用。

- **老化速率**：指定系统以多快的速度老化高速缓存条目。老化速率的范围在 0（最慢的老化速度）到 10（最快的老化速度）之间。缺省值 0。

| | |
|---|---|
| 提示 | 老化速率的值大于 0 时,会增大 http 对象在本地已驻留时间,加快 http 对象在本系统的老化过程。<br>已驻留时间 = 实际驻留时间*2^n,n 指老化速率的值。 |

2. 进入**服务器负载>虚拟服务**，将缓存模板与虚拟服务关联。

点击要启用缓存功能的虚拟服务名称，找到协议模板这一栏，在 Web 缓存模板后的下拉菜单中选择要引用的缓存模板。如下图：




## 33.2.2 配置高级模式

**配置步骤：**

1. 进入**服务器负载>应用加速>Web 缓存>缓存模板**

点击**新建**或者编辑已存在缓存模板。

配置 Web 缓存基本参数，如下图：


**高级模式参数说明：**

- **最大缓存内存:**指定 Web 缓存的可用内存最大值。缺省值为 100 兆字节。

注意

最大可用内存是当前缓存模板中可以用于存储 http 对象的内存大小。当高速缓存内存使用达到最大值时，系统将开始删除最早未被使用的对象。最大可用内存直接影响缓存功能的有效性，用户应该根据服务器可缓存内容大小和系统自身的内存配置一个合理的最大可用内存值。

- **最小缓存对象**: 指定该模板认为可以进行缓存的最小对象,缺省为 500 字节。
- **最大缓存对象**: 指定该模板可以缓存的最大对象,缺省为 50000 字节。
- **策略树**：描述高级模式缓存动作的树形策略集合。

注意

在配置了高级模式后，如果没有引用合法的策略树，缓存将无法正常工作。

2. 进入**服务器负载>虚拟服务**，将缓存模板与虚拟服务关联。

点击要启用缓存功能的虚拟服务名称，找到协议模板这一栏，在 Web 缓存模板后的下拉菜单中选择要引用的缓存模板。如下图：


## 33.3 配置案例

### 33.3.1 配置案例1:使用缺省配置

**案例描述**

Web 缓存模板的缺省配置可以实现缓存的基本功能。

**配置步骤**

1. 新建缓存模板，设置模板名称为 http-cache-default,继承模板选择 httpcache,点击**提交**按钮保存模板。如图：


2. 在虚拟服务中引用该新建的缓存模板 http-cache-default。


•

注意

如果想进一步提高 HTTP 缓存模块的加速能力，可根据内容服务器的特性适当的更改 Web 缓存的配置。例如根据后台服务器静态文件的总数适当调大最大可用内存。根据每个文件的字节数调整缓存对象的最大和最小字节数，使系统能够尽可能多的缓存住 http 对象。

## 33.3.2 配置案例2:配置高级模式

**案例描述**

如果后台内容服务器以动态生成的文件居多，则可根据每个请求的特征和动态生成的响应特征配置缓存的高级模式。

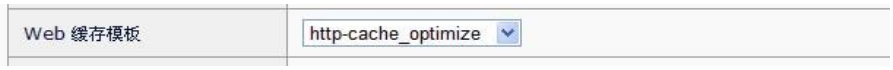
**配置步骤**

1. 新建缓存模板，设置模板名称为 http-cache-optimize。

2. 配置缓存特性:


缓存的高级模式所有的加速规则都在策略树中配置，缓存模板中指定了最大可用内存和可缓存对象的最大与最小字节数。高级模式下必须引用一个合理的策略树，否则缓存功能失效。如果当前没有可引用的策略树，请进入**服务器负载>应用加速>Web 缓存>策略树**中新建一个策略树。策略树的配置参见 Web 缓存-策略树章节。

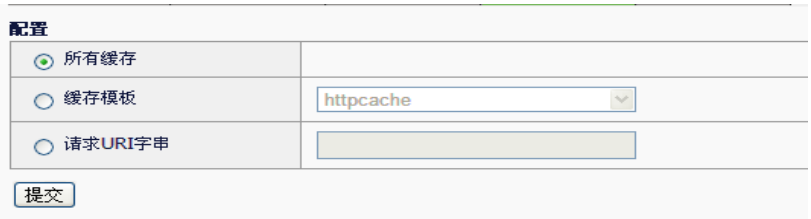
3. 在虚拟服务中引用该新建的 http-cache-optimize 模板。




## 33.4 监控与维护

### 33.4.1 清除缓存对象

进入**服务器负载>应用加速>Web 缓存>缓存手动失效**，可根据需要强制设备对本地保存的缓存副本进行清除。如下图：



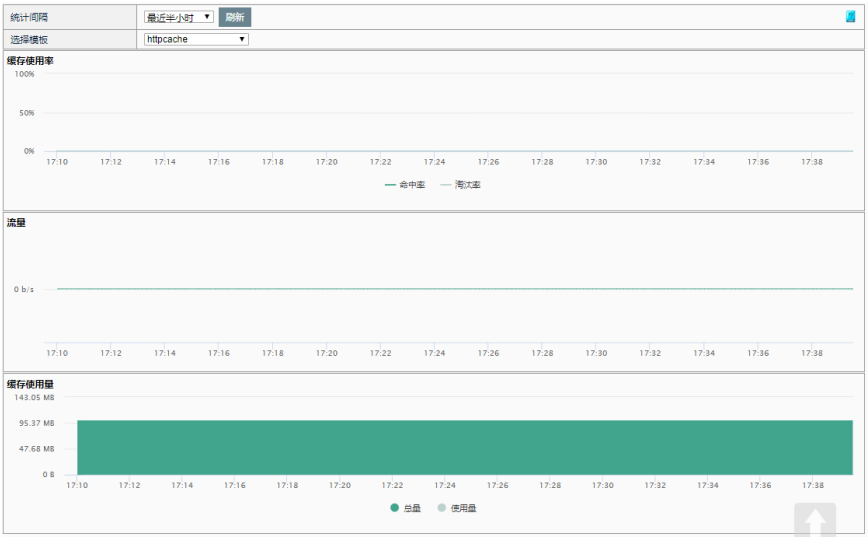

选择 **所有缓存** ，点击 **提交** ，系统中所有缓存模板中保存的缓存副本都会被清除。

选择 **缓存模板**，在之后的下拉菜单中选择要一个缓存模板名称，点击 **提交** ，则该模板保存的所有缓存副本会被清除。

选择 **请求 URI 字串** ，在之后的文本框中输入请求的 URI，字串必须包含完整的 host 和 path，点击 提交 ，则该请求对应的响应如果已存在本设备中，该响应的缓存副本会被清除。

### 33.4.2 查看Web缓存统计图

进入**系统信息**->**统计信息**->**HTTP 缓存统计**，可查看到 Web 缓存最近一段时间的统计图表。如下图：




## 33.5 常见故障分析

### 33.5.1 常见故障1：Web缓存不生效

| | |
|---|---|
| 现象 | 缓存功能启动，但是没有缓存住任何条目 |
| 分析 | 有可能是以下几种情况导致的：<br>1、 系统当前的内存使用率过高,超过了80%。<br>2、 **缓存对象最小字节**和**缓存对象最大字节**设置不合理,导致无法缓存。<br>3、 **最大可用内存**配置的太小。<br>4、 **高级模式**下没有引用策略树。<br>5、 被引用的策略树配置不合理。 |
| 解决 | 检查配置的规则是否正确。<br>如果是因为系统内存使用超过80%,则等内存使用率降低到70%后，缓存会正常启用。 |

### 33.5.2 常见故障2：启用缓存，缓存住的对象很少

| | |
|---|---|
| 现象 | 缓存功能启用,但是缓存住的条目特别少 |
| 分析 | 有可能是以下几种情况导致的：<br>1. 服务器中的http文件大部分不符合RFC中的缓存规则。<br>2. **最大可用内存**配置太小,**缓存对象最小字节**和**缓存对象最大字节**设置不合理。<br>3. 高级模式策略树配置不合理。 |
| 解决 | **基础模式**下如果服务器中的http文件大部分不符合RFC规定的缓存条件,但是用户有想让设备缓存这些文件,则可以在**uri列表的包好列表**中添加想要缓存住的uri。<br>**高级模式**，检查被引用的策略树的配置是否合理，检查配置的规则是否正确 |

### 33.5.3 常见故障3：启用缓存，命中率低

| | |
|---|---|
| 现象 | 缓存条目的命中率低 |
| 分析 | 有可能是以下几种情况导致的：<br>1. 缓存的文件不是经常被访问的文件。<br>2. **最大可用内存**和**最大缓存对象数量**值太小,导致文件不停被淘汰<br>3. **高级模式，**策略树的匹配规则和加速规则中的差异性配置不合理。 |
| 解决 | 检查配置的规则是否正确。<br>修改缓存文件的过滤条件,尽量只缓存住经常被访问的条目。<br>高级模式下，检查策略树的匹配规则和加速规则中的差异性配置。 |

# 34 第34章 Web 缓存-策略树

## 34.1 策略树概述

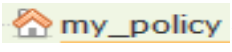
### 34.1.1 策略树介绍

Web 缓存模板高级模式中，加速规则引用的是一条配置好的策略。该策略以树形结构存在称为策略树，如下图：

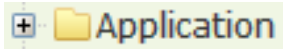

一棵策略树是一系列缓存规则的集合，以一个不多于 63 个字符的字串来命名和唯一区分一棵树。点击图中的树名称，可以进入到策略树的编辑界面如下图：


一条策略就是一颗树，它由若干的树节点生成，每个树节点包含匹配和加速两类规则。如下图，树的编辑界面分为树形展示区与右边的规则展示和配置区。规则详细信息请参考规则介绍。

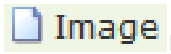
树形展示区显示当前编辑的策略树的名称和所有节点信息。图中策略树 my_policy 包含了三类节点：

- 

根节点：根节点表现为树的名称。一棵树只能有一个根节点并且该节点没有任何匹配规则和加速规则。该节点为系统根据树名称自动生成，不可更名和删除，可以在此节点下创建多个子节点；

- 

分支节点：分支节点的存在只是为了实现规则的继承性（详见规则继承性介绍）。用户创建一个分支节点并指定了匹配规则和加速规则，这样很容易可以将相同规则的参数传递给它的一个或多个叶子节点。分支节点可以拥有多个叶子节点或者分支节点。

- 

叶子节点：是匹配的最终目标，它包含父节点及所有祖先节点的所有规则，这些规则最终将请求分组，并将加速规则作用于这些分组。

### 34.1.2 规则介绍

策略树由若干的树节点组成，而每个树节点包含匹配规则和加速规则。

**匹配规则**：如下图，匹配规则包含若干的参数（parameter），这些参数属于 http 请求的字段。系统根据匹配规则的这些参数去匹配请求中的字段，例如域名，uri 路径，文件扩展名，uri 查询字段等，将请求分组。符合从根节点到某一个叶子节点的所有匹配规则的请求称为一组，该叶子节点对应的加速规则将作用于这些请求。

规则展示和配置区

**加速规则**：如下图，加速规则规定了缓存模块如何去管理每个分组的请求。每条加速规则都有与之相对应的匹配规则。一旦缓存模块根据匹配规则找到一个符合条件的叶子节点，则该叶子节点的加速规则将被使用。


一个加速规则包含以下几个结构：

- 缓存：这部分规则指定符合该节点匹配规则的请求是否要缓存，如果开启缓存能够缓存那些响应状态码。
- 差异性：差异性规则包含若干参数（parameter）对象，这些参数存在于 http 请求头域中。他们用于标识响应的 Web 页面中可能包含的不同内容。缓存模块提取这些参数对象的值用来作为每个缓存对象的唯一标示符。差异性规则可以控制系统对同一个请求的 uri 保存不同的副本。列如，缓存模块可以用 cookie 这个参数对象对不同用户的请求提供特定的缓存副本。

- 生存期：生存期规则指示系统在缓存过程中是否使用原始的缓存相关头域。如果原始头域中没有缓存时间相关指示，生存期规则将制定缓存副本在系统中停留的最大时间。生存期规则还将指定浏览器端的缓存参数。
- 失效触发器：失效触发器是用来自动对某些缓存对象失效。用户在创建一个失效触发器的时候，必须指定触发失效规则的请求条件和将要失效的缓存对象的特征。

每一个匹配规则对应着一个加速规则，他们共同构成一个树节点的结构。一个请求到达时，从树的根节点开始逐层对这个请求进行匹配，直到一个叶子节点，然后根据叶子节点对应的加速规则对该请求进行加速处理。除了加速规则中的失效触发器外，其余的规则都具有继承性，请参考规则的继承性介绍。

### 34.1.3 请求相关参数介绍

匹配规则，加速规则中的差异性和失效触发器配置都是由请求头域中的字段组合而成，这些特殊的字段我们称之为参数（parameter），可用于规则配置的参数包括：Protocal，Host，Path Segment，Extension，Query parameter，Cookie，User Agent，Referror，Header。

参数类型说明

**Protocal**：HTTP 请求使用的协议，如：
http://www.venustechnetworks.com/index.aspx

使用的协议为 http。

**Host**：http 请求中的 host。如：
http://www.venustechnetworks.com/index.aspx

host 值为 www.venustechnetworks.com。

**Path Segment**：PathSegment 是指请求 URI 中的 path 部分，它在请求的 host 之后，其余查询参数之前，如
http://www.venustechnetworks.com/index.aspx，

http://www.venustechnetworks.com/templates/H_list/index.aspx?nodeid=47

这两个 uri 的 path 分别是/index.aspx，/templates/H_list/index.aspx。

**Extension**：请求中文件的扩展名，如
http://www.venustechnetworks.com/index.aspx，
http://www.baidu.com/images/down.jpg，这两个请求的扩展名分别为 aspx，jpg。

**Query parameter**：在 uri 中 pathsegment 之后的形如 name=value 的参数，value 可为空，如：

http://www.venustechnetworks.com/templates/H_fangan/index.aspx?node

id=125

查询参数 nodeid=125 。

**Cookie**：请求中的 cookie 头域值，cookie 名称和 cookie 值，值可为空，如：

Cookie：userid=123\r\n 名称是 userid，值为 123。

**User Agent**：请求头域中的 User-Agent 头域。

**Referror**：请求头域中的 Referror 头域。

**Header**：请求头中除了以上定义过类型的其他头域。

参数是策略树规则的重要组成部分，参数配置的合理性直接会影响到缓存功能正常与否。每个参数由类型，名称，属性，成员组，四个部分构成。

### 34.1.4 规则的继承性

一个叶子节点可以继承根节点和分支节点的规则，这样用户可以快速的创建多个叶子节点，它们包含了从根节点到父节点的所有规则。如果用户在分支节点重写或者新建一项规则，系统会将这项规则分发到该分支节点的所有子孙节点中。

规则的继承：在一个分支节点下新建一个叶子节点，该叶子节点会继承父节点的规则属性。比如有一个父节点 Home 匹配规则中有 Host 和 Path 两个参数对象。在 Home 节点下新建一个叶子节点 Imge，该叶子节点的匹配规则中也有 Host 和 Path 两个参数对象，并且参数列表中的这两个参数时不可删除的。要删除这两个参数对象必须找到创建它们的根节点或者分支节点，在根节点或者分支节点中删除。用户也可以在叶子节点中新建参数对象，比如 Extension。此时刷新参数列表发现多了 Extension 参数对象并且该对象时刻删除的。除了匹配规则和差异性参数的继承特性外，缓存标签和生存周期标签中的配置也具有这个特性。

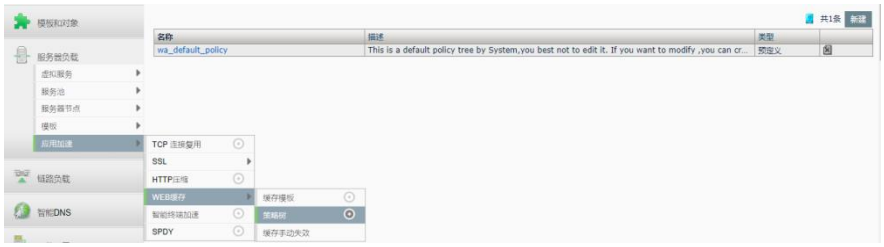
规则的重写：在叶子节点编辑一个从父节点继承来的规则参数时，可以修改该参数的值和其他一些相关属性，这个过程称之为规则的重写。值得注意的是，当用户在分支节点重写一个参数对象时，重写的值会分发到它的所有子孙节点。除非用户确定这个重写适用于所有的子节点，否则建议在叶子节点进行重写操作。除了匹配规则和差异性参数的继承特性外，缓存标签和生存周期标签中的配置也具有这个特性。

## 34.2 配置策略树

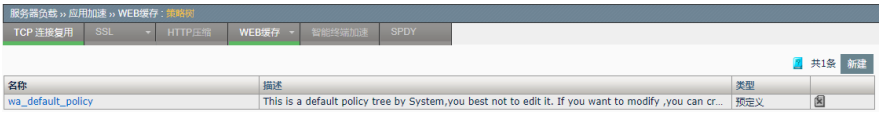
### 34.2.1 新建策略树

**步骤：**

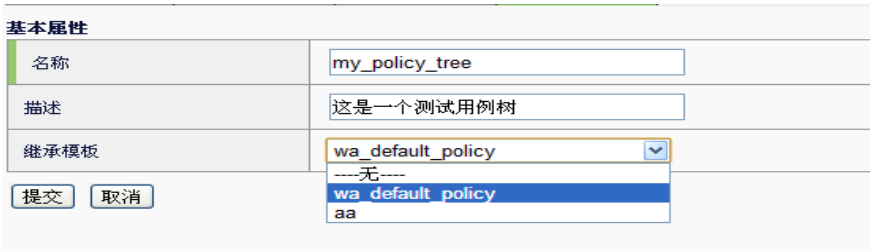
1 .创建一棵策略树：如下图，进入到策略树菜单下：




2. 点击下图策略树列表右上角的新建按钮。




3. 在新建界面中输入策略树的名称和描述，如下图，点击提交，创建策略树完成




**参数说明**

名称：策略树的名称，最多可输入 63 个字符。

描述：这棵策略树的一些用途，创建时间和创建者等说明。

继承模板：继承模板下拉菜单中显示系统已有的策略树，选择一个策略树的名称，则新建的策略树的节点名称和规则会完全从模板中拷贝过来。

## 34.2.2 树节点操作

用户新建了一个树，如果没有选择模板，则会生成一棵只有根节点的空树，点击策略树列表中的名称，进入到树的编辑界面，如下图：


图 2.2.2-1

点击这个根节点名称右边的加号浮标可以新建一个节点。依次新建如下图的节点

图 2.2.2-2

选择一个节点，节点名称右边会有该节点支持的一系列操作浮标分别是：

 添加：为该节点添加一个叶子节点，叶子节点继承该节点的所有属性。

 重命名：可以修改该节点的名称。

 删除：删除该节点和它的所有子孙节点。

 上移：向上移动一个位置。只能在同一个父节点中上移，如果已经是父节点的第一个孩子节点，则没有该操作。

 下移：向下移动一个位置。只能在同一个父节点中上移，如果已经是父节点的最后一个孩子节点，则没有该操作。

 警告：改节点的匹配规则和父节点的匹配规则完全一致，需要修改。

创建完一棵树和它的节点后，可以对树节点的规则进行配置，首先是匹配规则。

### 34.2.3 匹配规则的配置

当系统有请求进入缓存模块的时候，缓存模块会提取 http 请求头域中的信息，并将这些信息与用户配置的匹配规则进行逐一的匹配，通过策略树的不同分支节点将 http 请求分组，匹配过程中必须定位到一个叶子节点并且满足该叶子节点的所有参数规则，否则认为该次匹配不成功。对于没有匹配到叶子节点的请求，系统会直接将该请求转发到后台的内容服务器。点击一个树形展示区中的节点，则该节点的所有匹配规则会显示在右边的规则展示区中，如下图选择 Home 节点。点击下图列表的名称字段，可以编辑已有参数的成员。


表格中显示 Home 匹配规则中已有的参数 Host 和 PathSegment，点击**选择参数**下拉菜单，可以查看可用的其余的参数。

添加一个新的参数，在**选择参数**下拉菜单中选择一个参数类型，比如 QueryParameter，点击按钮**添加**，弹出如下图的参数配置界面：


**参数说明**

**类型：**参数的类型，这个字段在选择参数的时候，系统就已将默认，用户不可更改。

**名称：**参数的名称，支持不多于 63 个字符的输入。除了 queryparameter，cookie，和 header 三个类型的参数外，其余的参数名称由系统默认。参数的名称只认可完全相等的字串，*代表全部，其余的字符都当做字面字符处理。列如有个请求为：http://venustechnetworks.com/templates/H_content/index.aspx?nodeid=179&page=CoContentPa&contentid=12 添加这个匹配规则中的 QueryParameter 时，名称是*，则指整个查询字段 nodeid=179&page=CoContentPa&contentid=12，或者只能添加名称为 nodeid 或者 page 或者 contentid 这个三个，其余的配置都不可能与这个请求匹配成功。

**成员：**一个参数只能有一个类型和名称，但是可以有多个成员，每个成员由匹配结果，匹配算法，匹配字串三个部分组成。这个三个部分互相依赖，改变任何一个都可能影响最终的结果。

**匹配结果：**匹配结果可以选择匹配或者排除。

**匹配算法：**匹配算法可以选择正则，包含，完全等于，开头等于，结尾等于。

**匹配字串：**用来和请求中的特定字段做比较的字符串。

参数的成员之间是或的关系，成员表中位置靠上的优先匹配。可以选择成员表中的字串，点击上移或者下移，改变成员的匹配优先级。

### 34.2.4 加速规则—缓存的配置

缓存标签页提供用户配置节点的缓存开关和将要缓存的响应状态码。默认缓存开启，并只缓存 200，201，203，207。该页面的规则可继承，所以用户最好是在叶子节点修改这个标签页的规则。选中 Home 节点，在右边的的标签栏中的下拉菜单选择**加速规则**，则出现如下图的缓存配置：


**参数说明：**

**启用：**缓存控制开关，默认开启并强制开启 200 系列的回应为可缓存状态码。如果关闭，则匹配到该节点的请求不能用本地缓存来响应也不缓存该请求的服务器响应。

**缓存状态码：**控制可缓存的状态码。

### 34.2.5 加速规则—差异性配置

每个缓存对象结构中都有一个唯一的识别码，简称 UCI。UCI 通常是请求头的一些字段的组合，当有后续的 http 请求到达，使用 UCI 和请求中的字段做比较，这样确保给每个请求回应正确的副本。加速规则中的差异性配置就是为了让用户可以修改和完善缓存过程中创建 UCI 用到的元素。缓存模块默认的 UCI 字段是每个请求的 Host 和 Path，如果加速规则中存在差异性配置，则差异性参数将被作为 UCI 的元素。每个叶子节点的差异性规则是若干个参数组合而成，这些参数可以是这个节点新建的也可以是从祖先节点继承来的。

一个缓存的流程大致如下：

1. 缓存模块接到一个 HTTP 请求，根据匹配规则匹配到策略树中的一个叶子节点。

2. 检查这个叶子节点加速规则中的差异性配置，如果这个叶子节点有差异性规则，模块就会遍历规则中的每个参数设置，检查该请求相关的字段是否需要用于 UCI 创建。

3. 缓存模块根据默认的 Host 和 Path 字段以及差异性规则生成一个 UCI。

4. 缓存模块根据这个 UCI 去查找 hash 表，如果查找到一个具有相同

UCI 的缓存副本并且是非过期的则用这个缓存副本对请求做响应。如果没有查找到，缓存模块会根据加速规则的配置判断是否用这个 UCI 创建一个新的缓存对象。

差异性配置界面如下图，点击列表名称字段可以编辑已有参数成员。


表格中显示 Home 匹配规则中已有的参数 Host 和 PathSegment，点击**选择参数**下拉菜单，可以查看可用的其余的参数。

添加一个新的参数，在**选择参数**下拉菜单中选择一个参数类型，比如 Cookie，点击按钮**添加**，弹出如下图的参数配置界面：


**参数说明：**

**类型：**参数的类型，这个字段在选择参数的时候，系统已将默认，用户不可更改。

**名称：**参数的名称，支持不多于 63 个字符的输入。除了 queryparameter，cookie，和 header 三个类型的参数外，其余的参数名称由系统默认。参数的名称只认可完全相等的字串，*代表全部，其余的字符都当做字面字符处理。列如有个请求为的头域中出现 Cookie：username=aaa；sessionid=123\r\n 名称是*，则指整个 Cookie 字段 username=aaa；sessionid=123，或者只能添加名称为 username 或者 sessionid 两个，其余的配置都不可能与这个请求的 cookie 字段匹配成功。

**成员：**一个参数只能有一个类型和名称，但是可以有多个成员，每个成员由匹配算法，保存副本，匹配字串三个部分组成。这三个部分互相依赖，改变任何一个都可能影响最终的结果。

**匹配算法：**匹配算法可以选择正则，包含，完全等于，开头等于，结尾等于。

**匹配字串：**用来和请求中的特定字段做比较的字符串。如果匹配算法是正则，则该字串代表正则表达式，否则理解为字面字符。匹配算法加速匹配字串代表该成员的匹配规则。

**保存副本：**保存副本可以选择不同副本，相同副本。不同副本是指符合该成员匹配规则的请求对应的响应不同。相同副本是指符合该成员匹配规则的请求对应的响应为同一个副本。例如：Cookie：username=aaa；sessionid=123\r\n 当 username 的值不同时，回应的内容也不同，则可以配置名称是 username 的 cookie 参数，成员是"正则不同 .*",那么缓存模块就会根据不同的 username 创建不同的副本。

参数的成员之间是或的关系，成员表中位置靠上的优先匹配。可以选择成员表中的字串，点击上移或者下移，改变成员的匹配优先级。

### 34.2.6 加速规则—生存期配置

Lifetime 用来计算缓存副本在本地的 TTL（time to live），如果缓存副本在本地的停留时间超过 TTL，那么这个缓存副本将被认为是过期的。动态缓存 lifetime 配置包含三大部分如下图：


**参数说明：**

**生存周期相关的头域设置**

**使用原始头域中出现的生存周期：**如果这个开关开启，如果响应头域中存在生存周期相关的头域，则使用这些头域信息计算缓存对象的 TTL，否则使用本地缓存时间配置的参数计算 TTL。

**忽略请求头中的 no-cache：**如果这个选项关闭，当请求头域中出现 Cache-Control 头域中有 no-cache，no-store 字串时，响应不能被缓存。如果开启则忽略这些字段。

**忽略响应头中的 no-cache：**如果这个选项关闭，当响应头域中出现 Cache-Control 头域中有 no-cache，no-store 字串时，响应不能被缓存。如果开启则忽略这些字段。

**本地缓存时间设置**

**最大生存周期：**缓存副本可存活的最大时间。默认 3600 秒。

**过期后仍有效周期：**默认缓存在超过生存时间不多于这个设置的时候仍然视为可用的。

**启发式生存周期百分比：**当用 last-modifed 时间来估算生存周期时使用的百分比。

**客户端缓存设置**

**使用原始头域：**使用服务器的头域信息。

**最大生存期改为 X 秒：**将擦除服务器的 cache-control 头域，插入 Cache-Control：maxage=X 头域。

**将缓存控制头域改为 no-cache：**将擦除服务器的 cache-control 头域，插入 Cache-Control：no-cache 头域。

## 34.2.7 加速规则—失效触发器配置

失效触发器的规则没有继承性，所以只有叶子节点的失效触发才会真正的有效，其余节点无效。如下图，只有在 Home，Default,Search,Image 四个节点配置失效触发器才可能生效，在节点 Application 节点的失效触发器是无效的。缓存模块不会去检查非叶子节点的失效触发器。


如上图，选择 Default 节点，下拉菜单选择加速规则并点击失效触发器标签页，该标签页显示节点已有的失效触发列表，点击**新建**可以新建一个失效触发器。


**参数说明：**

**名称：**指定该失效触发器的名称，最多可输入 63 个字符。

**描述：**简要的说明该失效触发器的一些失效规则等，最多支持 255 个字符。

输入名称和描述后点击**提交**新建失效触发器，然后在列表中可看到新建的实现触发器的名称和描述。


点击名称字段可进入失效触发器的规则配置，如下图：


**列表说明：**

**触发器请求头匹配标准：**

失效触发器只作用于每个叶子节点，但并不是符合这个节点匹配规则的请求都能触发失效动作。这个请求还必须匹配触发器请求头标准规则的所有参数对象规则。基于这个设定，触发器请求头匹配标准配置的过滤规则不能和这个叶子节点的匹配规则相斥，它的条件只能是匹配规则的子集，只有这样才能触发失效动作。

上图中第一个参数下拉菜单中包含所有可以用来配置**触发器请求头匹配标准**的参数类型。选择一个参数类型如 Query Parameter，点击**添加**，出现参数配置界面，如下图：


**参数说明：**

**类型：**参数的类型，这个字段在选择参数的时候，系统就已将默认，用户不可更改。

**名称：**参数的名称，支持不多于 63 个字符的输入。除了

queryparameter，cookie，和 header 三个类型的参数外，其余的参数名称由系统默认。参数的名称只认可完全相等的字串，*代表全部，其余的字符都当做字面字符处理。列如有个请求为：http://venustechnetworks.com/templates/H_content/index.aspx?nodeid=179&page=CoContentPa&contentid=12 添加这个匹配规则中的 QueryParameter 时，名称是*，则指整个查询字段 nodeid=179&page=CoContentPa&contentid=12，或者只能添加名称为 nodeid 或者 page 或者 contentid 这个三个，其余的配置都不可能与这个请求匹配成功。

**成员：**一个参数只能有一个类型和名称，但是可以有多个成员，每个成员由匹配结果，匹配算法，匹配字串三个部分组成。这个三个部分互相依赖，改变任何一个都可能影响最终的结果。

**匹配结果：**匹配结果可以选择匹配或者排除。

**匹配算法：**匹配算法可以选择正则，包含，完全等于，开头等于，结尾等于。

**匹配字串：**用来和请求中的特定字段做比较的字符串。

参数的成员之间是或的关系，成员表中位置靠上的优先匹配。可以选择成员表中的字串，点击上移或者下移，改变成员的匹配优先级。

**触发器失效缓存对象特征：**

一个请求完全符合请求头匹配标准后，它将指定一些缓存对象失效。在缓存哈希表中，所有符合失效缓存对象特征的缓存副本将别删除。

在失效触发器规则配置页面的第二个参数下拉菜单中包含所有可以用来配置**触发器失效缓存对象特征**的参数类型。选择一个参数类型如 Query Parameter，点击添加，出现参数配置界面，如下图：


**参数说明：**

**类型：**参数的类型，这个字段在选择参数的时候，系统就已将默认，用户不可更改。

**名称：**参数的名称，支持不多于 63 个字符的输入。除了

queryparameter，cookie，和 header 三个类型的参数外，其余的参数名称由系统默认。参数的名称只认可完全相等的字串，*代表全部，其余的字符都当做字面字符处理。列如有个请求为：http://venustechnetworks.com/templates/H_content/index.aspx?nodeid=179&page=CoContentPa&contentid=12 添加这个匹配规则中的 QueryParameter 时，名称是*，则指整个查询字段 nodeid=179&page=CoContentPa&contentid=12，或者只能添加名称为 nodeid 或者 page 或者 contentid 这个三个，其余的配置都不可能与这个请求匹配成功。

**成员：**一个参数只能有一个类型和名称，但是可以有多个成员，每个成员由匹配结果，匹配算法，匹配字串三个部分组成。这个三个部分互相依赖，改变任何一个都可能影响最终的结果。

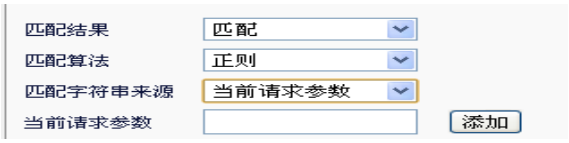
**匹配结果：**匹配结果可以选择匹配或者排除。

**匹配算法：**匹配算法可以选择正则，包含，完全等于，开头等于，结尾等于。

**匹配字符串来源：**指定用来作为匹配的字串来源，可选择字符串组或者当前请求参数。匹配字符串来源选择字符串组，则该下拉菜单下方出现匹配字串的文本编辑框，该文本编辑框输入用来作为匹配的字符串。

**匹配字串：**用来和缓存副本中的特定字段做比较的字符串。

匹配字符串来源选择当前请求参数则该下拉菜单下方出现当前请求参数的文本编辑框，如下图：




**当前请求参数：**该文本编辑框中输入的字符代表当前请求的一个字段名称，列如列如有个请求为：http://venustechnetworks.com/templates/H_content/index.aspx?nodeid=179&page=CoContentPa&contentid=12。在文本编辑框中输入 nodeid，那么在匹配的时候匹配的字串就是 179 而不是 nodeid。只有当缓存副本的查询字段的 nodeid 为 179 时，该缓存副本会被清除。

参数的成员之间是或的关系，成员表中位置靠上的优先匹配。可以选择成员表中的字串，点击上移或者下移，改变成员的匹配优先级。

如下图为节点配置了 my_trigger 的失效触发器，参数列表如下：


每个列表都添加了两个参数，在触发器请求头匹配标准列表有 query parameter 和 referrer 两个参数，在匹配过程中，这两个参数是与的关系，请求必须同时满足这两个参数的规则，匹配成功。

在触发器失效缓存对象特征列表中有 query parameter 和 cookie 两个参数，在匹配过程中，这两个参数是与的关系，缓存对象副本必须同时满足这两个参数的规则，这个副本才能被清除。

## 34.3 配置案例

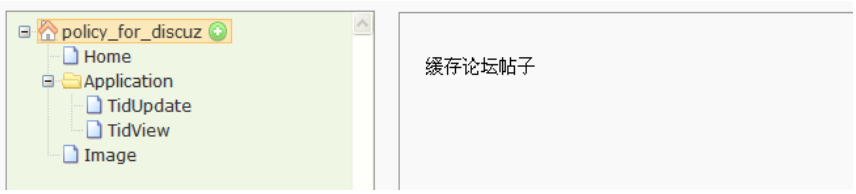
假设负载均衡设备的后台是一个 DISCUZ 为模板的论坛服务器，这个论坛允许用户注册，登陆，浏览帖子，发新帖和发表评论。由于访问量过大，导致服务器请求压力过大，为了缓解这一问题，我们可以将用户浏览的帖子缓存到设备本地，这样可以减少服务器的压力。我们针对这个个 DISCUZ 为模板的论坛配置一棵策略树，主要缓存论坛的帖子。

### 34.3.1 配置步骤

**步骤：**

**步骤 1：**分析用户浏览帖子，发新帖，发评论这些动作的响应特征。论坛帖子根据 tid 区分，登陆用户会显示在线用户的名称。根据这个特征创建一个策略树 policy_for_discuz，如图


**步骤 2：**在策略树编辑界面，为这棵树创建树节点，如下图：




Home 节点规则适用于该论坛的主页，包含登陆界面。

Image 节点规则适用于所有的图片文件。

TidUpdate 节点规则适用于发表新帖或者发表评论的请求。

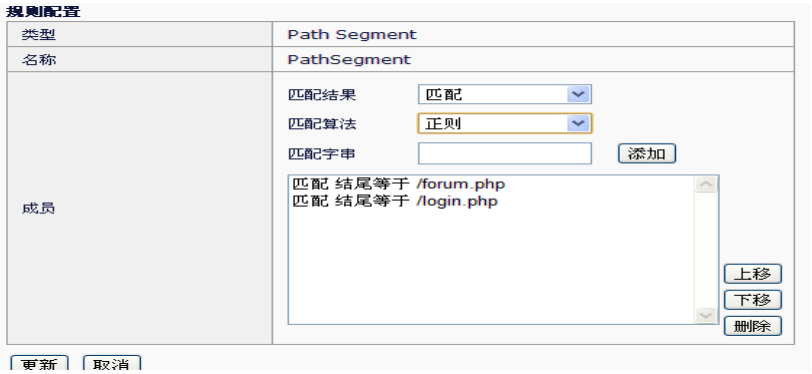
TidView 节点规则适用于浏览帖子的请求。

Application 节点用来配置 TidUpdate 和 TidView 节点共同的规则。

**步骤 3：**为每个节点配置适当的规则。

**Home 匹配规则：**

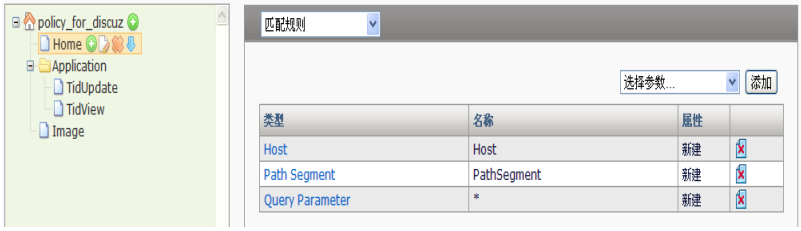
1. 默认 Host 参数规则。
2. 点击 Path Segment 字段，在出现的参数配置界面中删除默认的成员，添加配置如下



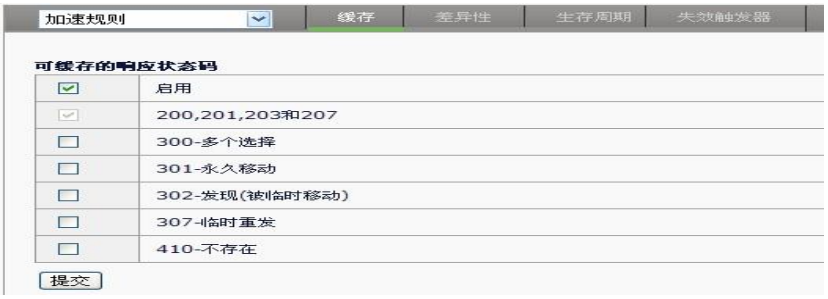

3. 在选择参数下拉菜单中选中 QueryParameter 类型，点击添加，进入参数配置界面，如下：


因为主页的请求不包含任何查询字段，所以必须对所有的查询字段进行排除。

1. Home 节点的匹配规则完成如下




2. 缓存：




3. 差异性：

因为主页面中，登陆用户和非登陆用户的界面不一致，所以要缓存不同的副本，而登陆和非登陆用户的区分是 cookie 中的 discuz_2132_auth 字段，所以配置差异性如下：

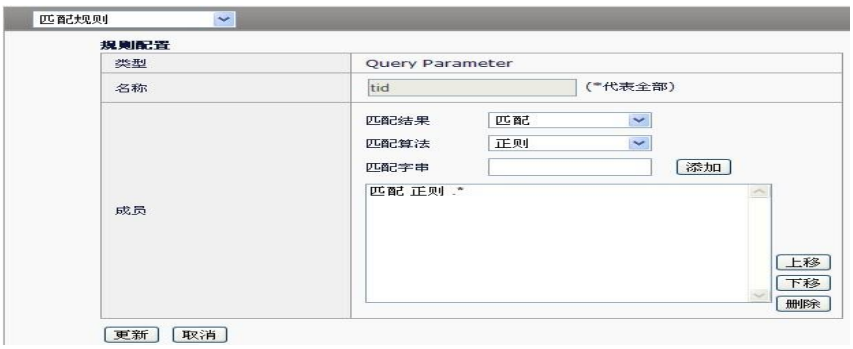


4. 生存周期：因为该主页是一个动态页面，服务器的回应头域中带有 no-cache 字段，并且 maxage=0.所以我们为了缓存这个页面，强制不是用服务器的头域信息，生存期是用本地配置的时间。

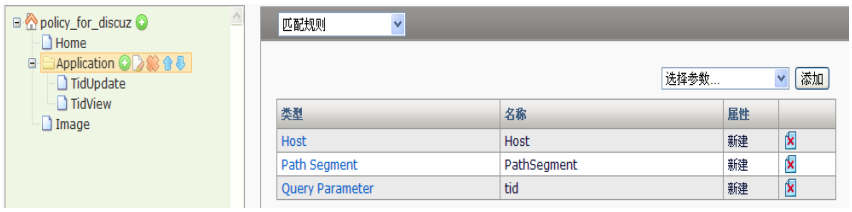

**Application 节点配置**

1. 配置匹配规则 host 是用默认值，pathsegment 参数配置如下：


添加 query 参数，因为所有对贴子的操作请求中都含有 tid 这个查询参数，所以配置如下：




匹配参数列表如下：




2. 缓存是用默认配置。

3. 差异性删除默认配置的 query 参数，添加 cookie，如下图：

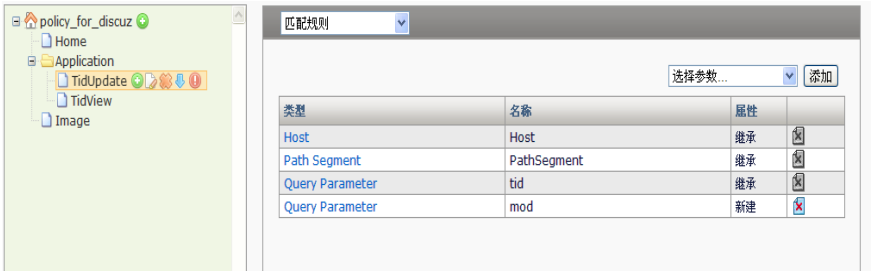


**TidUpdate 节点配置**

该节点为用户用户提交跟新帖子等的数据操作请求中的查询字段带有 mod=post 的字符。该节点配置如下

1. 匹配规则，出了继承与 Application 的参数外，添加 query 参数，如图：


该节点的匹配规则：




2. 缓存因为该节点是用户提交数据到服务器，所以命中该节点的所有请求不缓存


3. 差异性使用默认配置

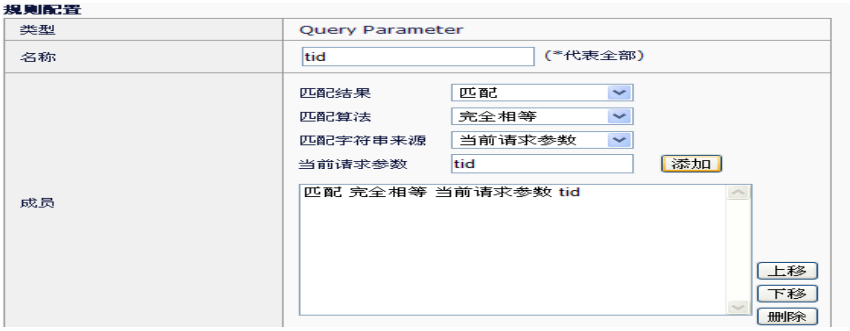
4. 生存周期使用默认配置

5. 失效触发器命中这个节点的请求表明是用户发表了评论，所以对于请求浏览这个帖子的回应有了更新，存在于设备本地的相应的缓存副本必须清除。我们为这个行为配置一个失效触发器。点击新建，如下图新建一个触发器


到触发器的编辑界面添加参数，触发器请求头匹配标准只要符合这个节点的匹配规则就可以了，所以不需要载添加更具体的参数。

触发器失效缓存对象特征，如下配置：

添加一个 query 参数，成员配置如下：



该条配置是得缓存副本中 tid 字段等于请求中 tid 字段的副本被删除。

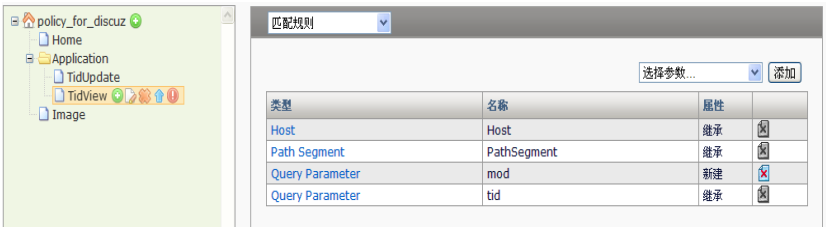
该节点的触发器配置如下：


**TidView 节点配置**

当用户浏览一个帖子的请求会命中该节点。

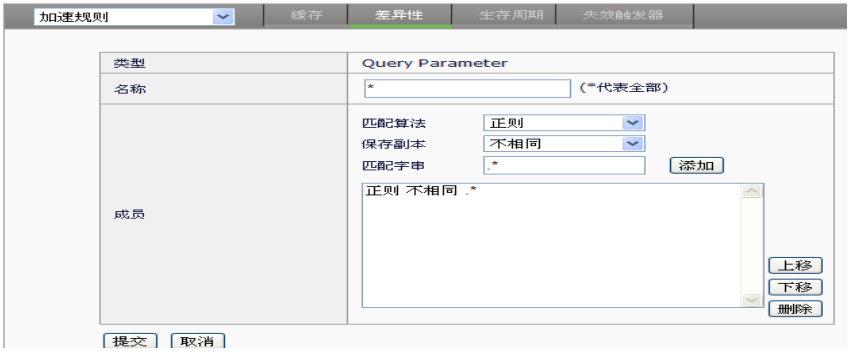
1. 匹配规则除了继承的参数外，需要添加 Query 参数，配置如下：


匹配规则参数列表如下：




2. 缓存


3. 差异性当用户浏览不同帖子的查询字段的 tid，page 等都不相同，为里安全我们将整个查询字段作为 UCI 关键字段。所以除了继承的 cookie 参数，我们添加 query 参数如下：




差异性列表


4. 生存周期


**Image 节点配置**

1. 匹配规则

使用默认的 host path 参数规则，添加一个 Extension 参数，如下图：


匹配规则参数列表


2. 缓存默认值
3. 差异性默认值
4. 生存周期默认值

**步骤 4**：新建一个缓存模板 cache_for_discuz，将配置模式设置为高级模式，在策略树中引用 policy_for_discuz。如下图：


**步骤 5**：在虚拟服务中引用 cache_for_discuz 缓存模板，如图：


### 34.3.2 启用案例配置效果

当第一个请求访问帖子 aaa 的响应到达缓存模块，该响应会被缓存到设备的缓存中，第二个请求访问帖子 aaa 的响应则直接从设备的缓存中获取，不需要跟服务器建立连接。当有一个用户对帖子 aaa 发表评论的时候，设备接收到这个评论的提交请求后，会把帖子 aaa 在设备的缓存清除。当第三个请求访问帖子 aaa 的用户会重新到服务器获取并再次被缓存到设备本地。这个策略配置可以实现缓存及时更新，在帖子没有新的评论的时候用户可以从缓存中获取响应，减少服务器连接数。

## 34.4 常见故障分析

### 34.4.1 常见故障1

| | |
|---|---|
| 现象 | 请求没有命中到预期的叶子节点 |
| 分析 | 有可能是以下几种情况导致的：<br>1.节点的匹配规则不合理，父子节点的匹配规则相斥，导致无法匹配到叶子节点。<br>2.同级节点情况下，将规则范围小的节点移到规则范围大的节点之上。 |
| 解决 | 检查配置的规则是否正确是否能达到预期的效果，适当调整配置。 |

### 34.4.2 常见故障2

| | |
|---|---|
| 现象 | 不同的请求命中了同一个缓存副本 |
| 分析 | 有可能是以下几种情况导致的：<br>1.节点的差异性配置不对，将请求配置成匹配相同相同副本。<br>2.节点的差异性配置不够详细，导致不同请求计算出来的UCI字段相同，无法区分。 |
| 解决 | 检查配置的规则是否正确是否能达到预期的效果，适当调整配置。 |

# 35 第35章 智能终端加速

## 35.1 智能终端加速概述

智能终端加速，旨在为各个移动终端提供相应的加速功能，目前这些智能终端一般为 Android 或者 IOS 系统。

目前提供针对移动智能终端的图片加速功能，指通过图片压缩、缓存以及压缩配置，减少智能终端流量的加速方式。

网络上的图片占用流量越来越大，对于没有专门对图片进行优化的网站而言，图片压缩能节省比较大的流量。而传统的压缩功能对图片的压缩率几乎是可以忽略不计的，所以需要专门对图片的压缩进行处理。另外，在压缩过程中调整大小以使图片能适应移动终端设备，也减轻了用户配置服务器的开销。

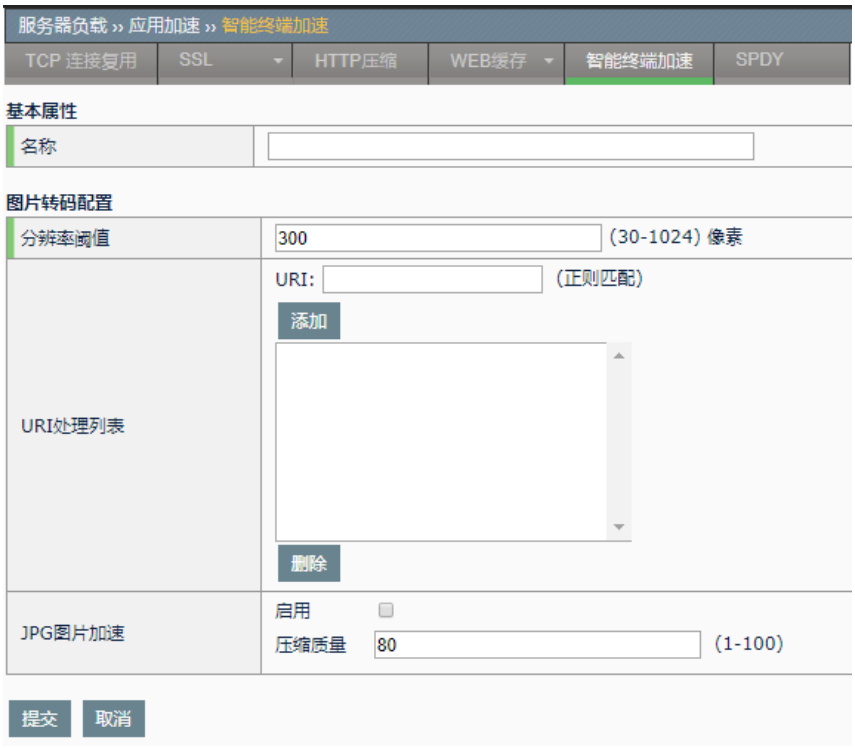
图片类型：

- JPG 格式。支持大小调整和按质量压缩。大小调整功能依据 useragent 和用户配置的大小，以最小的为准对原图片进行缩放，实现图片对移动端的支持。按质量压缩依据用户的配置，将图片质量降低，实现对图片的压缩。

## 35.2 配置模板

**配置步骤：**

1.进入**服务器负载>应用加速>智能终端加速**，点击**新建**




**参数说明：**

**名称：**智能终端加速的名称

**分辨率阈值：**指的是图片的分辨率宽度。将把原始图片按比例压缩成该宽度对应的大小。

**URI 处理列表：**客户端的请求符合该列表的 URI 将被处理，进行压缩。支持正则匹配

**JPG 图片加速：**对 jpg 图片进行处理

**启用：**启用 jpg 图片加速

**压缩质量：**jpg 图片的压缩质量

## 35.3 配置案例

### 35.3.1 案例1：对网站上的jpg图片压缩

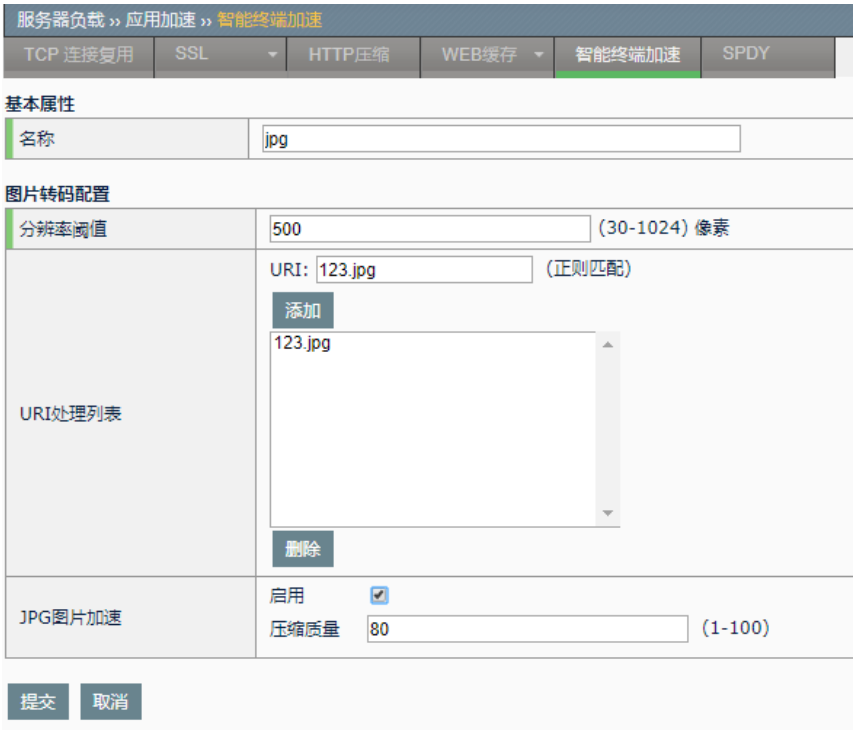
**案例描述**

配置一个模板，移动终端访问 123.jpg 时，对其按宽度为 500 进行大小调整，压缩质量为 80。

**配置步骤：**

1．进入**服务器负载>应用加速>智能终端加速**，点击**新建**

2．配置参数，如图




3．点击提交。

4．在虚拟服务中引用，同时需要引用 http 模板


## 35.4 常见故障分析

### 35.4.1 故障现象1：无法按配置进行压缩

| | |
|---|---|
| 现象 | 配置了对应的智能终端加速，但是无法对原图像进行压缩 |
| 分析 | 有可能是以下几种情况导致的：<br>1.原来图像超过5k*4k的分辨率<br>2.原图像太大，超过5M<br>3.虚拟服务未引用相关模板 |
| 解决 | 应在虚拟服务中引用该模板，并且需同时引用了某个http模板才能生效。<br>检查配置的规则是否正确。 |

# 36 第36章 SPDY

## 36.1 SPDY概述

SPDY 是谷歌提出的一种新的网络协议，“SPDY”一词的发音同“speedy”，名称是从"speedy"这个单词而来。协议设计的初衷是通过头压缩和流复用来达到比传统 HTTP 协议更快的网络传输速度，更小的网络传输延迟，以及更优化的用户的网络体验。

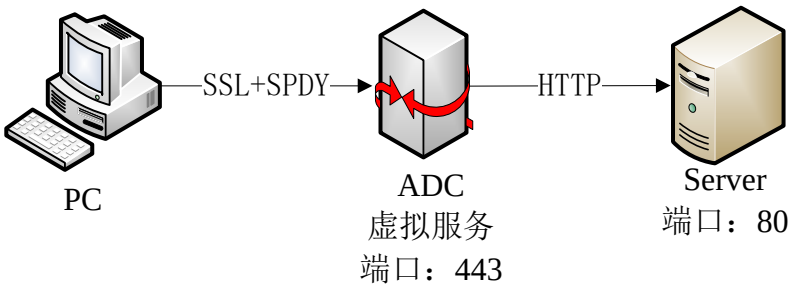
当在代理模式的虚拟服务中配置了 SPDY 模版，将能够在不改变后台服务器配置的情况下，使得服务器获得处理 SPDY 协议的能力。当收到客户端的 SPDY 请求，SPDY 模块会把 SPDY 请求装换为 HTTP 请求，发送给服务器。当收到服务器 HTTP 响应后，SPDY 把 HTTP 响应装换为 SPDY 响应，回应给客户端。

## 36.2 SPDY使用场景

SPDY 最开始设计时，要求协议保证安全性，所以目前应用中的 SPDY 协议几乎都运行在 SSL 加密的基础上。比如 Google 的所有应用、Facebook、Amazon 等等。

目前支持 SPDY 协议的浏览器有 Chrome、Firefox、IE11 等，Chrome 和 Firefox 是默认开启的。当浏览器通过通过 Https 访问站点的时候，通过 SSL 的 NPN 协商机制，SPDY 模块可以智能判断浏览器是否支持 SPDY，若浏览器支持 SPDY，那么 SPDY 模块会用 SPDY 协议和浏览器进行通信，否则使用 HTTP 协议进行通信。

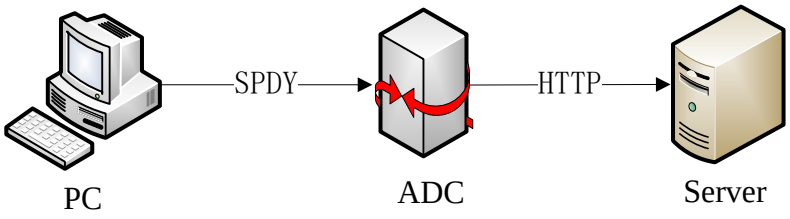
**通常应用场景举例：**




其中 ADC 上配置代理模式的虚拟服务配置 443 端口。开启 SSL 客户端模版、HTTP 模版和 SPDY 模版。浏览器通过 443 端口用 Https 的方式访问虚拟服务，SPDY 模块根据客户端的信息智能选择开启 SPDY 协议进行通信。

通过这种配置可以使 web 服务器不做任何修改，和支持 SPDY 协议的浏览器进行

**特殊应用场景举例：**



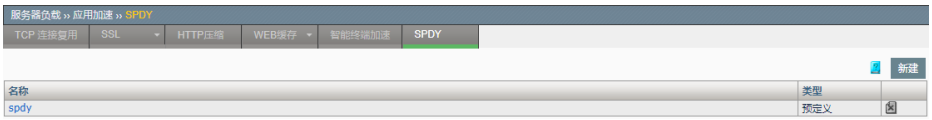

这种应用场景，需要用户确定客户端采用的是 SPDY 协议，这样不需要开启 SSL 客户端模版

## 36.3 SPDY配置

### 36.3.1 配置SPDY模版

**配置步骤：**

1. 进入**服务器负载>应用加速>SPDY**，如下图：

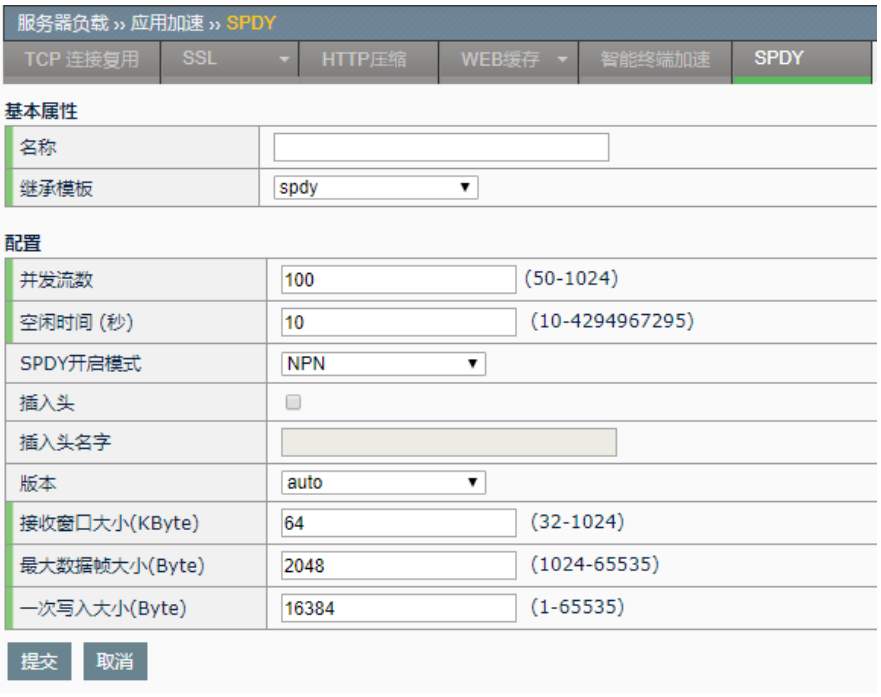



**新建：**添加一个 SPDY 模板。

：删除掉该模板。

点击名称，可以对已配置的 SPDY 模板内容进行编辑。

2. 点击**新建**




**名称：**该模板的名称

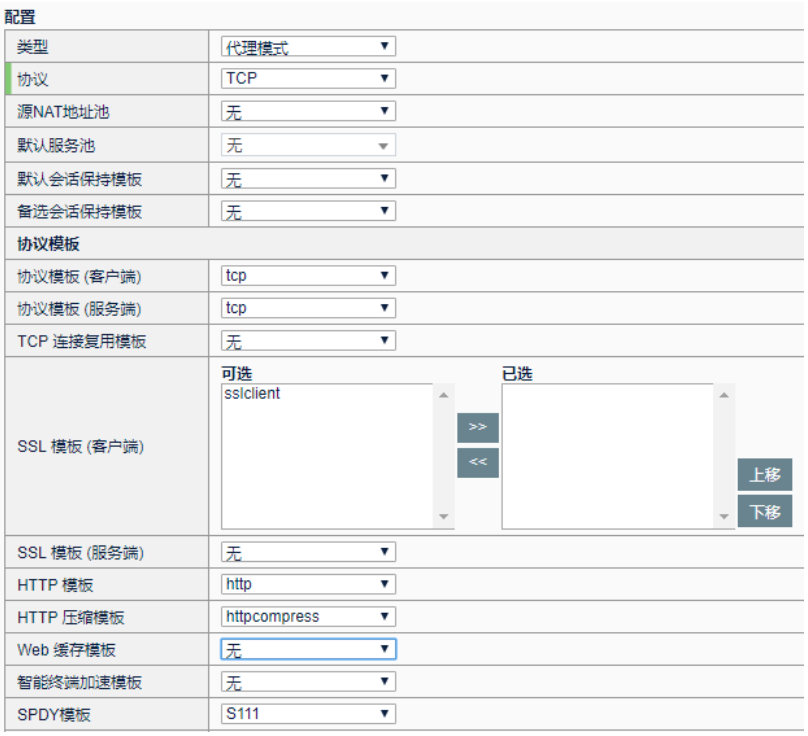
**继承模板：**下拉选择后，把所选模板的配置继承下来

例如，上图中创建了一个名称为 s111 的 SPDY 模板，其配置继承了系统预定的模板 spdy。

3. 虚拟服务中引用 SPDY 模板

要使所配置的 SPDY 模板生效，需要在对应的虚拟服务中引用。

进入**服务器负载>虚拟服务**，在**新建**或**编辑**虚拟服务的界面中，从 **SPDY 模板**的下拉列表中选择需要引用的 SPDY 模板，例如引用上面新建成功的模板 s111：



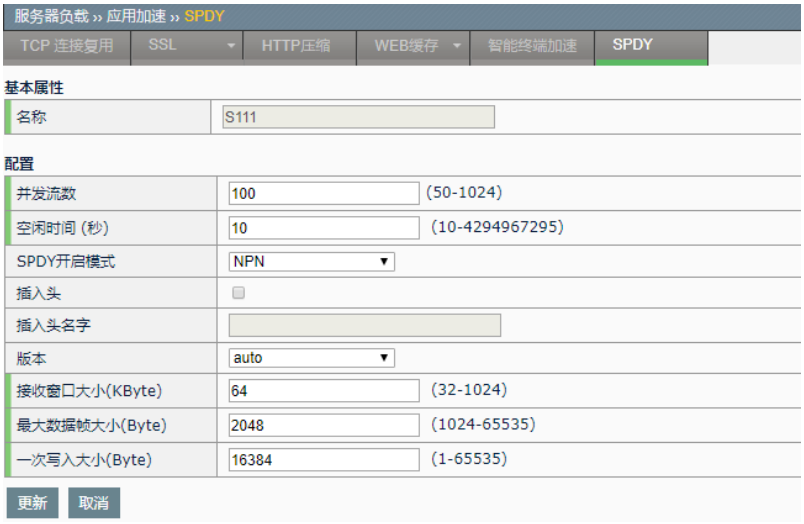

4. 点击**更新**提交，这样 SPDY 模板 s111 就在虚拟服务中生效。

提示　通常 SPDY 模板要搭配 SSL 客户端模版同时使用。

注意　虚拟服务需要是代理模式。
SPDY 模版必须和 HTTP 模版同时配置。否则无法生效。

### 36.3.2 SPDY模版参数配置

进入**服务器负载>应用加速>SPDY**，点击要编辑的 SPDY 模版，进入如下页面：




- **并发流数：**指定允许客户端最大的并发请求数。

  当客户端超过了最大并发数，SPDY 模块会回应 SYN_RST。

- **空闲时间：**当所有请求处理结束，连接保持的时间。

- **SPDY 开启模式：**可选择“NPN”、“强制开启”。

| | |
|---|---|
| 提示 | “NPN”模式需要在虚拟服务中关联 ssl 客户端模版。<br>“强制开启”模式，必须保证客户端一定会使用 SPDY 协议通信。 |

- **插入头：**选择是否开启插入头的功能。

- **插入头名字：**开启插入头功能后，在回应中插入头的名字，可作为 SPDY 协议的标记。

| | |
|---|---|
| 提示 | 根据 SPDY 协议文档，插入头只能是小写字母，并插入头的名字不能和其他 HTTP 头域名字冲突，否则插入无效。 |

- **版本：**SPDY 的版本，可选“auto”，“spdy3.1”，“spdy3”，“spdy2”。

| | |
|---|---|
| 提示 | “auto”表示根据浏览器的版本，自动选择 SPDY 的版本<br>如果想要固定使用的 SPDY 版本，那么直接选中要使用的版本。 |

- **接收窗口大小：**设置处理上传流时的接收窗口大小。

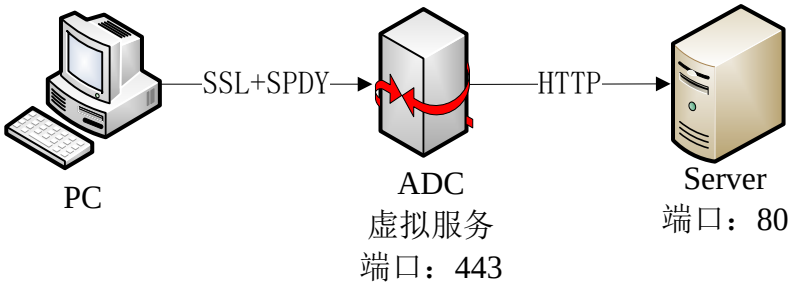

只对 SPDY3 以上版本有效。

- **最大数据帧大小：**设置最大的 data 帧的长度。
- **一次写入大小：**设置一次发送的数据大小。


为了防止出现网络中出现多次小数据的发送，所以把要发送的数据收集到一定数量发送。

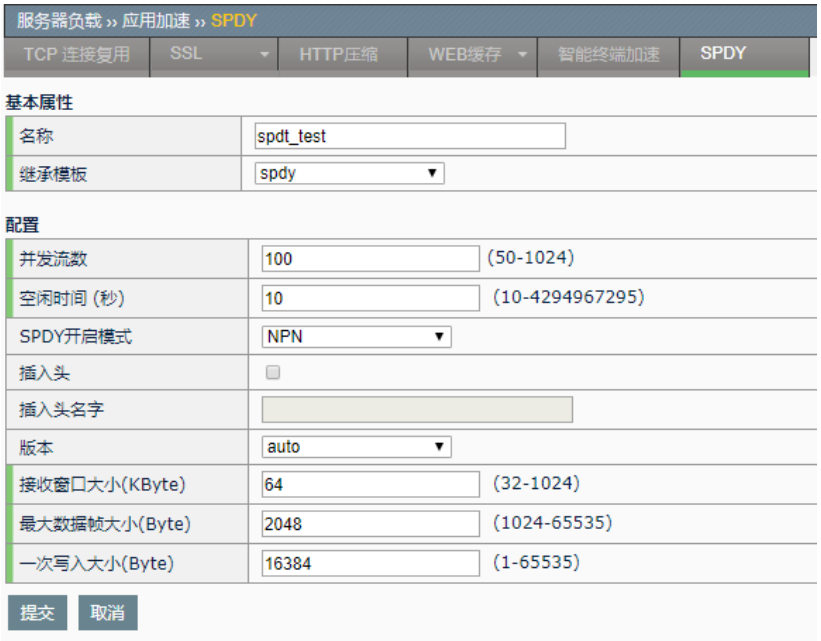
## 36.4 SPDY使用场景

**通常应用场景举例：**

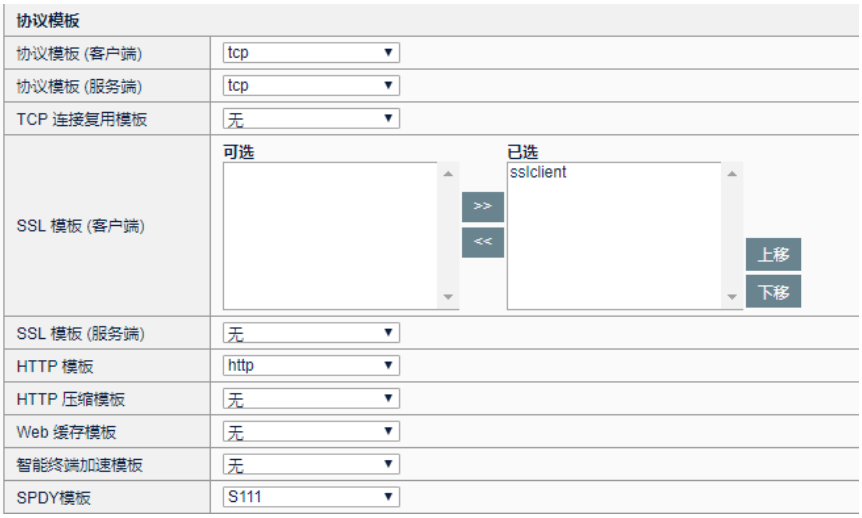



**步骤：**

1. 配置虚拟服务，端口 443.，默认服务池用户配置。
2. “服务器负载”->“应用加速”->“SPDY”，新建 SPDY 模版，选择默认配置：




3. 在虚拟服务的协议模版部分配置 SSL 客户端模版、HTTP 模版、SPDY 模版。




点击“保存”后，虚拟服务就添加了 SPDY 的支持。

## 36.5 常见故障分析

### 36.5.1 故障现象1：如何看出SPDY生效

| | |
|---|---|
| 现象 | 不容易看出是否SPDY生效 |
| 分析 | 通过开启SPDY模版的插入头开关，可以在SPDY回应中插入一个新的http头域，指明这个请求是SPDY协议处理的。 |

| | |
|---|---|
| | 通过浏览器的调试模式，可以看到插入的http头。 |
| 解决 | 在SPDY模版中开启插入头，并且输入要插入的头名字。 |

# 37 第37章 虚拟链路

## 37.1 虚拟链路概述

随着企业开始更多地使用互联网来交付其关键业务应用，一条 Internet 接入线路意味着可能存在单点故障，越来越多的企业开始使用多条 Internet 接入线路。

使用虚拟链路（VLINK）功能可以无缝地监控多条 WAN 连接的可用性和性能，智能地管理到每一站点的双向流量，从而提供出色的容错性和优化的互联网访问，保证关键业务的稳定运行。该功能可以将网络的多个出口模拟成多个虚拟链路，可以根据用户的实际需求智能选择出口链路，分配网络流量。

虚拟链路在有新会话时，会先基于用户所设的路由策略顺序进行匹配，按照命中的路由策略选择下一跳；如果都未命中，则从默认链路地址池中进行选路。

## 37.2 配置虚拟链路

系统把虚拟链路配置分为：**基本属性**、**基础选项**和**高级选项**。**基本属性**是创建虚拟链路的必填选项；**基础选项**和**高级选项**是虚拟链路的高级属性，可以根据网络环境灵活设定。

### 37.2.1 配置虚拟链路

1. 进入**链路负载>虚拟链路>虚拟链路**，点击**新建**。
2. 配置基本属性。

**名称**：虚拟链路的名称。

**启用**：是否启用该虚拟链路，只有启用的情况下，该虚拟链路才会参与匹配，

该选项不是必填项

**目标地址**：指定虚拟链路匹配地址或网段，目标地址分为 IPv4 和 IPv6 两种类型，匹配到所配置的地址或者网段的报文才会进入到虚拟链路选路流程中。

**目标服务**：指定虚拟链路匹配协议和端口，报文协议匹配到所配置的协议和端口号才会进入到虚拟链路选路流程中。

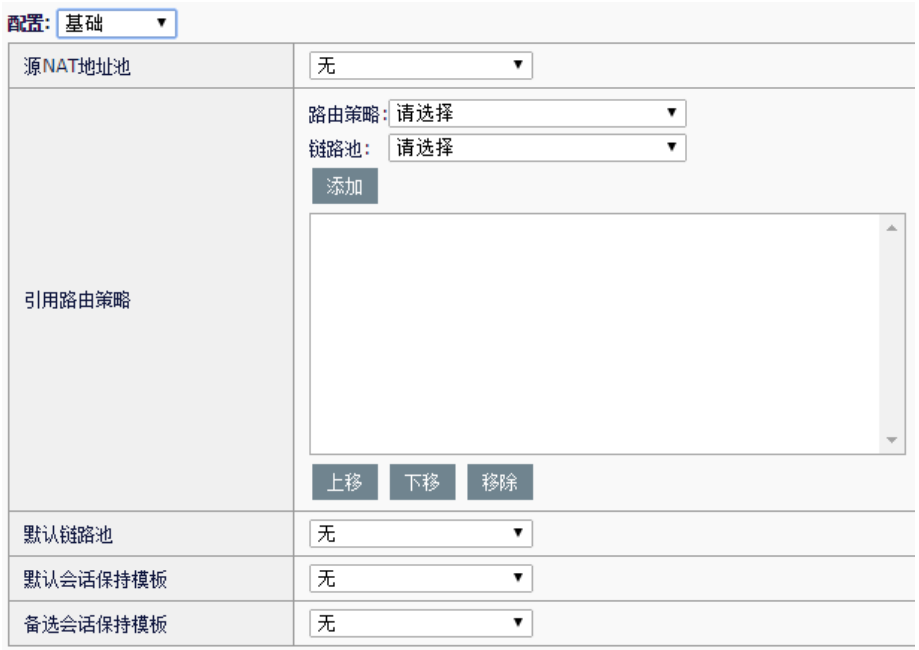
**入接口**：指定虚拟链路匹配入接口，只有从该接口进入的报文才会进入到虚拟链路选路流程中。两个选项：所有接口，即所有接口；自定义，可以根据实际指定接口。

注意

1.虚拟链路根据目标地址，目标服务，以及入接口来作冲突检查，如果配置出现重叠或冲突，则会提示配置错误。

2.流量匹配虚拟链路时，配置越精细的匹配优先级越高，例如，配置目的地址为 10.0.0.1 的虚拟链路，和配置目的地址为 10.0.0.0/24 的虚拟链路，前者的匹配优先级会更高。

3．配置基础选项。




**源 NAT 地址池**：对报文的源地址进行转换，可以选择自定义 NAT 地址池；也可以选择自动映射，将源地址自动映射为出接口地址；如果选择

无，则表示不启用源地址转换。

**引用路由策略**：把指定的路由策略与链路地址池对应，匹配到该路由策略的使用对应的链路地址池选路。

**默认链路池**：指定默认链路地址池，当路由策略匹配失败之后，通过该链路地址池选路。

**默认会话保持模板**：优先匹配该会话保持项，可以为源地址会话保持或者目的地址会话保持。

**备选会话保持模板**：当默认会话保持项匹配失败，匹配该会话保持项，可以为源地址会话保持或者目的会话保持。

4. 配置高级选项。


**路径一致性**：开启之后，反向报文根据正向报文的入接口选路，保证往返路径一致。

**TCP 加速**：开启之后，在网络延时较大、丢包严重以及报文乱序的网络场景中能够起到加速 TCP 数据传输的效果。

**多连接选路**：开启之后，反向子链接的正向报文根据路由选路，只适用于

多级连接（如 H323）的情况。

**链路拥塞控制**：开启之后，发生拥塞的出链路不参与选路。如果链路地址池中的链路全部拥塞，所有拥塞链路都参与选路。

**直连路由优先**：开启之后，对于访问同一网段的报文通过直连路由转发。

**DNS 代理关联**：开启之后，该虚拟链路上的报文要进行 DNS 代理。

**源主机连接限制**：同一源地址的连接数限制，值为 0 表示不限制。

**源主机连接速率限制**：同一源地址的连接速率限制，值为 0 表示不限制。

**流量控制**：开启之后，有如下四个选项：


**总上行带宽限制**：设定该虚拟链路总上行带宽限制。

**总下行带宽限制**：设定该虚拟链路总下行带宽限制。

**主机上行带宽限制**：设定该虚拟链路每个源主机的上行带宽限制。

**主机下行带宽限制**：设定该虚拟链路每个源主机的下行带宽限制。

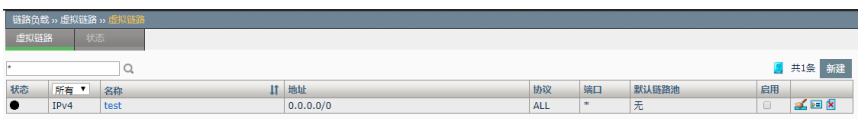
**HA 状态同步**：开启之后，该虚拟链路对应的流会同步到 HA 备设备上。

**镜像接口**：只能指定物理接口且不能为 VLAN 口，匹配到该虚拟链路的流量备份转发到该物理口上，该物理接口尽量不要用于转发流量。

5. 点击**提交**。

## 37.2.2 查看虚拟链路列表

进入**链路负载>虚拟链路>链路列表**




1. 链路状态：两种状态， - 开启； - 关闭

2. 点击**名称列表**下面的**名称字段**可编辑链路。

3. 点击 可**删除虚拟链路。**
4. 编辑完成之后点击**提交。**
5. 勾选**启用**可以使用虚拟链路。


当栏目为灰色的时候即该选项不能被编辑，即名称是不能被编辑修改的。

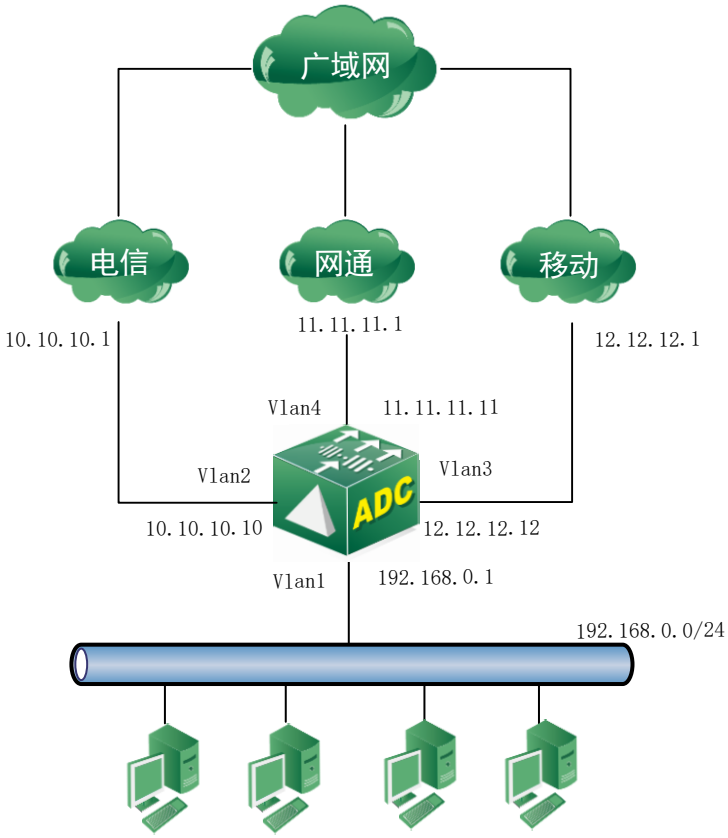
## 37.3 配置案例

### 37.3.1 配置虚拟链路

企业需要通过 ADC 进行互联网访问，内网地址段为 192.168.0.0/24。现在有三条出口链路分别属于电信、网通和移动，电信的公网地址为 10.10.10.10，网关为 10.10.10.1；网通的公网地址为 11.11.11.11，网关为 11.11.11.1；移动的公网地址为 12.12.12.12，网关为 12.12.12.1。

用户的需求如下：

1. 目的地址为电信 IP 地址，选择电信的链路作为出链路
2. 目的地址为电信 IP 地址，且当电信的链路拥塞之后，选择移动的链路作为出链路
3. 目的地址为网通 IP 地址，选择网通的链路作为出链路
4. 目的地址为网通 IP 地址，且当网通的链路拥塞之后，选择移动的链路作为出链路
5. 目的地址为移动 IP 地址，选择移动的链路作为出链路
6. 目的地址为移动 IP 地址，切当移动的链路拥塞之后，均匀选择一条没有发生拥塞的链路作为出链路
7. 目的地址不属于电信、网通和移动，可以均匀选择出链路
8. 转发报文不限定协议和端口号

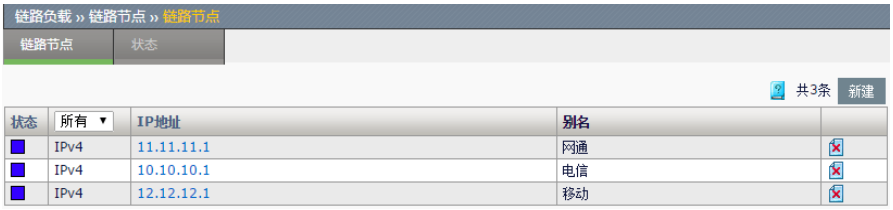



**配置步骤：**

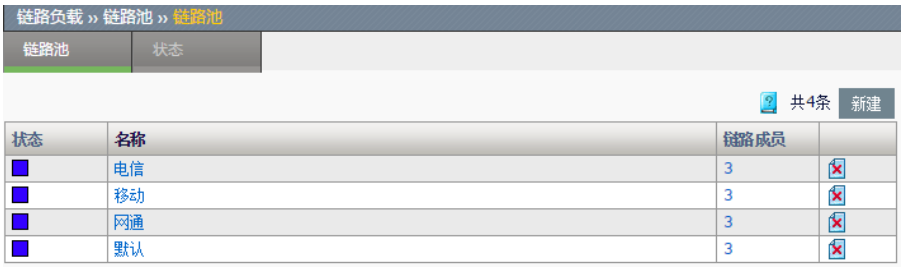
1. 进入**模板和对象>对象管理>地址对象**，分别创建包含**电信 ISP 地址库**、**网通 ISP 地址库**和**移动 ISP 地址库**的地址对象。


2. 进入**模版和对象>路由策略**，分别创建**电信路由策略**、**网通路由策略**和**移动路由策略**。


3. 进入**链路负载>链路节点**，分别创建**电信链路**、**网通链路**和**移动链路**。




4. 进入**链路负载>链路池**，分别创建**电信链路池**、**网通链路池**、**移动链路池**和**默认链路池**。




**电信链路池**


电信链路的优先级最高，当匹配到该链路池所对应的路由策略时，使用优先级最高的链路作为出链路；当发生拥塞的时候使用次优先级的链路作为出链路，移动设为次优先级可以达到当电信链路发生拥塞时，流量引导到移动链路上

**网通链路池**


网通链路的优先级最高，当匹配到该链路池所对应的路由策略时，使用优

先级最高的链路作为出链路；当发生拥塞的时候使用次优先级的链路作为出链路，移动设为次优先级可以达到当电信链路发生拥塞时，流量引导到移动链路上

**移动链路池**

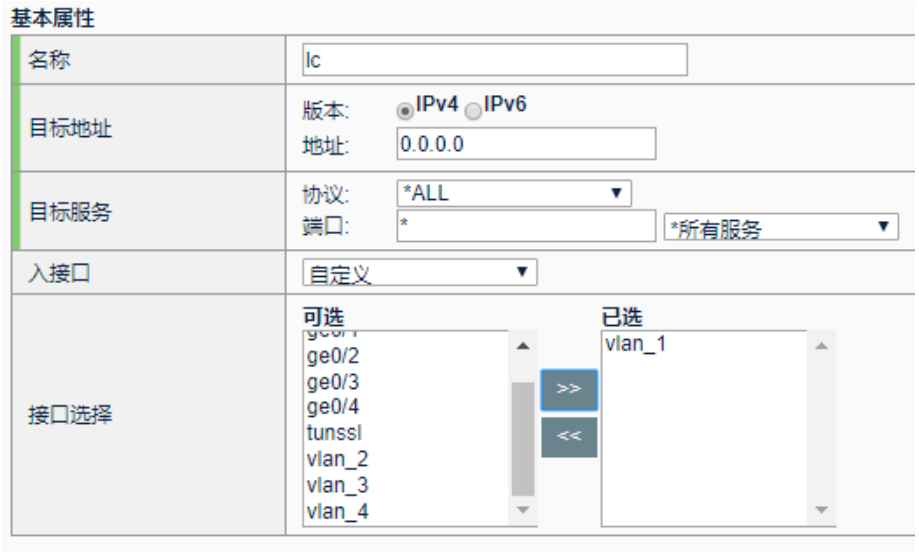

移动链路的优先级最高，当匹配到该链路池所对应的路由策略时，使用优先级最高的链路作为出链路；当发生拥塞的时候使用次优先级的链路作为出链路，电信和网通的优先级都为 1，可以实现当移动链路发生拥塞时，将流量均匀引导到电信和网通链路上

**默认链路池**


默认链路池被虚拟链路的默认链路池引用，当报文未匹配到路由策略时，可以均匀的将流量转发到不同的链路中

5. 进入**链路负载>虚拟链路**。创建**虚拟链路 - "lc"**。

**基本属性**


基本属性
名称
lc
目标地址
版本:
IPv4
IPv6
地址:
0.0.0.0
目标服务
协议:
*ALL
端口:
*
*所有服务
入接口
自定义
接口选择
可选
ge0/2
ge0/3
ge0/4
tunssl
vlan_2
vlan_3
vlan_4
>>
<<
已选
vlan_1

## 基础配置


配置:
基础
源NAT地址池
自动映射
路由策略:
移动
链路池:
移动
添加
引用路由策略
电信:电信
网通:网通
移动:移动
上移
下移
移除
默认链路池
默认
默认会话保持模板
无
备选会话保持模板
无

## 高级选项


## 37.4 常见故障分析

### 37.4.1 TCP报文访问直连主机无法建立连接

| | |
|---|---|
| 故障现象 | TCP报文通过虚拟链路选路访问直连主机无法建立连接 |
| 分析 | 当SYN报文通过选路到达网关，该网关设备可能是防火墙设备，转发给直连主机，直连主机直接绕过网关设备进行SYN+ACK应答。此时网关设备无法建流，所以当ACK报文到达网关设备的时候无法转发，直接丢弃，导致TCP无法完成三次握手 |
| 解决 | 如需通过虚拟链路访问与ADC直连的主机，建议开启直连路由优先即可 |

### 37.4.2 多连接协议数据传输失败

| | |
|---|---|
| 故障现象 | 多连接报文的反向子连接报文选路与主连接不同，导致数据传输失败 |
| 分析 | 对于多连接协议，反向子连接的正向报文通过路由选路，假如配置了多条等价路由，出接口可能与正向主连接的入接口不同，若到客户端的过程中串接着其他基于流的设备（例如防火墙），在没有建立主连接的情况下去建立子连接，这样可能导致子连接建立失败，最终无法传输数据 |
| 解决 | 如需处理只有一级子连接的多连接协议，建议勾选路径一致性 |

# 38 第38章 链路池

## 38.1 链路池概述

通常在出口多链路的环境中，会定义链路节点和链路池来实现多链路负载均衡和链路备份的功能。链路池是链路成员的集合，链路成员表示单条链路，通常把多个备份链路加入同一个链路池。在虚拟链路的配置中，可以通过引用链路池把流量按比例分配到不同的链路上。

## 38.2 创建链路池

链路池中可以指定健康检查算法、负载均衡算法和链路成员。

**配置步骤：**

1. 进入**链路负载>链路池**，点击**新建**，如下图：


**名称：**为新建链路池设置名称。

**健康检查方法选择：**为新建链路池选择健康检查方法，可选的健康检查方法参见健康检查章节。

**有效性：**配置链路成员健康检查通过的有效条件，可以选择：

至少：当健康检查通过数量不少于指定数量时，认为该链路成员可用。

所有：当健康检查全部通过时，认为该链路成员可用。

**健康检查失败动作：**配置链路成员健康检查失败时的动作。可选动作和服务池相同。

**负载均衡算法：**配置链路成员的调度策略。可选算法和服务池负载均衡算法基本相同，同时额外支持最小延时，最小抖动，最小丢包率算法。当链路池采用最小延时、最小抖动或最小丢包率算法进行调度时，对应链路池需引用检查类型为 icmp 质量检查的健康检查模板（模板具体配置为类型选择 icmp，应用范围选择链路质量）。

**低优先级组激活：**配置低优先级组激活的条件。当高优先级组内的可用链路成员数量少于指定的数量时，低优先级组内的链路成员被激活，参与计算。默认不可用。

**链路成员：**添加新的链路成员。指定新建链路成员的地址，点击**添加**。链路成员地址可以选择：

新地址：配置链路成员的 IP 地址。

链路列表：选择一个已经配置的链路节点。

2. 点击**提交**。

注意

当链路池中的可用成员总数少于低优先级组激活的可用成员数时，链路池中的所有链路成员都无法被调度。

## 38.3 编辑链路池配置参数

对于已经创建的链路池，可以修改基本配置参数。

**配置步骤：**

1. 进入**链路负载 >链路池**，点击链路池名称。
2. 进入**配置参数**，如下图：


**状态：**显示链路池的实时状态。

3. 点击**更新**。

## 38.4 创建链路成员

在已经创建的链路池中，可以新建链路成员。

**配置步骤：**

1. 进入**链路负载>链路池**，点击链路池名称。
2. 进入**链路成员**，如下图：


3. 点击**新建**


**地址类型：**可以根据链路成员的 IP 地址格式。选择使用 IPv4 地址或者使用 IPv6 地址

**地址：**指定新建链路成员的地址，可以选择：

**新地址：**配置链路成员的 IP 地址。

**链路列表：**选择一个已经配置的链路节点。

**权重**：配置链路成员在链路池中的权重，用于基于成员的负载均衡算法。

**优先级组**：指定链路成员在链路池中的优先级组别。

**连接限制**：指定链路成员的连接限制。

**健康检查**：配置链路成员的健康检查方法，可以选择：

**无**：不进行健康检查。

**继承自链路池**：使用和链路池相同的健康检查方法。

**自定义**：为链路成员配置自己的健康检查方法。

4. 点击**提交**。


注意

1. 自定义健康检查方法后，不再继承链路池的健康检查方法。

## 38.5 编辑链路成员

对于已经创建的链路成员，可以修改配置。

**配置步骤：**

1. 进入**链路负载>链路池**，点击链路池名称。
2. 进入**链路成员**，点击链路成员名称。


**父节点状态：**显示链路成员对应的链路节点的状态。

**状态：**显示链路成员的状态。

**健康检查结果：**显示链路成员的健康检查结果。

**状态调整：**手动修改链路成员的状态。

3. 点击**更新**。


当用户新建一个链路成员时，系统会自动生成一个链路节点，该链路节点为链路成员的父节点。

## 38.6 配置案例

### 38.6.1 新建链路池

**案例描述**

增加一个链路池，包含两条出口链路，使用轮询算法在两条链路中选路。

**配置步骤：**

1. 进入**链路负载>链路池**，点击**新建**，如下图：

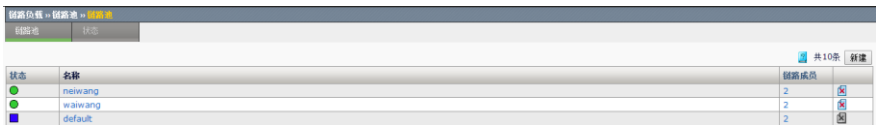

2. 输入参数。

3. 点击**提交**完成设置。

# 38.7 链路池监控与维护

## 38.7.1 查看链路池

点击**链路负载>链路池**，如下图：




点击**链路负载>链路池**，切换到**状态**，如下图：


## 38.7.2 查看链路成员

点击**链路负载>链路池**，点击已经创建的链路池名称，点击**链路成员**，如下图：

# 39 第39章 链路节点

## 39.1 链路概述池

通常在出口多链路的环境中，会定义链路节点和链路池来实现多链路负载均衡和链路备份的功能。

链路节点表示单条链路，链路池是单条链路的集合，可以包含多个链路节点。

## 39.2 创建链路节点

链路节点中可以指定健康检查算法、权重和上下行带宽。

**配置步骤：**

1. 进入**链路负载>链路节点**，点击**新建**，如下图：


**参数说明：**

**地址类型：**可以根据链路节点的 IP 地址格式。选择使用 IPv4 地址或者使用 IPv6 地址

**地址：**指定新建链路节点的 IP 地址。

**名称：**为新建链路节点的设置名称。

**健康检查方法选择：**为新建链路池选择健康检查方法，可以选择：

**无：**不对链路节点做健康检查。

**默认：**使用健康检查默认模板。

**自定义：**使用自定义健康检查方法，可选的健康检查方法参见健康检查章节。

**权重：**配置链路节点的权重，用于基于节点的负载均衡算法。

**上行带宽：**配置链路节点的上行带宽。

**上行带宽阈值上限：**当链路节点的上行流量超过上行带宽阈值上限时，该链路节点不再参与调度。

**上行带宽阈值下限：**当链路节点的上行流量低于上行带宽阈值下限时，该链路节点可以重新参与调度。

**下行带宽：**配置链路节点的下行带宽。

**下行带宽阈值上限：**当链路节点的下行流量超过下行带宽阈值上限时，该链路节点不再参与调度。

**下行带宽阈值下限：**当链路节点的下行流量低于下行带宽阈值下限时，该链路节点可以重新参与调度。

**连接限制：**配置链路节点的连接限制。

2. 点击**提交**。


当用户新建一个链路成员时，系统会自动生成一个链路节点，该链路节点为链路成员的父节点。

## 39.3 编辑链路节点

对于已经创建的链路节点，可以修改配置。

**配置步骤：**

1. 进入**链路负载>链路节点**，点击 1.2 中创建好的链路节点名称，如下图：


**状态：**显示链路节点的实时状态。

**状态调整：**手动修改链路节点的状态。

2. 点击**更新**。

## 39.4 配置案例

### 39.4.1 新建链路节点

**案例描述**

增加一个链路节点，上下行带宽分别为 100M。

**配置步骤：**

1. 进入**链路负载>链路节点**，点击**新建**，如下图：

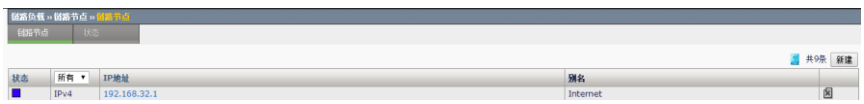

2. 输入参数。

3. 点击**提交**完成设置。

## 39.5 链路节点监控与维护

### 39.5.1 查看链路节点

点击**链路负载>链路节点**，如下图：



# 40 第40章 DNS 代理

## 40.1 DNS代理概述

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

## 40.2 配置DNS代理

### 40.2.1 配置服务器

1. 进入**链路负载>DNS 代理>服务器**，如下图所示：


**IP 地址**：DNS 服务器地址。

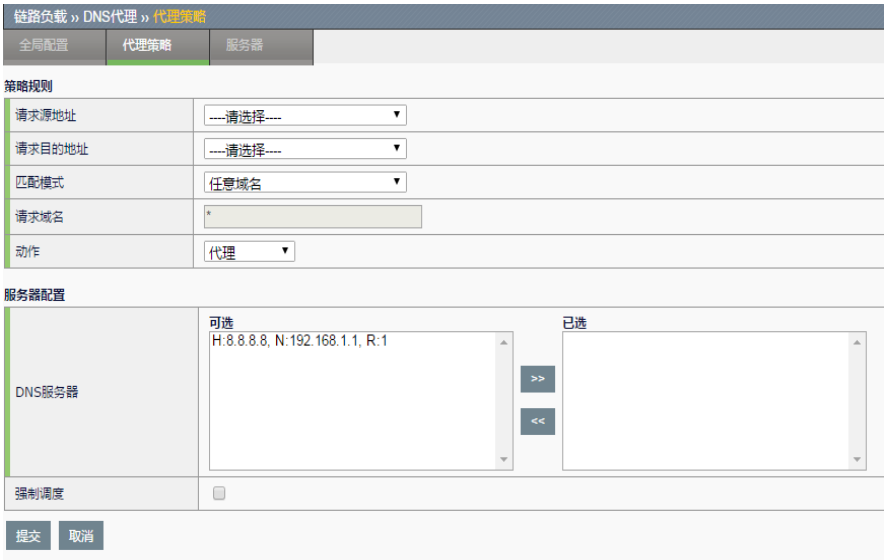
**下一跳地址**：到达 DNS 服务器选择的下一跳地址，此选项只能从链路节点中选择。

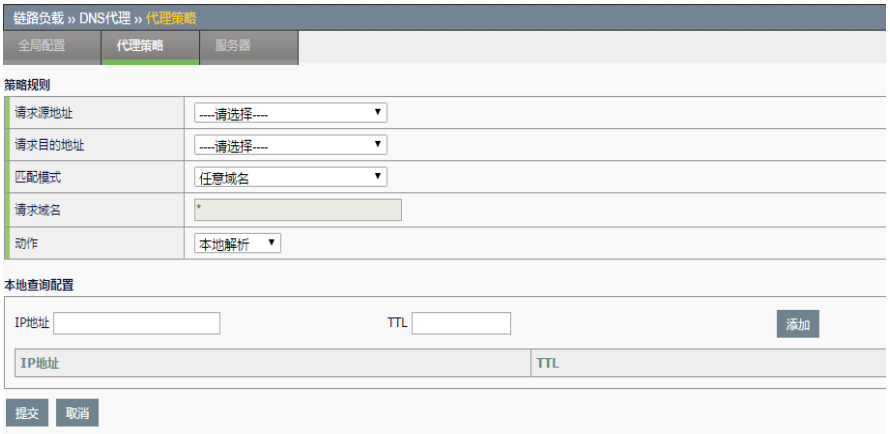
**权值**：当前 DNS 服务器的权值或优先级，取值范围[1,100]。

2. 根据需要修改参数。
3. 点击**确定**，提交配置。

### 40.2.2 配置代理策略

1. 进入**链路负载>DNS 代理>代理策略**，如下图所示：




**策略规则配置参数说明：**

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

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

**匹配模式**：任意域名、包含、完全匹配、域名地址库。

**请求域名**：DNS 报文请求的域名。

**域名地址库**：引用的域名地址库名字。

**动作**：命中策略后是做代理、转发还是本地解析。

**服务器配置参数说明：**

**DNS 服务器**：命中策略后，如果动作是代理，可以选择的服务器。

**本地查询配置参数说明：**

**IP 地址**：点分十进制，配置 DNS 的域名请求所对应的指定 IP 地址。

**TTL**：DNS 配置的本地解析 IP 地址缓存时间。

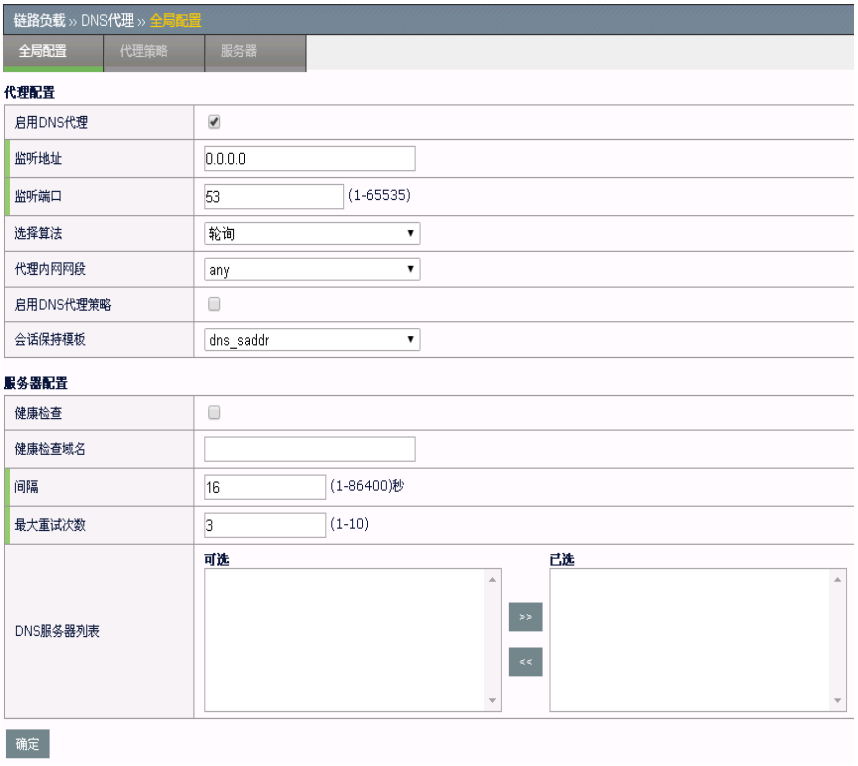
**添加**：添加需要配置的 DNS 本地解析条目（限制范围是 5 条）。

2. 根据需要修改参数。

3. 点击**确定**，提交配置。

### 40.2.3 配置全局配置

1. 进入**链路负载>DNS 代理>全局配置**，如下图所示：




**代理配置参数说明：**

**启用 DNS 代理**：用于设定是否启用 DNS 代理功能。

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

**监听端口**：用来设定监听的 DNS 服务器的端口，默认为 53 端口。

**选择算法**：选择服务器的算法，包含轮询，加权轮询，加权最小流量，优先级。

**代理内网网段**：选择需要代理的源 IP 地址对象。

**启用 DNS 代理策略**：默认不勾选。勾选后，DNS 代理>代理策略页面配置的内容生效。

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

**服务器配置参数说明：**

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

**服务器健康检查域名**：要检查的 dns 域名。

**间隔**：DNS 服务器列表中服务器进行健康检查的间隔时间，默认为 16 秒。

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

**DNS 服务器列表**：选择使用的 DNS 服务器。

2. 根据需要修改参数。

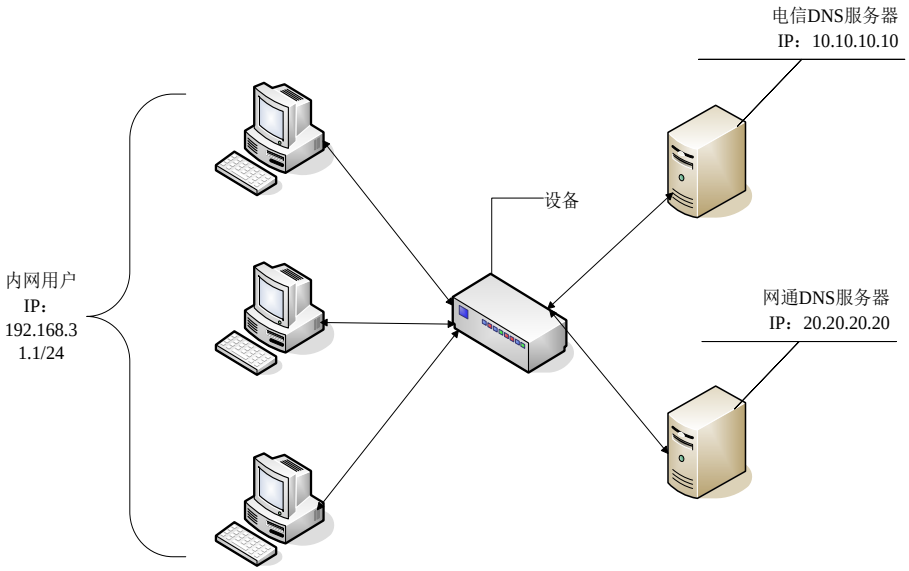
3. 点击**确定**，提交配置。

## 40.3 配置案例

### 40.3.1 DNS代理配置案例1

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

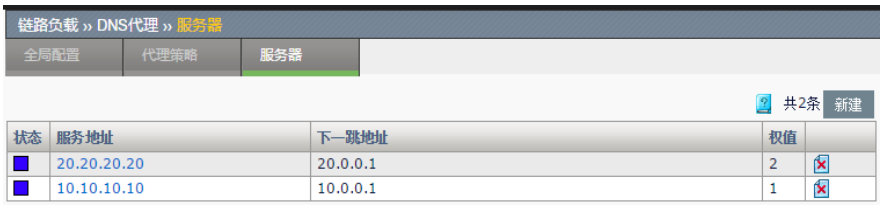
**配置步骤：**



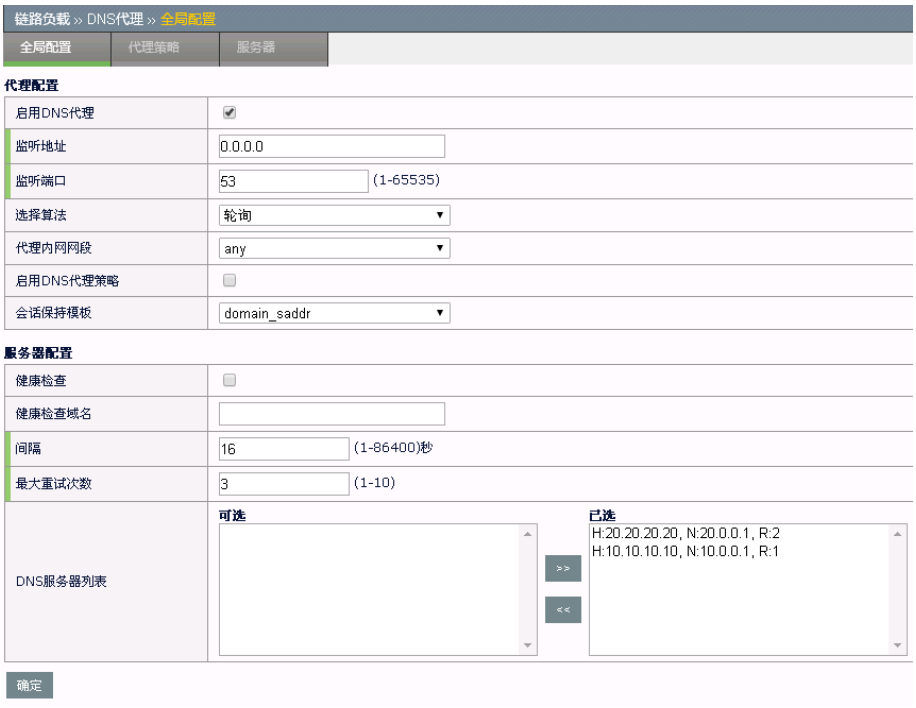

1. 配置虚拟链路，虚拟链路设置参考对应章节，要保证内网用户流量可以通过虚拟链路正确访问外网。
2. 配置参数如下：

2.1 配置**服务器**





2.2 配置**全局配置**



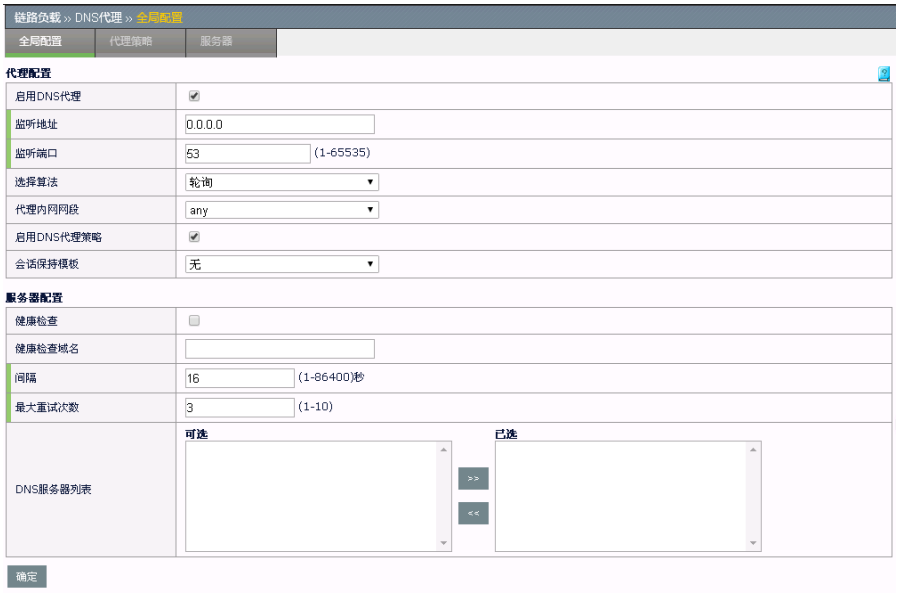

## 40.3.2 DNS代理配置案例2

设备配置了一条虚拟链路，并在虚拟链路中勾选 DNS 代理关联，这时如果没有配置本地解析功能的 DNS 策略，用户会根据电脑配置的 DNS 地址或通过我们的负载均衡设备匹配 DNS 代理策略和全局配置进行 DNS 请求转发，设备会根据设定的调度策略选择合适的 DNS 服务器并把解析后的地址返回给用户；而如果配置了 DNS 本地解析功能，那么用户发出的 DNS 请求就不会发往 DNS 服务器进行解析，而是根据本地的手动配置进行 DNS 的 A 记录请求的解析，并把解析后的地址返回给用户，这样就可以省去访问 DNS 服务器进行域名解析的过程。

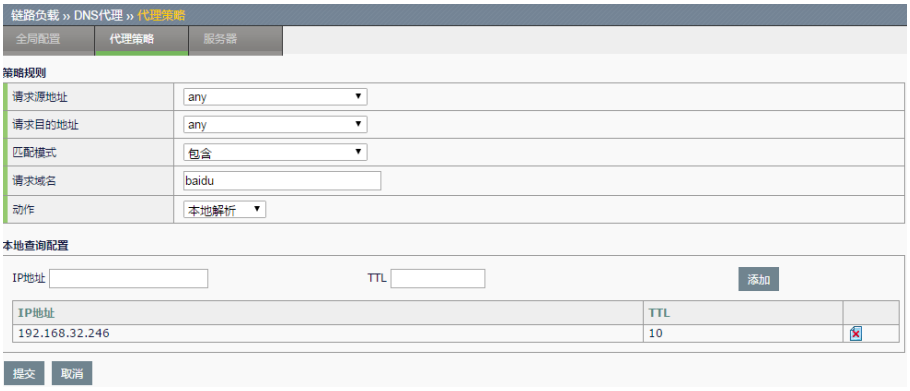
**配置步骤：**

1. 配置虚拟链路，虚拟链路设置参考对应章节，要保证在虚拟链路中勾选 DNS 代理关联，此案例配置的虚拟链路可以通过虚拟链路正确访问外网。
2. 配置参数如下：

2.1 配置**全局配置：**




2.2 配置本地解析代理策略并勾选**启用**：





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

# 41 第41章 动态就近性

## 41.1 动态就近性概述

动态就近性作为链路池的一种算法，通过动态收集到达同一目的主机各条链路上的延迟，来选择出一条最快的出链路进行转发。

动态就近性算法分为被动探测和主动探测两种。主动探测收集延迟准确，收敛迅速。当设备性能宽裕时，建议使用主动探测。


当没有匹配到路由策略的会话，会命中到默认链路池。动态就近性算法多用在默认链路池里。

## 41.2 配置动态就近性

动态就近性分为探测配置和算法开启两部分：

1. 探测配置是全局生效，即对所有链路地址池选中的动态就近性算法生效。动态就近性存在默认配置，用户可以根据实际的网络情况对该配置进行编辑。

2. 算法开启对选择动态就近性算法的链路地址池生效。

### 41.2.1 配置动态就近性参数

1. 进入**链路负载>动态就近性**，如下图：


**探测掩码**：指定探测掩码，不同目的地址在同一掩码范围内时，按同一动态就近性探测和选路，默认为 255.255.255.0。

**探测时间**：指定采集延迟的时间范围，时间到达之后计算出每条链路到达不同地址范围的延迟值，默认为 10 秒。

**缓存刷新周期**：指定清空所有延迟统计的时间间隔，默认为 7200 秒。

**最大响应延迟**：设定超时时间，超过该值的会话不参与延迟统计，默认为 5000 秒。

**主动探测**：设备主动探测各条链路的延迟，开启该功能时，需要配置探测次数，默认开启。

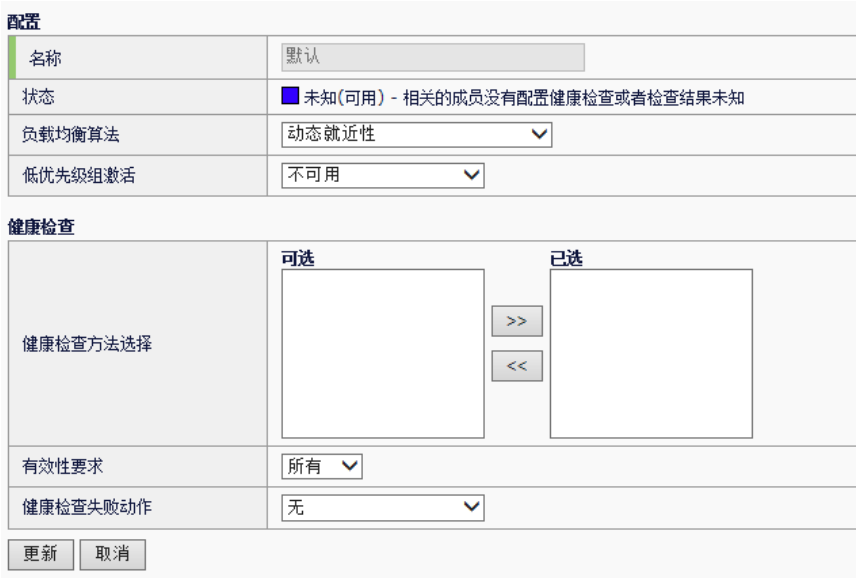
**探测次数**：对于同一目的地址各条链路的探测次数，默认为 2。

2．点击**确定**。

### 41.2.2 启用动态就近性

动态就近性是一种独立的算法，在链路地址池中选择。配置步骤如下：

1. 进入**链路负载>链路池**，编辑**默认链路地址池**。




2. 点击**更新**。

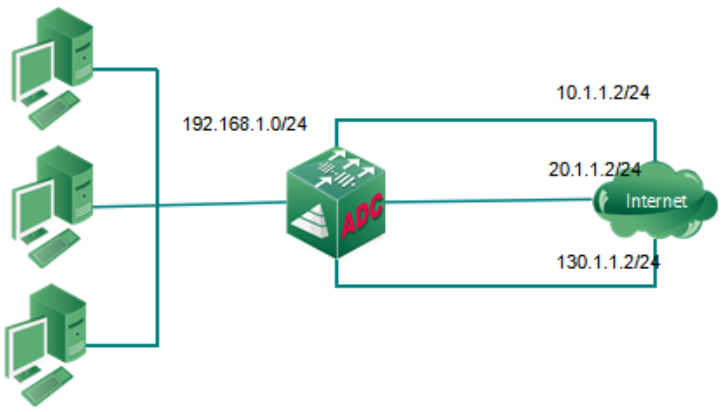
## 41.3 配置案例

### 41.3.1 配置动态就近性案例 1

**案例描述：**

企业通过 ADC 访问外网，现有三条分属于不同运营商的出链路：电信、网通和移动。在虚拟链路中会根据实际网络情况配置不同的路由策略，目的性的将已知报文转发到指定的链路中。希望不通过路由策略选路的流量，在三条链路中选择最快的一条链路作为出链路。

**配置步骤：**




1. 配置虚拟链路，虚拟链路设置参考对应章节，要保证内网用户流量可以

通过虚拟链路正确访问外网，并根据需求合理配置路由策略。

2. 进入**链路负载>链路池**，新建**默认链路池**“**default**”。


3. 进入**链路负载>虚拟链路**，编辑**虚拟链路**“**VLINK**”。


在虚拟链路中，通过默认链路池引用 default，可以将没有匹配到策略路由的流量，通过动态就近性选择一条最快的链路作为出链路。

# 42 第42章 智能 DNS

DNS 包含传统 DNS 服务器和 DNS 智能解析两部分主要功能，在提供负载分担的同时，也可用于内网用户的日常 DNS 解析。

智能解析包括本地负载和全局负载。对于单一站点入站链路分担的基本需求，通过配置本地负载功能可以满足。对于全局范围的多站点之间流量的分担，需要进行全局负载部分的配置，并且在功能上，全局负载覆盖了所有本地负载的功能。

DNS 服务器包括本地记录解析、转发解析以及本机递归解析三种解析方式，最大程度地将每一个 DNS 请求的正确网络资源返回给客户端。其中本地记录解析支持多种 DNS 记录类型。转发解析则在普通 DNS 服务器转发功能的基础上，新增智能转发功能，大大提高了 DNS 的解析效率。

通过监听地址接口收到的 DNS 请求，首先进入全局负载模块进行智能解析，全局负载域名匹配失败或解析失败后，进入本地负载模块进行智能解析，本地负载域名匹配失败或者解析失败后，进行本地记录解析，本地记录解析失败后进入转发解析，如果再次失败，且转发模式为优先转发，则进行本机主动递归解析，最终将解析结果返回请求端。

## 42.1 DNS服务器

### 42.1.1 概述

DNS 服务器是集成了本地多类型记录解析、转发解析以及递归解析多种 DNS 解析方式，致力于在设备性能开销相对最低的情况下，提供内网用户的 DNS 解析服务，满足一般局域网内部用户的日常 DNS 需求。

其中 DNS 转发功能，结合多种负载算法、对转发服务器的动态探测以及链路关联的影响，实现智能转发，使得每一次 DNS 解析请求都能得到最快的响应速度和最佳的响应内容。

同时本模块也是智能 DNS 的基础部分，提供整体 DNS 功能的基础配置，控制智能 DNS 的总体解析流程。

### 42.1.2 基础配置

进入**智能 DNS > DNS 服务器>基础配置**。


**监听地址**：配置监听 DNS 请求的设备接口地址，同时支持 ipv4 和 ipv6 类型。

**探测方法**：配置当智能解析调度算法为动态就近性时，获取动态数据的探测方法，可选的方法包括 ICMP、根查询和反向查询：

- **ICMP**：发送 ICMP 回显探测；
- **根查询**：发送查询根记录的 DNS 请求报文；
- **反向查询**：向 LDNS 发送该 LDNS IP 地址的反向查询请求（即 PTR 记录查询）。

**全局智能解析失败丢弃**：勾选该选项后，全局智能解析失败的 DNS 请求，将其丢弃，不返回请求端任何 DNS 响应报文

**本地智能解析失败丢弃**：勾选该选项后，本地智能解析失败的 DNS 请求，将其丢弃，不返回请求端任何 DNS 响应报文

**全局通信**：置空该选项后，用于全局负载的本地数据中心与远程数据中心间将不会进行通信，对已连接的数据中心不会影响。

**接受远程配置同步**：置空该选项后，将不再接受远程数据中心发送过来的配置。

**配置步骤：**

1. 配置**监听地址**：在左侧对话框选中想要监听 DNS 请求的设备 IP 地址，点击 

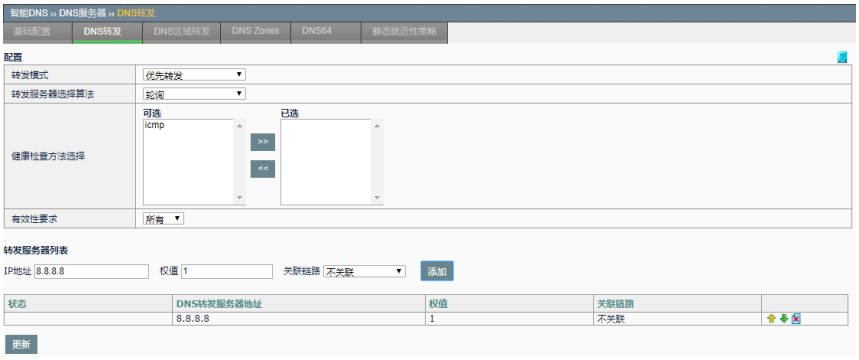
按钮选入到右侧对话框中。
2. 在探测方法下拉列表中，选中需要的**探测方法**。
3. 勾选或者置空**全局智能解析失败丢弃**选项。

4. 勾选或者置空**本地智能解析失败丢弃**选项。
5. 勾选或者置空**全局通信**选项。
6. 点击**更新**，提交配置。

### 42.1.3 配置DNS转发

当 DNS 通过本地解析失败后，可以根据 DNS 转发模块的配置将其转发到其他 DNS 服务器进行解析，或者通过本地主动递归的方式进行解析，转发时可以根据选择的算法智能地将 DNS 请求转发到不同的服务器上，同时可对转发服务器做健康检查，并将其关联到某一指定链路，根据转发服务器的健康状态和链路状态来决定转发服务器的可用状态。

进入**智能 DNS>DNS 服务器>DNS 转发**。




**转发模式**：不同的转发模式，DNS 请求将采用不同的解析方式，共有三种转发模式：

- **关闭**：关闭转发功能，关闭本地递归解析功能和转发功能；
- **只转发**：本地解析（包括全局智能解析、本地智能解析和本地记录解析）失败的 DNS 请求将转发到转发服务器列表中的某台服务器进行解析；
- **优先转发**：在只转发的基础上，如解析仍失败，则采取本机亲自递归查询的方式解析 DNS 请求。

**转发服务器选择算法**：配置转发 DNS 请求时，选择哪个服务器做转发的方法，可供选择的方法包括无、轮询、加权轮询以及静态就近性：

- **无**：不配置算法，在每个 DNS 服务器都转发过的基础上，优先选择 DNS 转发服务器响应环回时间较短的进行转发。
- **轮询**：依次返回可用转发地址。
- **加权轮询**：按各转发服务器权重比例返回各 IP 地址。
- **静态就近性**：根据请求 DNS 源 IP 所在子网段、ISP、用户区域、省或市，返回一定的转发服务器地址，需结合静态就近性策略的配置。

若静态就近性表项匹配失败，则请求域名不进行转发。

**健康检查**：配置的健康检查方法将对转发服务器列表中的每台 DNS 转发服务器进行探测，监视他们的健康状态，可以配置的健康检查模板只有 ICMP 以及 DNS 两种类型。

**有效性要求**：配合健康检查，指定可以通过的最小健康检查个数。

**转发服务器**：配置转发服务器时，需要指定三类信息：

- **IP 地址**：转发服务器的 IP 地址；
- **权值**：当转发服务器算法选择加权轮询时，按照该权值进行转发服务器之间的调度；
- **关联链路**：可以将设备某一入站链路的健康状态与转发服务器关联。

**配置步骤**：

1. 在**转发模式**下拉列表中选择期望的转发模式。
2. 在**转发服务器选择算法**下拉列表中选择期望的算法。
3. 在**健康检查方法**左侧列表中将期望的模板选到右边框中，同时在配置该部分健康检查的**有效性要求**个数。
4. 将每一个将要添加的**转发服务器**的 IP 地址，权值，是否关联链路或者关联到某一指定链路的信息分别添加到对应位置，点击**添加**加入到列表中，如需修改或者从列表中移除，则可点击已添加列表中对应列的 进行删除。
5. 确定所有配置信息无误后，点击**更新**，提交配置使其生效。

### 42.1.4 配置DNS区域转发

通过配置 DNS 区域转发，能够实现将特定区域下的域名查询转发到指定的服务器。

进入**智能 DNS>DNS 服务器>DNS 区域转发**，

点击**新建**，进入 DNS 区域转发新建页面：

**名称：**需要转发的区域名称。

**转发服务器列表：**将匹配区域的域名转发查询的服务器地址列表。

**配置步骤：**

1. 配置**名称。**
2. 配置**转发服务器列表。**


注意

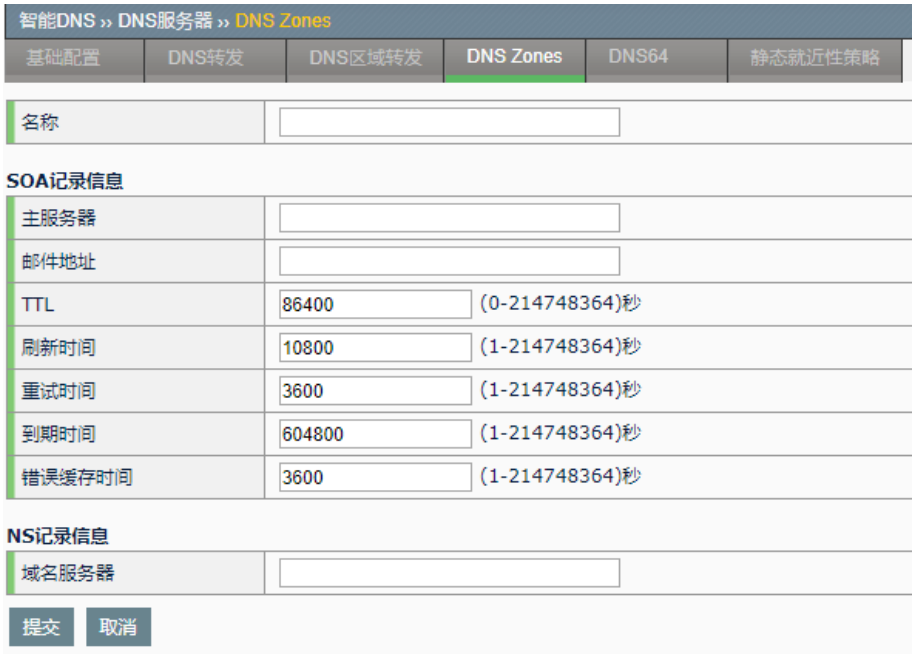
DNS 区域转发的匹配优先于 DNS 转发。

### 42.1.5 配置DNS记录

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

进入**智能 DNS>DNS 服务器> DNS Zones**，


点击**新建，**进入 zone 的新建页面：




**名称：**zone 的域名。

**主服务器：**该 zone 的主域名服务器名称。

**邮件地址：**该 zone 的联系邮件地址。

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

**刷新时间：**soa 记录的 refresh 值，用于该 zone 的辅域名服务器从主域名

服务器同步 zone 文件的周期时间。

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

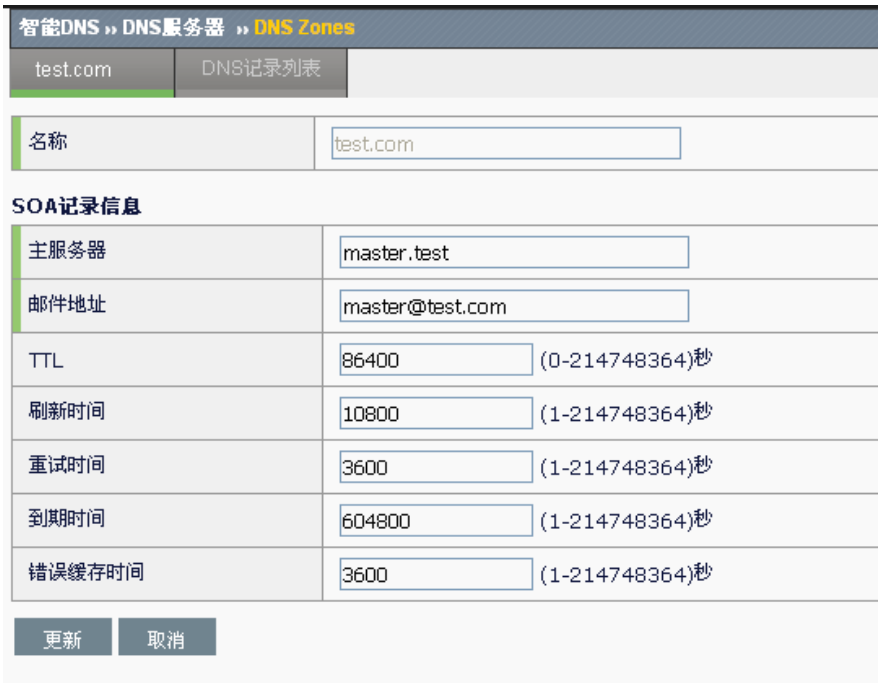
**到期时间**：soa 记录的 expire 值，若辅域名服务器与主域名服务器通信失败时间超过该值，则认定该 zone 失效。

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

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

**配置步骤：**

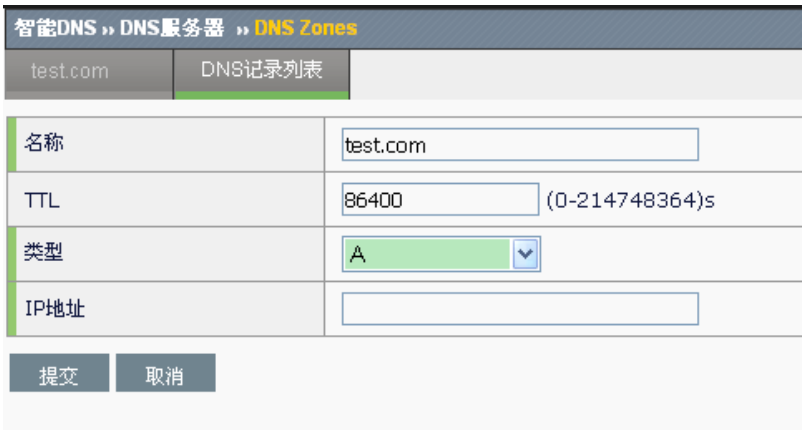
1. **添加**时，在所有配置项添入对应内容后，点击**提交。**
2. 当需要**修改**以上某项内容（除 zone 名称）时，在 zone 列表点击对应的 zone 名称，进入到如下页面：




在对应位置添入修改后的信息，点击**更新**，使得修改内容生效。

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


4. 点击新建，进入新建该 zone 的 DNS 记录的页面。




**名称**：记录名称。

**TTL**：当前记录的 ttl 值。

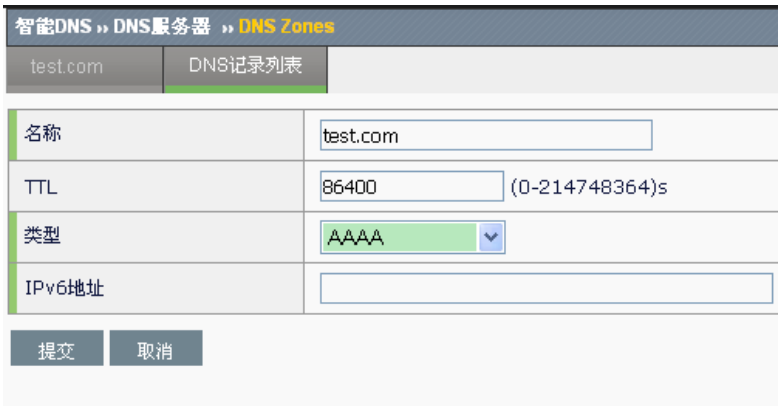
**类型**：记录类型，目前共支持 A、AAAA、NS、CNAME、MX、TXT 以及 PTR7 种类型：

**A**：ipv4 地址类型记录。

**IP 地址**：记录名对应的 IP 地址。


**AAAA**：ipv6 地址类型记录。

**IPv6 地址**：记录名对应的 IPv6 地址。

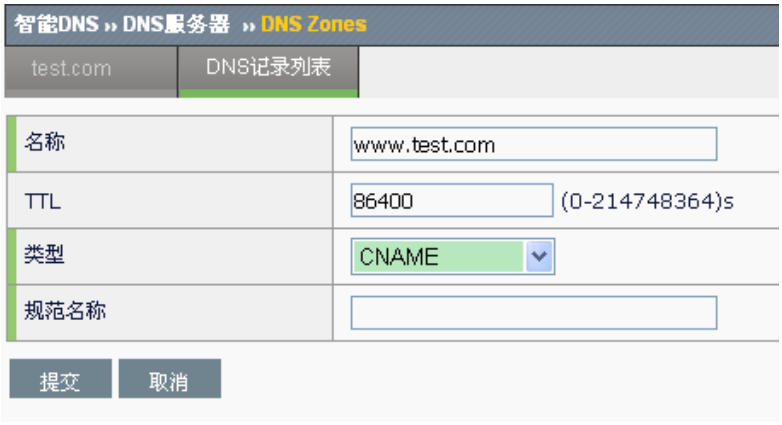



**NS**：域名服务器记录。

**域名服务器**：记录名称表示的 zone 对应的权威域名服务器名称。


**CNAME**：规范名记录。

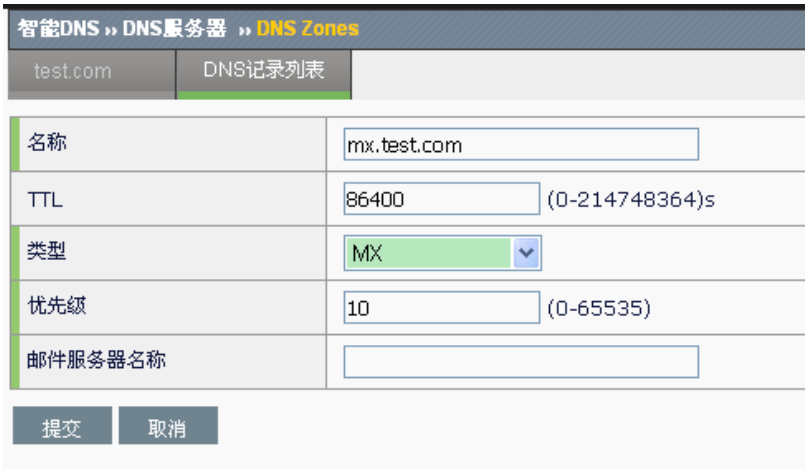
**规范名称**：记录名称表示的别名所对应的规范域名名称。




**MX**：邮件中转站记录。

**优先级**：选择 mx 记录的优先级，数值越小，优先级越高。

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

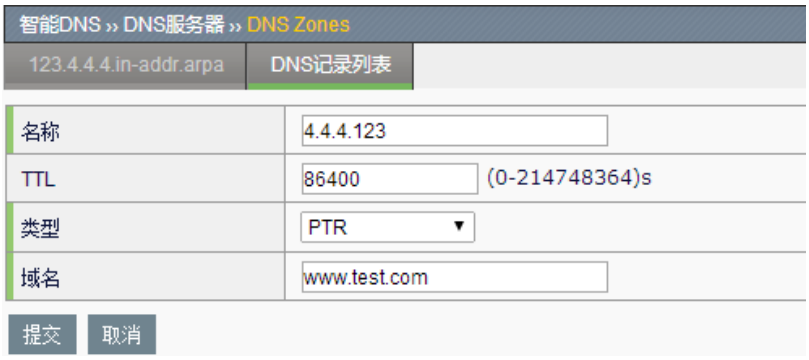



**TXT**：文本类记录。

**文本内容**：记录名称对应的一段文本信息，可由该 zone 管理员自定义，表示任意内容。


**PTR**：反向查询记录。

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




**配置步骤：**

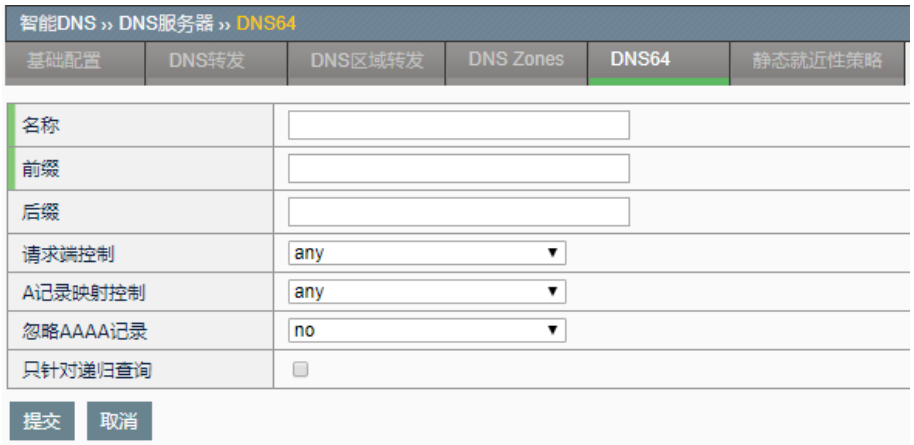
1. **新建** dns 记录，在新建页面从类型下拉列表选中新建记录类型，一次填入记录名称、ttl 值以及记录数据，点击提交。
2. **删除** dns 记录，在 zone 的记录列表页面点击想要删除记录一行的 ，删除该记录。

### 42.1.6 配置DNS64

DNS64 将 DNS 查询信息中的 A 记录（IPv4 地址）合成到 AAAA 记录（IPv6 地址）中，返回合成的 AAAA 记录用户给 IPv6 侧用户。

进入**智能 DNS>DNS 服务器>DNS64**，如下，为 DNS 服务器的 DNS64 策略管理界面如下。


点击**新建**，进入新建 DNS64 策略页面。




**名称：**DNS64 策略的名称。

**前缀：**将 A 记录转换为 AAAA 记录所使用的前缀。

**后缀：**将 A 记录转换为 AAAA 记录所使用的后缀。

**请求端控制**：如果配置，则只处理属于请求端地址列表中的地址发送的请求。

**A 记录映射控制**：如果配置，则只有在返回的 A 记录属于 A 记录映射控制列表中的地址才进行转换。

**忽略 AAAA 记录**：如果配置，则忽略列表中配置的 AAAA 记录地址，并进行 DNS6 转换。

**只针对递归查询**：如果选中，则只在进行递归查询时才进行 DNS64 转换。

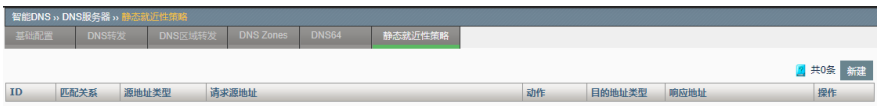
**配置步骤：**

1. 输入**名称**。
2. 输入**前缀**。
3. 点击**提交**。

### 42.1.7 配置静态就近性策略

本小结的静态就近性策略支持 DNS 转发算法中静态就近性算法的使用。

进入**智能 DNS>DNS 服务器>静态就近性策略**，如下，为 DNS 服务器的静态就近性策略列表。




**ID**：静态就近性策略 ID，用于标识每条静态就近性策略。

**匹配关系**：指定发来请求的 LDNS 的源地址与策略源对象是否应该匹配。

**源地址类型**：指定匹配源地址的类型，包括 IP 子网段、ISP、用户区域、省和市 5 种类型。

**请求源地址**：指定发来请求的 LDNS 的源地址需属于（或不属于）的 IP 子网（或 ISP 地址库、省、市、用户区域）。

**动作**：当源地址部分匹配策略指定的条件时，最终响应动作与策略指定响应地址之间的逻辑关系，响应所指定的目的地址，或者响应非所指定目的地址。

**目的地址类型**：指定响应的目的地址类型，目前包括 IP 子网段和用户区域两种类型。

**响应地址**：指定具体的响应目的地址。

点击右侧操作栏中的  或者  ，调整策略顺序，调整结束后点击**确定**完成操作。

点击右侧操作栏中的  ，删除指定策略。

点击**新建**，进入新建 DNS 服务器静态就近性策略页面。


**配置步骤：**

输入策略 **ID**，范围为 1-65535，或者不配置该项，系统则自动为该条策略分配 ID。

1. 指定源地址与源地址对象的**匹配关系**（**属于**，**不属于**）。
2. 指定**源地址匹配对象类型**，IP 子网段，ISP 地址库，省，市，用户区域。
3. 在下一个对话框输入需**源地址匹配的对象**
   a) 当源地址匹配对象类型选择 **IP 子网段**，该部分以 A.B.C.D/M 的格式输入具体 IP 网段地址，A.B.C.D 为 IP 地址，M 为子网掩码长度；
   b) 当源地址匹配对象类型选择 **ISP**，该部分则从设备的 ISP 地址库下拉列表选中期望的对象。
   c) 当源地址匹配对象类型选择**用户区域**，该部分则从用户区域下拉列表选中期望的对象。
   d) 当源地址匹配对象类型选择**省**，该部分则从国内省级地区的下拉列表选中期望的对象。
   e) 当源地址匹配对象类型选择**市**，首先从国内省级地区的下拉列表选中期望城市所在的省份，再从对应省份的城市列表中选择期望的城市。
4. 选择**响应动作**为**响应**，或者**不响应**。
5. 指定**目的对象类型**，IP 子网段，用户区域。
6. 在下一个对话框输入需**目的匹配的对象**
   a) 当源地址匹配对象类型选择 **IP 子网段**，该部分以 A.B.C.D/M 的格式输入具体 IP 网段地址，A.B.C.D 为 IP 地址，M 为子网掩码长度；
   b) 当源地址匹配对象类型选择**用户区域**，该部分则从**用户区域**下拉列表选中期望的对象。
7. 点击**提交**。

注意

同一个 ID 的静态就近性策略，只能配置一条，当 ID 不同时，对应源和目的相同内容也只能配置一条策略。

## 42.2 本地负载

### 42.2.1 概述

本地负载通常在提供服务的单一站点内，通过指定域名的智能 DNS 解析，对入站流量的访问进行负载。用户发送对某指定域名的 DNS 请求，该请求最终发往 ADC 设备，本地负载模块根据配置，综合考虑用户所处运营商网络、动态探测时间、或者当前链路带宽质量等多种因素，返回虚拟服务地址，用户根据返回的 IP 地址，对服务进行访问，从而智能的分配入站流量。

本地负载支持动态就近性、静态就近性、轮询、加权轮询、全局可用性、最小连接数、最小带宽、备选 IP 等数十种负载均衡算法，结合动态权值功能，最大限度的根据用户当前需求灵活地实现入站负载。

同时，通过健康检查，探测物理链路的连通性，结合链路的当前流量带宽统计，获得当前链路的实际状况，准确的响应 DNS 请求，和服务器负载均衡配合使用，引导后续业务流量使用当前最优的服务器业务入口。

### 42.2.2 配置静态就近性策略

当域名映射（参见下一小节）选择算法为静态就近性时，算法调度的依据是在该配置项配置的一个或多个静态就近性策略。

进入**智能 DNS >本地负载>静态就近性策略**。


**ID**：静态就近性策略 ID，用于标识每条静态就近性策略。

**匹配关系**：指定发来请求的 LDNS 的源地址与策略源对象是否应该匹配。

**源地址类型**，指定匹配源地址的类型，包括 IP 子网段、ISP 两种类型。

**请求源地址**：指定发来请求的 LDNS 的源地址需属于（或不属于）的 IP 子网（或 ISP 地址库）。

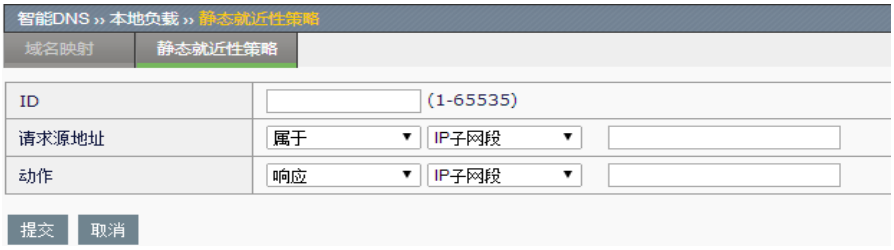
**动作**：当源地址部分匹配策略指定的条件时，最终响应动作与策略之间的逻辑关系，响应所指定的目的地址，或者响应非所指定目的地址。

**响应地址**：指定具体的响应目的地址。

点击右侧操作栏中的  或者  ，调整策略顺序，调整结束后点击**确定**完成操作。

点击右侧操作栏中的  ，删除置顶一条策略。

点击**新建**，进入新建本地静态就近性策略页面。




**配置步骤：**

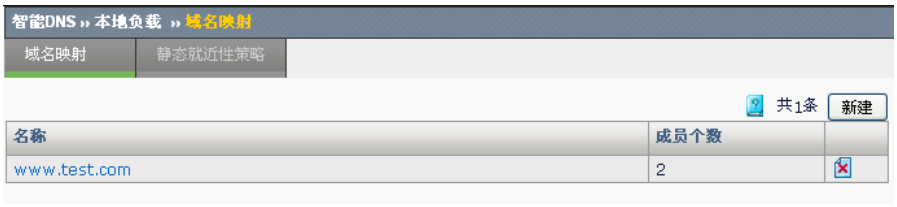
1. 输入策略 **ID**，范围为 1-65535，或者不配置该项，系统则自动为该条策略分配 ID。
2. 指定源地址与源地址对象的**匹配关系**（**属于**，**不属于**）。
3. 指定**源地址匹配对象类型**，IP 子网段，ISP 地址库。
4. 在下一个对话框输入需**源地址匹配的对象**
   a) 当源地址匹配对象类型选择 **IP 子网段**，该部分以 A.B.C.D/M 的格式输入具体 IP 网段地址，A.B.C.D 为 IP 地址，M 为子网掩码长度；
   b) 当源地址匹配对象类型选择 **ISP**，该部分则从设备的 ISP 地址库下拉列表选中期望的对象。
5. 选择**响应动作**为**响应**，或者**不响应**。
6. 在下一个对话框输入需**目的匹配的 IP 子网段**，该部分以 A.B.C.D/M 的格式输入具体 IP 网段地址，A.B.C.D 为 IP 地址，M 为子网掩码长度。
7. 点击**提交**。


同一个 ID 的静态就近性策略，只能配置一条，当 ID 不同时，对应源和目的相同内容也只能配置一条策略。

### 42.2.3 配置域名映射

该配置项对需要进行本地智能解析的域名进行配置，将指定域名与一个或多个 vs 关联起来，当收到对该指定域名的 DNS 请求时，根据配置算法从这些 vs 中选出一个，将对应 IP 的 A 记录返回给请求方，完成智能 DNS 域名解析。

进入**智能 DNS >本地负载>域名映射**，显示当前域名映射列表。




**名称**：域名映射的域名。

**成员个数**：域名映射对应的 vs 个数。

点击**新建**，进入新建域名映射页面。


**配置步骤：**

1. 在**名称**字段输入需要做指定 DNS 解析的域名，域名须符合合法域名。
2. 在 **TTL** 部分输入期望对应该域名的 A 记录的 TTL 值，以秒为单位，缺省为 86400s（1 天），输入范围为 0-2147483647s。
3. 在**会话保持**部分，勾选会话保持表示开启对该域名解析的会话保持功能，并添入期望的会话保持时间，单位为秒，缺省值为 60s，选择会话保持时间为 5-31536000s；不勾选会话保持表示关闭该功能，缺省情况不开启该功能。
4. 选择**负载均衡算法**，分别从**首选算法**和**备选算法**的下拉列表中选择期望使用的对应算法，当选择 vs 时先使用首选算法进行选择，当选取失败时，在利用备选算法进行选择，缺省算法都为轮询。首选算法可选范围为

无、轮询、加权轮询、全局可用性、静态就近性、备选 IP、动态就近性、最小连接数、加权最小链接、最小 pkt/s 以及最小带宽，备选算法可选范围为无、轮询、加权轮询、全局可用性、静态就近性、备选 IP 以及动态就近性。

**无**：不配置算法。

**轮询**：依次返回可用 vs 地址。

**加权轮询**：按各 vs 权重比例返回各 IP 地址。

**全局可用性**：总是返回 vs 列表中第一个可用 vs 的 IP 地址。

**静态就近性**：根据请求 DNS 源 IP 所在子网段或者 ISP，返回一定的 vs 地址，需结合静态就近性策略的配置（参见上一小节 1.1.6 静态就近性策略）。

**备选 IP**：总是返回备选 IP 地址的 DNS 记录，选择该算法时应配置所期望的备选 IP 地址。

**动态就近性**：返回和 LDSN 之间探测时间最短的 vs 地址。

**最小连接数**：返回当前连接数最小的 vs 地址。

**加权最小连接**：综合考虑 vs 权值以及当前连接数，返回当前权值大且当前连接数较小的 vs 地址。

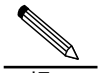
**最小 pkt/s**：以 pkt/s 为参考单位，返回当前包速率最小的 vs 地址。

**最小带宽**：以 bit/s 为单位，返回当前带宽最小的 vs 地址。


注意

当首选算法和备选算法都设置为“无”时，不可能选出 vs 地址进行 DNS 响应。

5. **动态权值**，当算法为最小连接数、加权最小连接、最小 pkt/s 或者最小带宽时，勾选动态权值，按个 vs 当前动态参数比例返回 DNS 响应地址，缺省情况下不勾选该项。


提示

当算法为最小连接数、加权最小连接、最小 pkt/s 或者最小带宽四种动态算法时，推荐启用动态权值功能。

6. **备选 IP 地址**，当算法选中备选 IP 时，需在该处设置期望返回的 IP 地址。
7. 管理**成员**，从虚拟服务列表中选择需要返回的 vs 添加到域名映射中的成员，在**权值**栏填写用于加权算法的权值，权值范围 1-65535，缺省为 1，在**关联链路**下拉列表中从**不关联**、**自动关联**以及当前所有**入站链路**中选中其中一项以确定是否将该 vs 关联入站链路，缺省为**自动关**

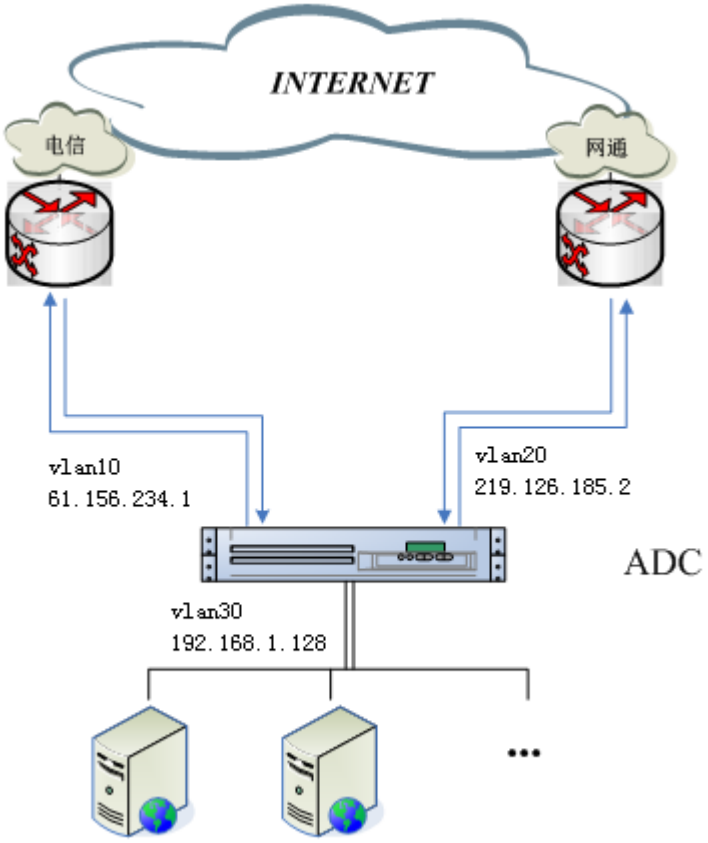
**联**入站链路，点击**添加**将该 vs 作为成员加入到该域名映射中。

8. 点击**提交**。

### 42.2.4 配置案例

案例拓扑如下图所示，设备通过接口 vlan10 以及 vlan20，分别从电信和网通两条链路接入互联网，通过对域名 www.test.com 的智能解析进行入站流量管理。

使电信用户走电信链路，网通用户走网通链路，用户访问尽量不跨运营商，当某条链路出现故障时，另一运营商链路能够实现冗余备份。



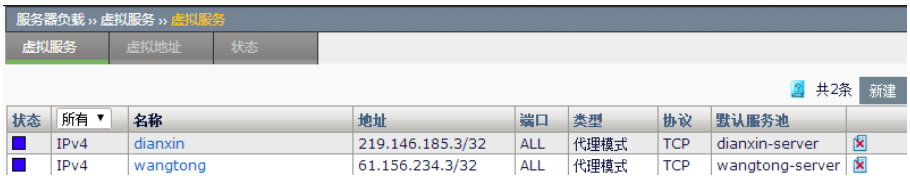

**配置步骤：**

1. 配置接口 IP

点击**网络配置>接口>vlan 列表**，添加 vlan 接口 IP，列表如下：


2. 配置虚拟服务

点击**服务器负载>虚拟服务**，配置虚拟服务，列表如下：

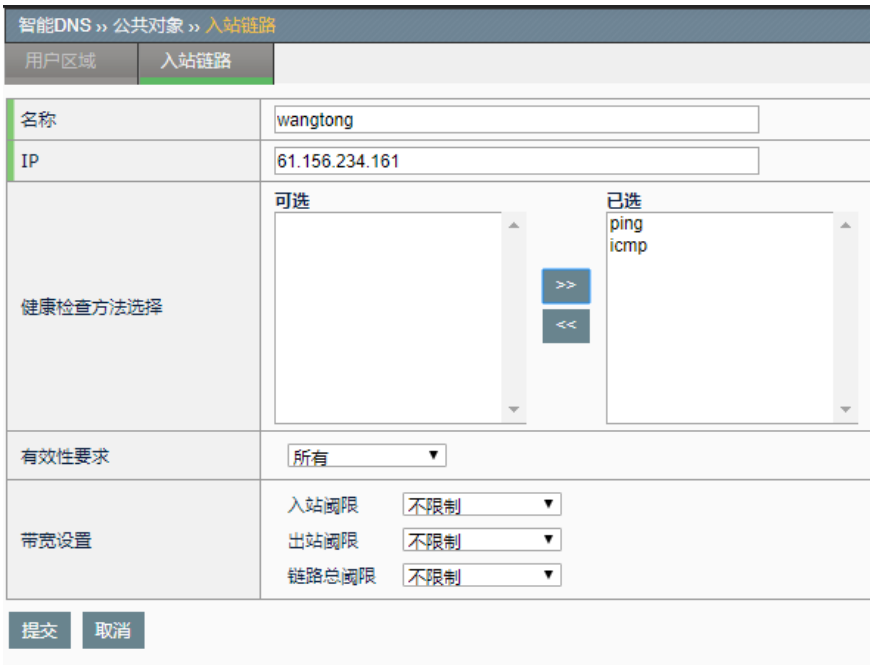


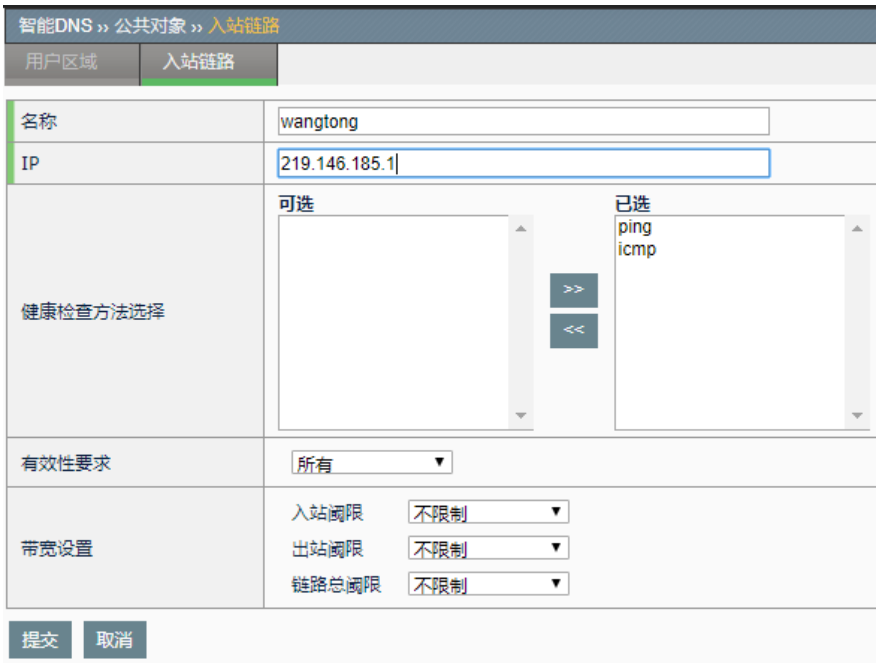

3. 配置监听地址

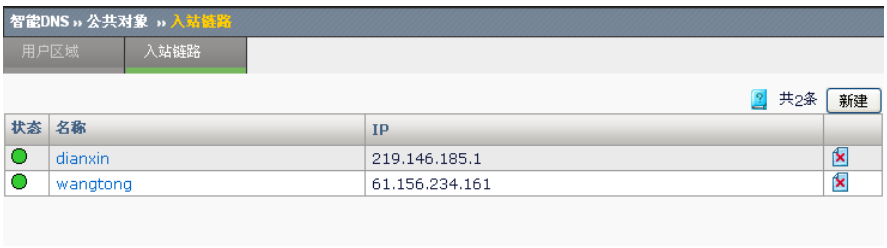
点击**智能 DNS > DNS 服务器>基础配置**，将 61.156.234.1 和 219.146.185.2 选入右侧列表进行 DNS 监听。


4. 配置入站链路

点击**智能 DNS >公共对象>入站链路**，针对网通、电信两条链路分别配置两条入站链路。



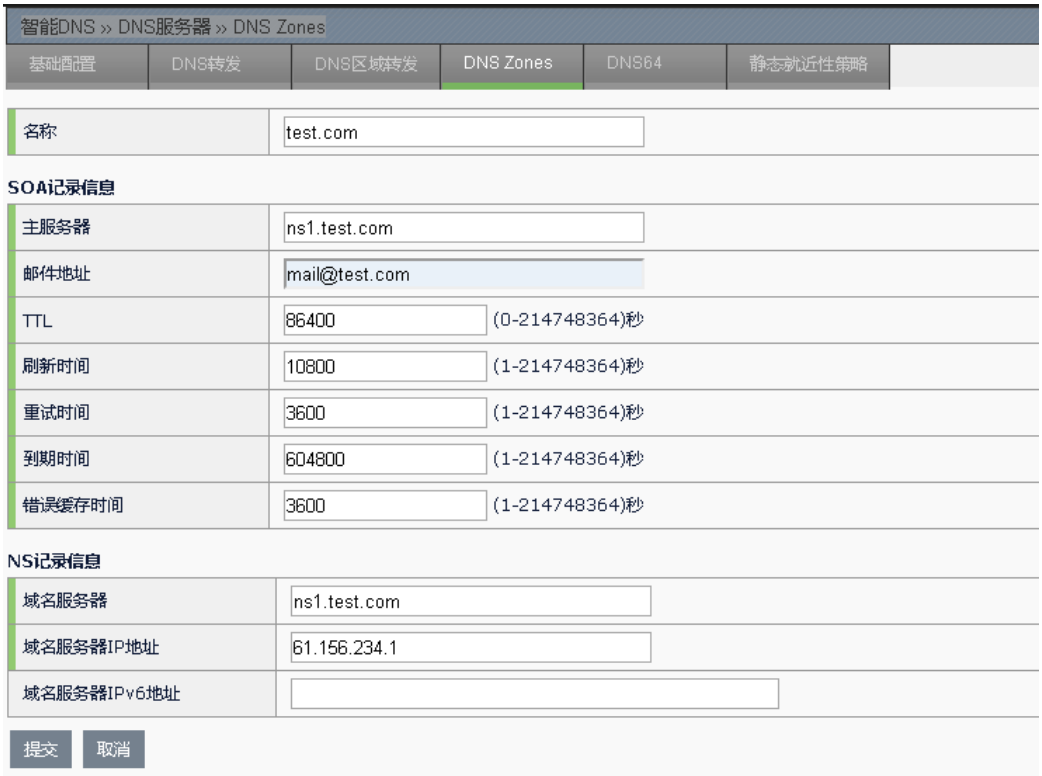

5. 配置静态就近性策略

点击**智能 DNS >本地负载>静态就近性策略**。为支持静态就近性算法，配置两条静态就近性策略，源地址为 ISP 电信用户的 DNS 请求返回

219.146.185.3/32 网段的 vs 地址，源地址为 ISP 网通用户的 DNS 请求返回 61.156.234.3/32 网段的 vs 地址。

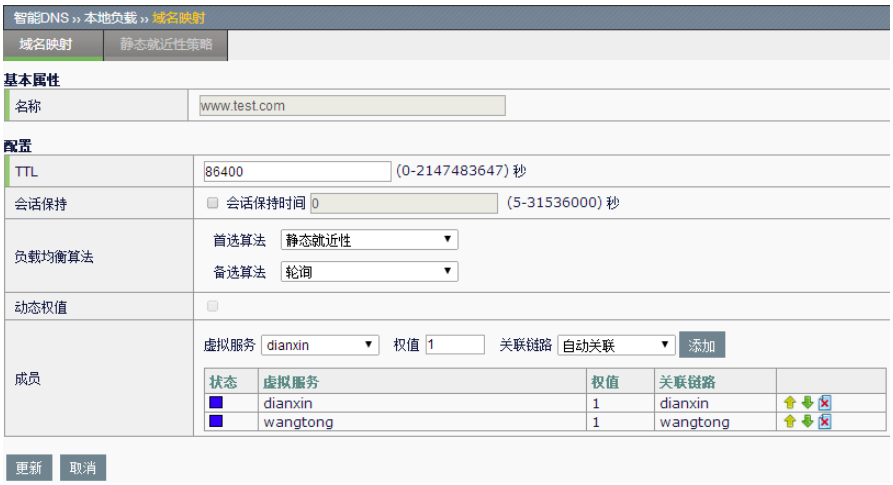

6. 配置 DNS zone

点击智能 DNS>DNS 服务器>DNS Zones，新建名称为 test.com 的 DNS zones。




7. 配置本地负载域名映射

点击**智能 DNS >本地负载>域名映射**，配置智能解析 www.test.com 的域名映射，选择首选算法为静态就近性，备选算法轮询，将 dianxin、wangtong 两个 vs 加入成员列表，分别制定关联入站链路 dianxin 和 wangtong，点击**提交**完成配置。




### 42.2.5 常见故障分析

案例 1：故障现象：对已配置智能 DNS 的域名不能返回正常解析结果

| | |
|---|---|
| | 对于某域名的DNS请求，已进行相应的智能DNS配置，但不能返回正常解析结果。 |
| | 1. 对该域名的解析请求是否为A记录的请求。<br>2. 域名映射中首选算法以及备选算法是否均设置为“无”。<br>3. 域名映射中设置了“备选IP”作为调度算法，却没有设置备选IP地址。<br>4. vs关联的链路节点健康检查是否通过，是否已设置带宽限制并当前带宽超出阀限。<br>5. vs是否可用。<br>6. 是否配置静态就近性为调度算法，并且静态就近性策略不够完善，以致该次DNS请没有匹配的策略。<br>7. 对应的设备IP地址是否加入到监听地址中。 |
| | 1. 智能DNS目前只对A记录类型请求进行响应。<br>2. 确保域名映射中至少设置一种有效算法。<br>3. 如果域名映射中已设置“备选IP”作为算法，则应设置一个有效的备选IP地址。<br>4. 确保vs不关联link，或者关联link可用。<br>5. 在“服务器负载”中检查对应vs状态为unknow或者up，确保其可用性。<br>6. 如果域名映射中已设置“静态就近性”作为算法，确保配置考虑周全的静态就近性策略。<br>7. 确定监听DNS的设备IP已加入到智能DNS的“监听地址”中。 |

## 42.3 全局负载

### 42.3.1 概述

全局负载针对多数据中心的应用场景，通过智能 DNS 响应的方式，将全局范围的访问流量合理地导入到每个数据中心。用户发送对某指定域名的 DNS 请求，该请求最终发往 ADC 设备，全局负载模块根据配置，综合考虑用户所处地域、运营商网络、动态探测时间、或者当前链路带宽质量等多种因素，返回虚拟服务地址，用户根据返回的 IP 地址，对服务进行访问，从而智能的分配全局入站流量。

全局负载支持动态就近性、静态就近性、轮询、加权轮询、全局可用性、最小连接数、最小带宽、备选 IP 等数十种负载均衡算法，结合动态权值功能，最大限度的根据用户当前需求灵活地实现入站负载。

同时，通过健康检查，探测远程服务的可用性，结合服务的当前流量带宽、连接数、新建连接等统计，获得远程服务当前的实际状况，准确的响应 DNS 请求，和服务器负载均衡配合使用，引导后续业务流量使用全局范围内当前最优的服务器业务入口。

### 42.3.2 配置数据中心（Datacenter）

该配置项基于全局范围内每个作为负载对象的服务站点（通常为一台 ADC 设备），是用于负载的各种资源的集合。每个数据中心分别包含了提供服务的虚拟服务。

进入**智能 DNS >全局负载>数据中心**，显示当前已配置数据中心列表。


**状态**：显示当前数据中心是否启用：

 ，表示启用；

 ，表示未启用。

**名称**：数据中心名称。

**类型**：指明该数据中心是本地还是远程。

**虚拟服务**：数据中心配置的虚拟服务个数。

**上次同步时间:**上次向该数据中心发起远程配置同步的时间。

**同步结果**：上次向该数据中心发起远程配置同步的结果。

**同步：**点击该按钮，向对应的数据中心同步全局负载配置。

注意

配置同步的内容：全局负载配置、用户区域配置、DNS 服务器配置、全局负载类型的健康检查配置。

点击**新建**，进入配置页面新建数据中心。


**配置步骤：**

1. 输入数据中心**名称**（该项为必填项）。
2. 在**描述**栏输入对该数据中心的描述信息。
3. 勾选或清除**启用**选项，以决定是否启用该数据中心的所有资源，缺省为启用。
4. 选择数据中心**类型**为**本地**或者**远程**，本地表示该台设备所在数据中心，反之则为远程数据中心，**本地**数据中心**只能配置一个**，远程则可以配置多个。
5. 当选择类型为**远程**时，出现地址列表的配置栏，该地址为远程数据中

心**用于通信的地址**，可配置多个。

6. 点击**提交**。

进入**智能 DNS >全局负载>数据中心**，在数据中心列表页面点击任意数据中心行虚拟服务栏表示虚拟服务个数的数字，进入对应数据中心虚拟服务器列表。


**状态**：显示当前虚拟服务是否启用：

，表示启用；

，表示未启用。

**名称**：虚拟服务名称。

**类型**：虚拟服务器类型，包括设备配置的虚拟服务器和第三方服务器两种类型。

**IP**：虚拟服务 IP 地址。

**端口**：虚拟服务对应端口。

**关联链路**：只针对本地数据中心，可以在将其中的虚拟服务器关联入站链路。

点击**新建**，进入配置页面新建虚拟服务。


**配置步骤：**

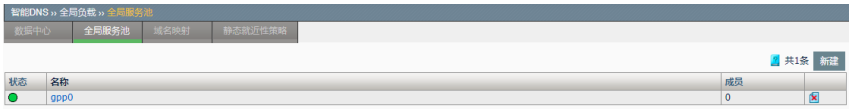
1. 在**类型**下拉列表中选择虚拟服务的类型，**虚拟服务器**表示在 ADC 设备上配置的 vs，**第三方服务器**表示第三方设备，无连接数、包速率、最大带宽等配置项。
2. 当新建本地数据中心的虚拟服务器时，可以从**虚拟服务**下拉列表中选择本地的虚拟服务，选中的虚拟服务信息（名称、IP 地址和端口）会自动配置在对应项中。
3. 对于远程数据中心的虚拟服务，需要输入虚拟服务**名称**、**IP 地址**以及**端口**，该信息必须与实际远程设备中心中虚拟服务信息完全符合，否则被视为不可用（该项为必填项）。
4. 勾选或清除**启用**选项，以决定是否启用该虚拟服务，缺省为启用。
5. 选择“不设置”或设置该虚拟服务**连接数、包速率和带宽**可以达到的最大限值，当实际虚拟服务对应数据超过所设限值，不再将该虚拟服务 IP 地址作为 DNS 请求返回的地址。缺省为不设置。
6. 当数据中心为本地类型时，可以将**入站链路**与虚拟服务关联，入站链路的可用状态会影响虚拟服务的可用状态，在出现的**本地链路关联**选项的下拉列表中选择不关联、自动关联或者指定关联某链路。
7. 点击**提交**。

### 42.3.3 配置全局服务池

全局 DNS 地址池是用于全局负载的资源地址的集合，作为全局负载的二级

单元，将一个或多个数据中心的虚拟服务作为成员整合在一起，提供作为 DNS 请求的资源响应地址。

进入**智能 DNS >全局负载>全局服务池，**显示当前全局 DNS 地址池列表。




**状态**：显示当前全局 DNS 地址池是否启用：

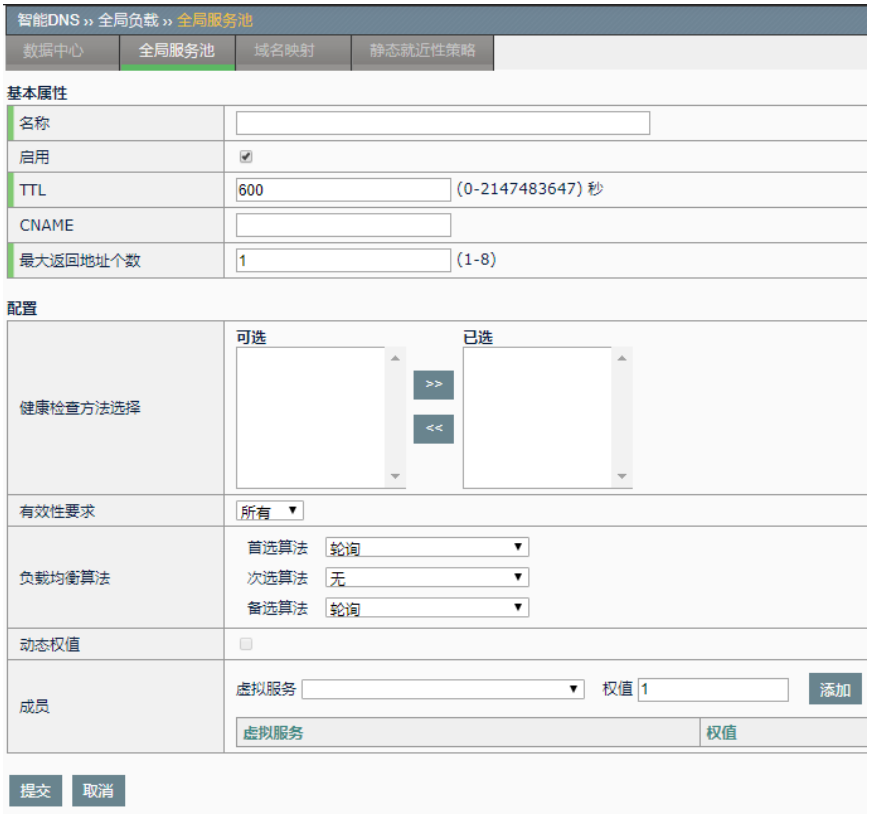
●，表示启用；

●，表示未启用。

**名称**：全局地址池名称。

**成员**：地址池中作为成员的虚拟服务个数。

点击**新建**，进入全局地址池的新建页面。




**配置步骤：**

1. 输入全局地址池的**名称**。
2. 勾选或清除**启用**选项，以决定是否启用该全局地址池，缺省为启用。
3. 在 **TTL** 部分输入期望对应的 A 记录的 TTL 值，以秒为单位，缺省为

86400s（1 天），输入范围为 0-2147483647。

4. 当期望该 g-pool 返回的结果为 **CNAME** 记录而非 A 记录时，在 CNAME 项中添入需要返回的 cname 记录的数据部分（规范名）。
5. **最大返回地址个数**，设置的 DNS 响应中 A 记录地址的最多个数，最大可设为 8，缺省为 1。


提示

当最大返回地址个数大于 1，导致 DNS 响应中有多个地址时，由于请求方通常使用首个地址进行服务访问，所以调度算法主要体现在第一个返回的地址。

6. 从左侧当前**健康检查**模板列表中选中期望的一个或多个到右侧列表中，用于检查当前全局地址池中 vs 成员的可用状态。
7. 在**有效性要求**中，选择**所有**表示当所有的健康检查都通过时该成员健康状态可用，选择**至少**并指定**个数**表示当指定个数的健康检查通过时该成员则可认为健康状态可用。
8. 选择**负载均衡算法**，分别从**首选算法**、**次选算法**和**备选算法**的下拉列表中选择期望使用的对应算法，当选择 vs 时先使用首选算法进行选择，当选取失败时，利用次选算法进行选择，再次失败后，使用备选算法进行选择，缺省情况首选和备选为轮询，次选并未选择算法。首选算法和备选算法可选范围为无、轮询、加权轮询、全局可用性、静态就近性、备选 IP、动态就近性、最小连接数、加权最小链接、最小 pkt/s 以及最小带宽，次选算法可选范围为无、轮询、加权轮询、全局可用性、静态就近性、备选 IP。

   **无**：不配置算法。

   **轮询**：依次轮询返回可用 vs 地址。

   **加权轮询**：按各 vs 设置的权重比例返回各 IP 地址。

   **全局可用性**：总是返回 vs 列表中第一个可用 vs 的 IP 地址。

   **静态就近性**：根据请求 DNS 源 IP 所在子网段、ISP、地域或者用户区域，返回一定的 vs 地址，需结合静态就近性策略的配置。

   **备选 IP**：总是返回备选 IP 地址的 DNS 记录，选择该算法时应配置所期望的备选 IP 地址。

   **动态就近性**：返回和 LDSN 之间探测时间最短的 vs 地址。

   **最小连接数**：返回当前连接数最小的 vs 地址。

   **加权最小连接**：综合考虑 vs 权值以及当前连接数，返回当前权值大且当前连接数较小的 vs 地址。

   **最小 pkt/s**：以 pkt/s 为参考单位，返回当前包速率最小的 vs 地址。

   **最小带宽**：以 bit/s 为单位，返回当前带宽最小的 vs 地址。

注意

当首选算法、次选算法和备选算法都设置为“无”时，不可能选出 vs 地址进行 DNS 响应。

9. **动态权值**，当算法为最小连接数、加权最小连接、最小 pkt/s 或者最小带宽时，该复选框变为可选状态，勾选动态权值，按个 vs 当前动态参数比例返回 DNS 响应地址，缺省情况下不勾选该项。

提示

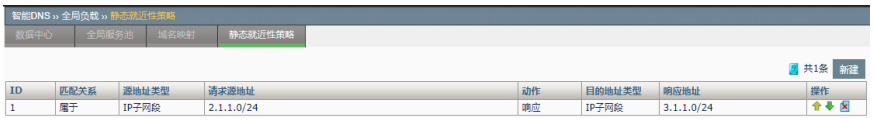
当算法为最小连接数、加权最小连接、最小 pkt/s 或者最小带宽四种动态算法时，推荐启用动态权值功能。

10. **备选 IP 地址**，当算法选中备选 IP 时，出现该选项，需在该处设置期望返回的 IP 地址。
11. **全局地址池成员**，从虚拟服务列表中选择需要添加到该 g-pool 中的成员，在**权值**栏填写用于加权算法的权值，权值范围 1-65535，缺省为 1，点击**添加**将该 vs 作为成员加入到 g-pool 中。
12. 点击**提交**。

### 42.3.4 配置静态就近性策略

当全局地址池（参见下一小节）选择算法为静态就近性时，算法调度的依据是在该配置项配置的一个或多个静态就近性策略。

进入**智能 DNS >全局负载>静态就近性策略**。




**ID**：静态就近性策略 ID，用于标识每条静态就近性策略。

**匹配关系**：指定发来请求的 LDNS 的源地址与策略源对象是否应该匹配。

**源地址范围**：指定发来请求的 LDNS 的源地址需属于（或不属于）的 IP 子网（或 ISP 地址库、省、市、用户区域）。

**动作**：当源地址部分匹配策略指定的条件时，最终响应动作与策略之间的逻辑关系。

**响应网段**：指定响应子网段地址（或者全局地址池）。

点击右侧操作栏中的或者，调整策略顺序，调整结束后点击**确定**完成操作。

点击右侧操作栏中的  ，删除置顶一条策略。

点击**新建**，进入新建全局静态就近性策略页面。


**配置步骤：**

1. 输入策略 **ID**，范围为 1-65535，或者不配置该项，系统则自动为该条策略分配 ID。
2. 指定源地址与源地址对象的**匹配关系**（**属于**，**不属于**）。
3. 指定**源地址匹配对象类型**，IP 子网段，ISP 地址库，省，市，用户区域。
4. 在下一个对话框输入需**源地址匹配的对象**
   - 当源地址匹配对象类型选择 **IP 子网段**，该部分以 A.B.C.D/M 的格式输入具体 IP 网段地址，A.B.C.D 为 IP 地址，M 为子网掩码长度；
   - 当源地址匹配对象类型选择 **ISP**，该部分则从设备的 ISP 地址库下拉列表选中期望的对象。
   - 当源地址匹配对象类型选择**用户区域**，该部分则从用户区域下拉列表选中期望的对象。
   - 当源地址匹配对象类型选择**省**，该部分则从国内省级地区的下拉列表选中期望的对象。
   - 当源地址匹配对象类型选择**市**，首先从国内省级地区的下拉列表选中期望城市所在的省份，再从对应省份的城市列表中选择期望的城市。
5. 选择**响应动作**为**响应**，或者**不响应**。
6. 指定**目的对象类型**，IP 子网段，G-pool（全局地址池）。
7. 在下一个对话框输入需**目的匹配的对象**
   a) 当源地址匹配对象类型选择 **IP 子网段**，该部分以 A.B.C.D/M 的格式输入具体 IP 网段地址，A.B.C.D 为 IP 地址，M 为子网掩码长度；
   b) 当源地址匹配对象类型选择 **G-pool**，该部分则从已配置备的 G-pool 下拉列表选中期望的对象。

8. 点击**提交**。

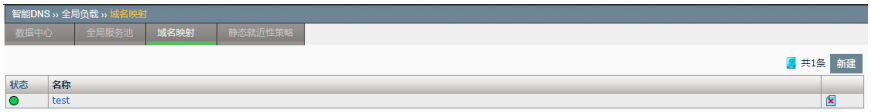

注意

同一个 ID 的静态就近性策略，只能配置一条，当 ID 不同时，对应源和目的相同内容也只能配置一条策略。

### 42.3.5 配置全局域名映射

该配置项对需要进行全局范围内智能 DNS 解析的域名进行配置，将指定域名与一个或多个 G-pool 关联起来，当收到对该指定域名的 DNS 请求时，根据配置算法从这些 G-pool 中选出一个，完成一级调度，进入选中的 G-pool 进行二级调度。

进入**智能 DNS >全局负载>域名映射**，显示当前域名映射列表。




**状态**：显示当前全局域名映射是否启用：

 ，表示启用；

 ，表示未启用。

**名称**，域名映射的域名。

点击**新建**，进入新建全局域名映射页面。

**配置步骤：**

1. 在**名称**字段输入需要做指定 DNS 解析的域名，域名须符合合法域名。
2. 勾选或清除**启用**选项，以决定是否启用该域名映射，缺省为启用。
3. 选择**负载均衡算法**，从下拉列表中选择期望使用的对应算法，可选范围为轮询、加权轮询、全局可用性、静态就近性。

   **轮询**，依次返回可用 G-pool。

   **加权轮询**，按各 G-pool 权重比例返回各 G-pool。

   **全局可用性**，总是返回 vs 列表中第一个可用 G-pool。

   **静态就近性**，根据请求 DNS 源 IP 所在子网段或者 ISP、用户区域等地址对象，返回某一 G-pool，需结合静态就近性策略的配置。
4. 在**会话保持**部分，勾选会话保持表示开启对该域名解析的会话保持功能，并添入期望的会话保持时间，单位为秒，缺省值为 300s，选择会话保持时间为 5-31536000s；不勾选会话保持表示关闭该功能，缺省情况不开启该功能。
5. 管理**成员**，从全局地址池列表中选择需要添加到域名映射中的成员，在**权值**栏填写用于加权算法的权值，权值范围 1-255，缺省为 1，点击**添加**将该 G-pool 作为成员加入到该域名映射中，同时选中成员列表中的某成员点击**上移**或者**下移**调整该成员在列表中的顺序。
6. 点击**提交**。

### 42.3.6 监控与维护

**1. 状态**

进入**系统信息>状态>全局负载均衡状态**，显示当前全局负载均衡状态信息。

选择类型为**数据中心**，显示当前各数据中心及其 vs 的当前状态。


**状态**：数据中心显示当前的启用状态和连接状态，虚拟服务显示当前启用状态、实际状态以及所在数据中心的可用状态。

选择类型为**全局地址池**，显示当前所有全局地址池及其成员的当前状态。


**状态**：全局地址池显示当前的启用状态和成员有效状态，成员显示所在地址池健康检查状态、对应虚拟服务可用状态以及所在地址池的启用状态。

### 2. 统计

进入**系统信息>统计信息> DNS 统计**，显示当前 DNS 请求的统计曲线。

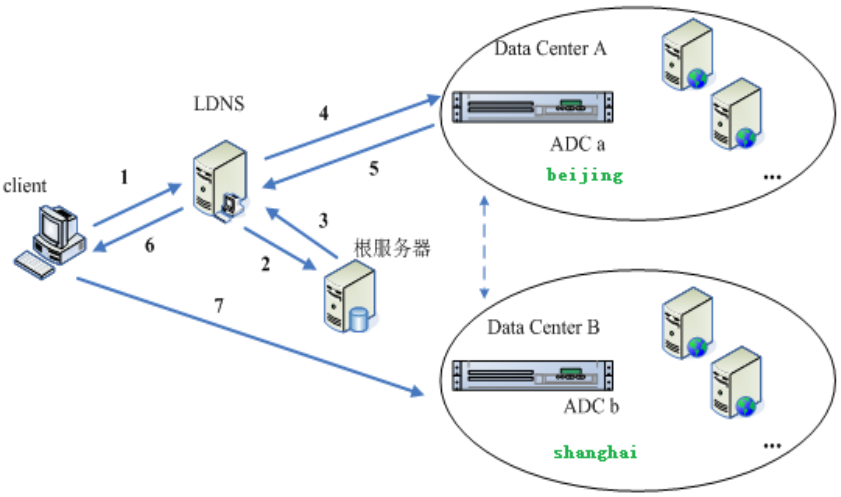
选择类型为**全局域名映射**，从域名下拉列表的全局域名映射中选择某域名，页面显示对应域名的 DNS 统计，鼠标定位到某数据点可以看到该点的 DNS 请求总数，通过调度成功响应个数，通过会话保持成功响应的个数以及失败个数。


## 42.3.7 配置案例

案例拓扑如下图所示，在全局范围内部署两个数据中心，北京所在的 datacenter A 和上海所在的 datacenter B，使北京用户访问走北京数据中心，上海用户访问走上海数据中心，用户访问尽量不跨地域，当某个数据中心服务出现故障时，另一数据中心能够实现全局流量冗余备份。

北京所在的 datacenter A 和上海所在的 datacenter B 下的设备都提供域名解析服务，当 datacenter A 下的设备故障，则 datacenter B 下的设备也能提供域名解析服务。

以下将示例在 dataenter A 设备 ADC a 上开启配置全局负载功能并将全局负载配置同步到 ADC b，通过对域名 www.gtmtest.com 智能解析进行全局流量管理。

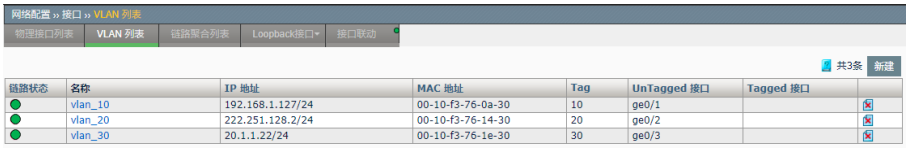



**配置步骤：**

**ADC b 配置**

1. 配置接口 IP

点击**网络配置>接口>vlan 列表，添加 vlan 接口 IP，**列表如下：




2. 配置监听地址：

点击**智能 DNS> DNS 服务器>基础配置**，将 222.251.128.2 选入右侧列表进行 DNS 监听，开启全局通信开关和接收远程配置同步。

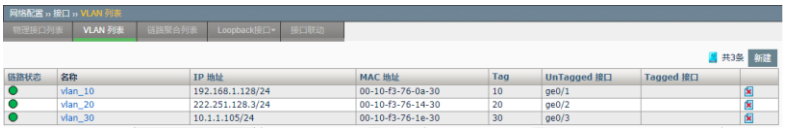

3. 配置虚拟服务

点击**服务器负载>虚拟服务**，配置虚拟服务，列表如下：


**ADC a 配置：**

1. 配置设备 IP

点击**网络配置>接口>vlan 列表，添加 vlan 接口 IP**，列表如下：




2. 配置虚拟服务

点击**服务器负载>虚拟服务**，配置虚拟服务，列表如下：


3. 配置监听地址

点击**智能 DNS> DNS 服务器>基础配置**，将 192.168. 1.128 选入右侧列表进行 DNS 监听，开启全局通信开关


4. 配置数据中心

点击**智能 DNS>全局负载>数据中心**，配置本地数据中心 beijing 和 ADC b 所在的远程数据中心 shanghai。




5. 向数据中心添加虚拟服务。


智能DNS ›› 全局负载 ›› 数据中心
bendi
虚拟服务器列表
类型
虚拟服务器
虚拟服务
b1
名称
b1
IP地址
10.1.1.1
端口
0
启用
数据中心
bendi
最大连接数
不设置
最大包速率
不设置
最大带宽
不设置
本地链路关联
自动关联
提交
取消


智能DNS ›› 全局负载 ›› 数据中心
bendi
虚拟服务器列表
类型
虚拟服务器
虚拟服务
b2
名称
b2
IP地址
10.1.1.2
端口
0
启用
数据中心
bendi
最大连接数
不设置
最大包速率
不设置
最大带宽
不设置
本地链路关联
自动关联
提交
取消

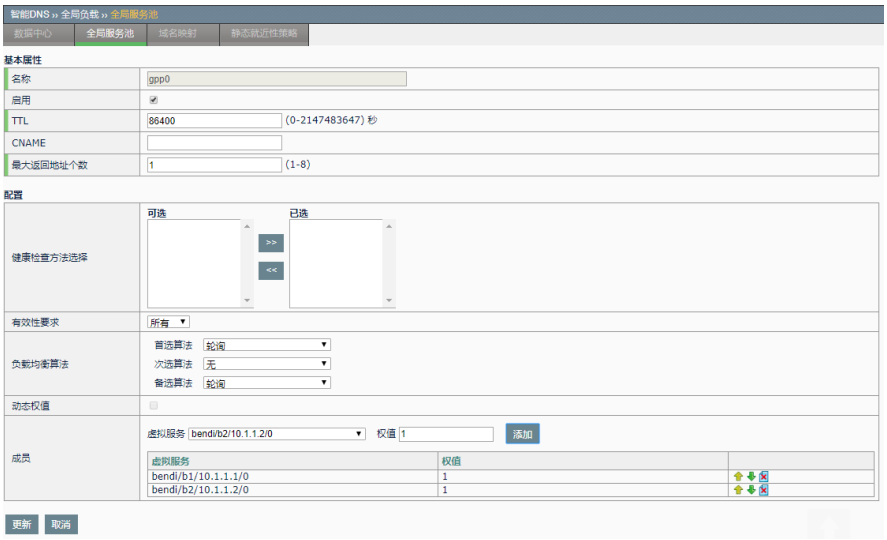

智能DNS ›› 全局负载 ›› 数据中心
bendi
虚拟服务器列表
共2条
新建
状态
名称
类型
IP地址
端口
关联链路
b2
虚拟服务器
10.1.1.2
0
自动关联
b1
虚拟服务器
10.1.1.1
0
自动关联



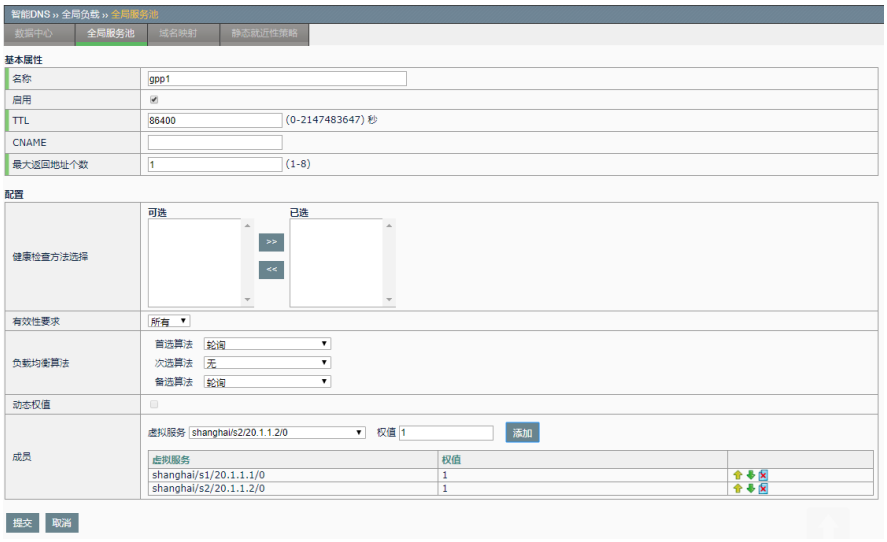

6. 配置全局地址池

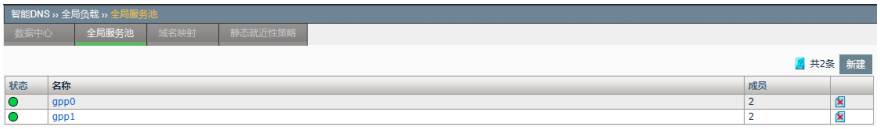
点击**智能 DNS>全局负载>DNS 地址池**，分别配置两个地址池将两个数据中心的 vs 作为成员。

G-pool gpp0：



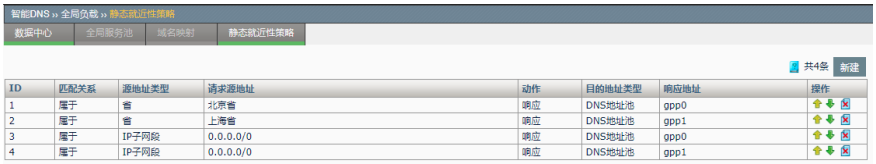

G-pool gpp1：




7. 配置静态就近性策略

点击**智能 DNS >全局负载>静态就近性策略**。为支持域名映射级别的静态就近性算法，配置两条静态就近性策略。




8. 配置域名映射

点击**智能 DNS >全局负载>域名映射**，配置智能解析 www.gtmtest.com 的域名映射，选择算法为静态就近性，将 gpp0、gpp1 两个 G-pool 加入成员列表，点击**提交**完成配置。



9. 将本地配置同步到对端 ADC b 数据中心

点击**智能 DNS >全局负载>数据中心**，保存设备配置，点击上海数据中心下的同步按钮，同步后本地的全局负载配置直接同步到对端设备并加载生效。


## 42.3.8 常见故障分析

案例 1：故障现象：对已配置全局域名映射不能返回正常解析结果

| | |
|---|---|
| | 对于某域名的DNS请求，已进行相应的全局负载的配置，但不能返回正常解析结果。 |
| | 1. 对该域名的解析请求是否为A记录的请求。<br>2. 域名映射中首选算法、次选算法以及备选算法是否均设置为“无”。<br>4. 域名映射中设置了“备选IP”作为调度算法，却没有设置备选IP地址。<br>5. 是否配置静态就近性为调度算法，并且静态就近性策略不够完善，以致该次DNS请没有匹配的策略。<br>6. 对应的设备IP地址是否加入到监听地址中。<br>7. vs关联的link的健康检查是否通过，是否已设置带宽限制并当前带宽超出阀限。 |

| | |
|---|---|
| | 8. vs是否可用，vs所在datacenter是否可用，关联的gpool是否启用。 |
| | 1. 智能DNS目前只对A记录类型请求进行响应。<br>2. 确保域名映射中至少设置一种有效算法。<br>3. 如果域名映射中已设置“备选IP”作为算法，则应设置一个有效的备选IP地址。<br>4. 如果域名映射中已设置“静态就近性”作为算法，确保配置考虑周全的静态就近性策略。<br>5. 确定监听DNS的设备IP已加入到智能DNS的“监听地址”中。<br>6. 在g-pool中检查对应vs状态为unknow或者up，确保其可用性。<br>7. 确保vs所在数据中心可用，vs在远程数据中心状态可用，vs所在g-pool已启用，DNS请求对应的域名映射已启用。 |

案例 2：故障现象：配置全局负载策略后远程数据中心下的服务器状态不可用

| | |
|---|---|
| | 对于某域名的DNS请求，已进行相应的全局负载的配置，添加的服务器地址为远端数据中心的虚拟服务地址，该服务器地址状态始终显示为不可用 |
| | 1. 对端数据中心是否禁用。<br>2. 全局服务池是否配置了到虚拟服务的健康检查且健康检查失败。<br>3. 添加虚拟服务的名称、IP地址和端口和远程数据中心虚拟服务配置不一致。 |
| | 1. 启用对端数据中心。<br>2. 确保本地到远程数据中心下的虚拟服务健康检查正常。<br>3. 全局通信需要通信虚拟服务器的状态信息，在数据中心下添加虚拟服务器地址时，需要确保和远程数据中心下的虚拟服务配置一致，包括名称、IP和端口信息的一致，否则通信时由于找不到匹配条件的虚拟服务而认为虚拟服务不可用。 |

案例 3：故障现象：全局负载配置同步不成功

| | |
|---|---|
| | 全局负载配置同步不成功 |
| | 1. 检查是否保存了本地配置后再执行的配置同步。<br>2. 检查到远程设备地址的65332端口是否能正常通信。<br>3. 检查是否开启了全局通信开关以及接受远程配置同步开关。<br>4. 查看配置同步不成功返回的提示，依据提示信息进行操作。 |

1. 保存本地配置后再同步。
2. 确保到远程设备地址的65332端口可正常通信。
3. 开启全局通信开关和接受远程配置同步开关。
4. 主要提示信息如下，可依据提示信息操作：

超时：通常为网络原因，设备通信不正常。

远程数据中心HA状态错误：检查对端HA环境主备机是否工作正常

虚拟服务错误：待同步的虚拟服务器信息在远端设备不存在

健康检查模板冲突：待同步的健康检查模板和对端已存在的健康检查模板冲突，如名称相同。

远程数据中心拒绝接受同步配置：远程数据中心未勾选接受远程配置同步。

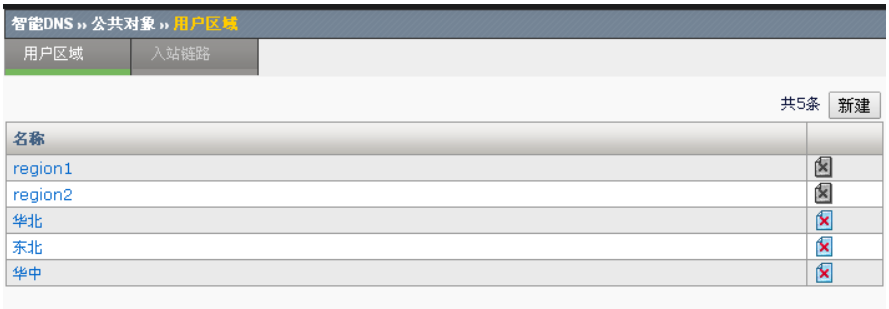
## 42.4 公共对象

DNS 服务器以及全局负载通用的配置对象。

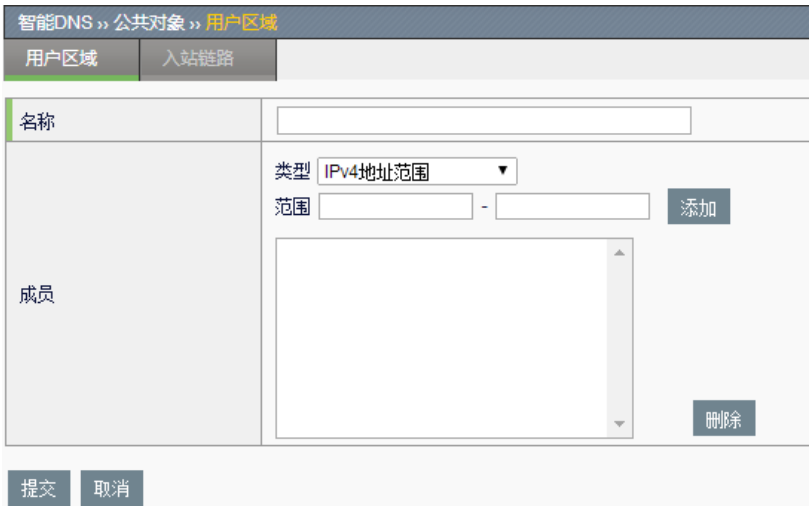
### 42.4.1 用户区域

用户区域是用户根据自定义需求，对 IP 网段、省市地域 IP 网段等信息进行整理后的集合，全局负载模块的静态就近性策略可以对其引用，引用后的用户区域被用于判断 DNS 请求的源 IP 地址属于哪个经用户定义后的范围，脱离单纯对省、市或者 IP 地址段范围的局限，从广义出发，使得全局负载的流量分配方式更具有实际应用价值。

进入**智能 DNS >公共对象>用户区域**，显示当前已配置用户区域列表。




点击**新建**，添加新的用户区域对象。




**配置步骤：**

1. **名称**，输入用户区域的自定义名称。
2. 添加**成员**，根据类型不同，可以将如下四种类型的地址对象作为成员添加到当前用户区域中：
   - **IPv4 地址范围**：在**范围**对应的文本框中输入自定义 IPv4 地址的真实范围；
   - **用户区域**：从**已创建**的用户区域列表中进行选择，加入到当前用户区域中，则选中用户区域中的所有地址对象范围也属于当前用户区域；
   - **省**：从中国所有省级区域的下拉列表中选择需要加入到当前用户区域的省份名称；
   - **市**：先从第一个下拉列表选中省份，再从第二个下拉列表中选出该省份中的城市名称。
3. 点击**提交**。

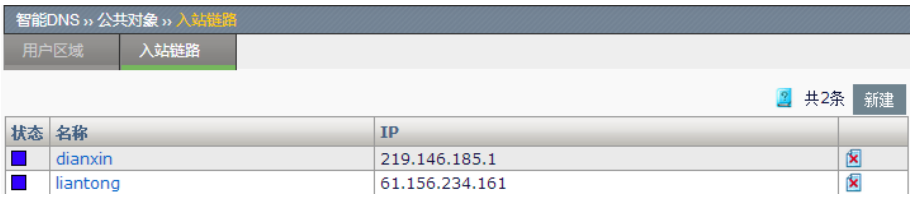
注意

作为成员，选中到用户区域的用户区域中不可以包含用户区域类型的成员，即用户区域只可以嵌套一层。

### 42.4.2 配置入站链路（Link）

该配置项基于 ADC 设备接入 ISP 的每条入站链路，通过健康检查动态探测每条链路的健康状态，及时的将其关联状态反映到智能 DNS 解析当中。

进入**智能 DNS >公共对象>入站链路**，显示当前已配置 link 列表。




**状态**：显示当前入站链路状态，共有三种：

■：表示**未知**，说明该链路未配置健康检查，此时链路可用；

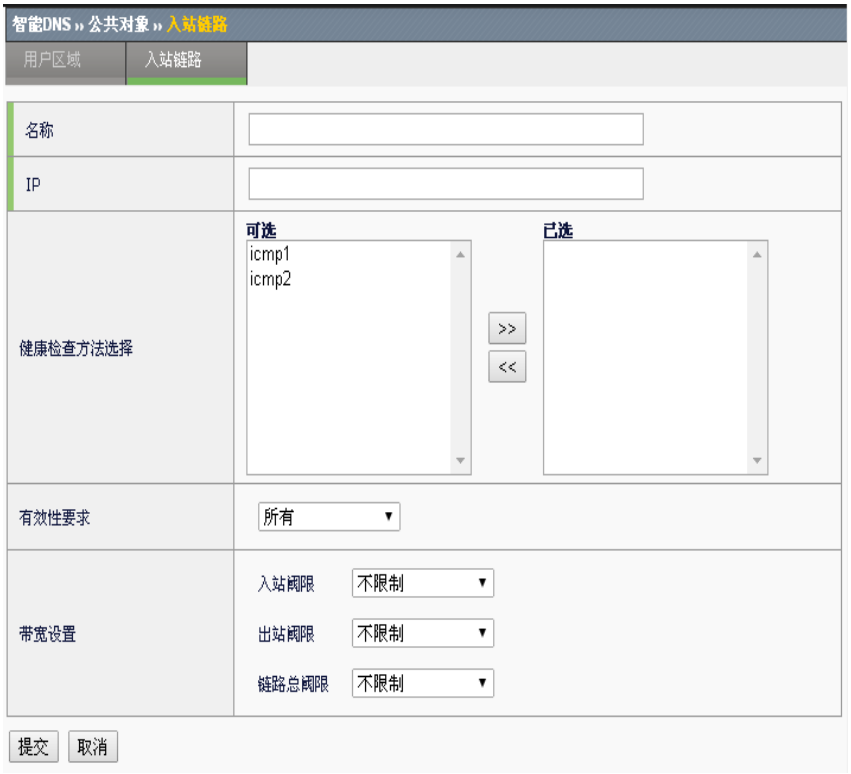
 ：表示 **DOWN**，说明该链路已配置健康检查并且不满足健康条件，此时链路不可用；

 ：表示 **UP**，说明该链路已配置健康检查并且满足健康条件，此时链路可用。

**名称**：入站链路名称。

**IP**：入站链路 IP 地址。

点击**新建**，进入配置页面新建 link。




**配置步骤：**

1. 输入 link **名称**（该项为必填项）。
2. 在 **IP** 栏输入该条链路出口路由地址（该项为必填项）。
3. 选择**健康检查最少通过个数**为**全部**或者**少于**，选中**少于**则需输入最少健康检查通过个数，缺省为所有。

4. 从**健康检查**左侧列表选中健康检查方法，选入到右侧列表，作为检查该链路健康状态的方法。
5. 在**带宽设置**部分设置该条链路的各种带宽阀限，包括**入站带宽阀限**、**出站带宽阀限**以及**链路总带宽阀限**，每种带宽设置可选择**所有**不设置带宽限制，或者选择**至少**并添入期望的带宽最大值，设置范围为 1-4294967295Mbits/s，缺省为均不设置带宽阀限。
6. 点击**提交**。

# 43 第43章 接口

## 43.1 接口概述

应用交付设备网络接口管理分为五种：物理接口配置管理、VLAN 配置管理、链路聚合配置管理、loopback 配置管理、接口联动配置管理。

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。

loopback 配置主要是在设备上添加本地环回虚接口，可以用于本地三层转发、OSPF 协议的路由 ID。

接口联动是将多个物理接口绑定成一个接口联动组，以实现同一个联动组中所有接口链路状态一致的功能。接口联动只针对多个物理接口之间相互联动，已经加入联动组中的物理接口不能再被其它联动组引用。

## 43.2 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以及端口协商、速率、双工等进行配置。

1. 进入**网络配置>接口>物理接口列表**，如下图：

| 链路状态 | 名称 | IP 地址 | MAC 地址 | 速率 | 双工模式 | 管理状态 | VLAN 数量 | 链路聚合 |
|---|---|---|---|---|---|---|---|---|
| | mgt | 192.168.1.29/24 | 00-e0-4c-08-32-... | 100 | FULL | UP | 0 | |
| | ge0/0(ge0/0) | | 00-e0-4c-08-32-... | N/A | N/A | UP | 1 | |
| | ge0/1(ge0/1) | 10.1.1.2/16 10.2.1.2/16 | 00-e0-4c-08-32-... | 1000 | FULL | UP | 0 | |
| | ge0/2(ge0/2) | | 00-e0-4c-08-32-... | 100 | FULL | UP | 0 | tvi1 |
| | ge0/3(ge0/3) | | 00-e0-4c-08-32-... | 1000 | FULL | UP | 0 | |

**链路状态**：物理接口链路状态，绿色为 up，红色为 down

**名称**：物理接口名称，mgt 是管理口，ge X/X 是千兆电光口，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）。

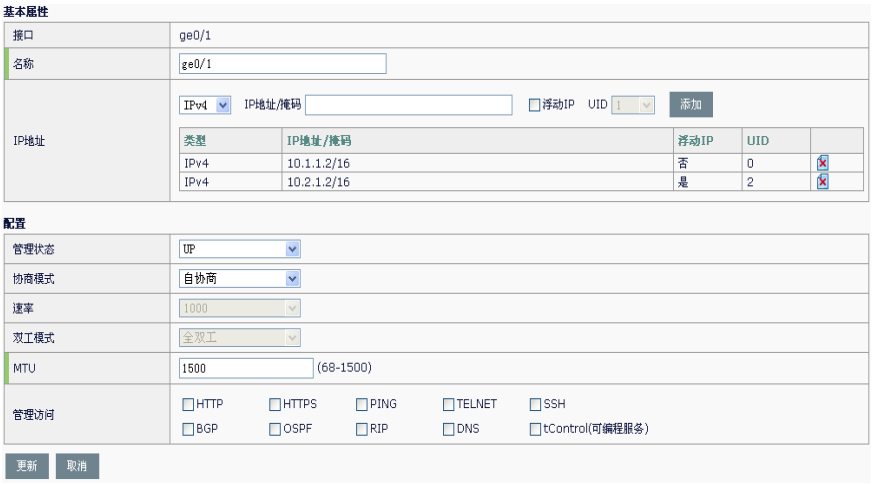
**管理状态**：物理接口手工管理状态，分为 UP/DOWN 两种状态。

**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。


一个物理接口可以以 tag 方式加入到多个 vlan 中。

2. 点击**接口名称**，进入单个物理接口配置，如下图：




**基本属性**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 是千兆电口或千兆光口，xge X/X 是万兆光口。**名称**：物理接口的别名。

**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。

**tControl**：可通过该接口地址，访问设备提供的可编程服务。


提示

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

3. 点击**更新**完成对物理接口的配置。

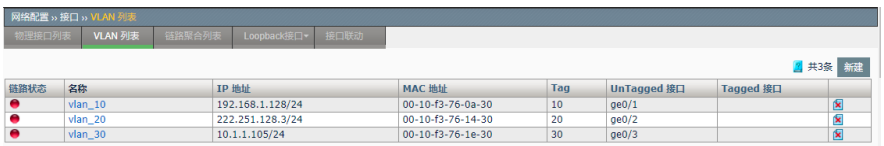
## 43.3 VLAN配置

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。

### 43.3.1 添加VLAN

1. 进入**网络配置>接口>VLAN 列表**，如下图：




**链路状态**：VLAN 的状态

**名称**：VLAN 名称

**IP 地址**：VLAN 的 IP 地址

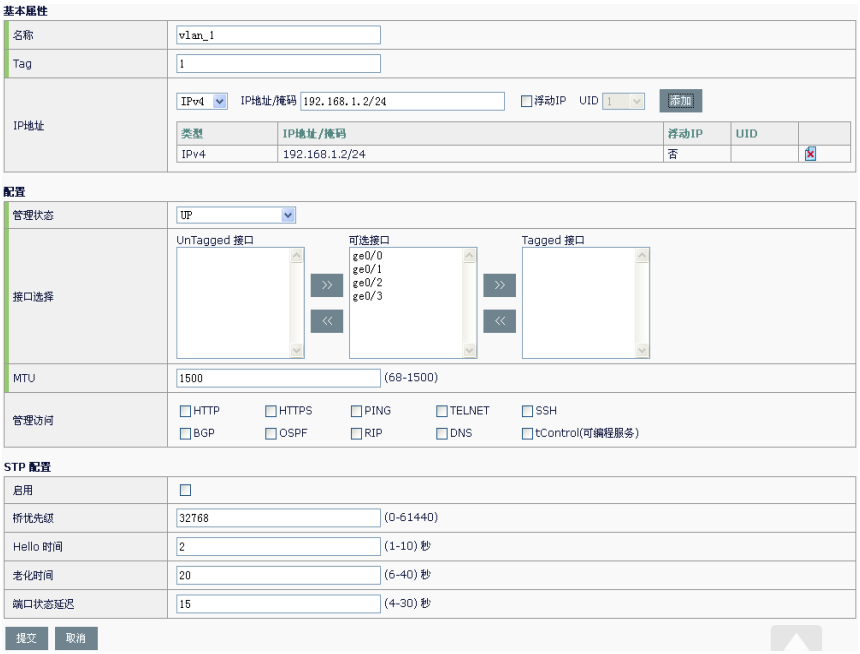
**MAC 地址**：VLAN 的 MAC 地址

**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 启用或关闭，可选 UP/DOWN

**可选接口**：设备中可以加入 VLAN 的接口

**UnTagged 接口**：以 UnTag 方式加入 VLAN 的接口

**Tagged 接口**：以 Tag 方式加入 VLAN 的接口，启用 802.1q 协议

**MTU**：VLAN 的 mtu 值，范围为 68-1500

**管理访问**：配置该接口地址上允许访问的服务类别。

**HTTP**:可通过 HTTP 协议访问该接口的地址，来访问管理设备。

**HTTPS**: 可通过 HTTPS 协议访问该接口的地址，来访问管理设备。

**PING**: 该接口地址允许响应 PING。

**TELNET**: 可通过 TELNET 协议访问该接口地址，来访问管理设备。

**SSH**: 可通过 SSH 协议访问该接口地址，来访问管理设备。

**BGP**: 可通过该接口地址访问设备提供的 BGP 服务。

**OSPF**：可通过该接口地址访问设备提供的 OSPF 服务.。

**RIP**：可通过该接口地址访问设备提供的 RIP 服务。

**DNS**：可通过该接口地址访问设备提供的 DNS 服务。

**tControl**：可通过该接口地址，访问设备提供的可编程服务。

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

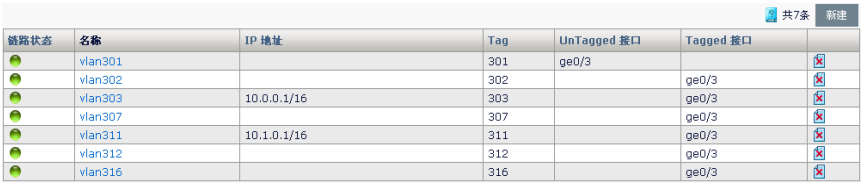
**端口状态延迟**：端口状态变换的时延，范围 4-30 秒


尽量设置性能较高、位置靠近中心的 VLAN 的优先级为最高。

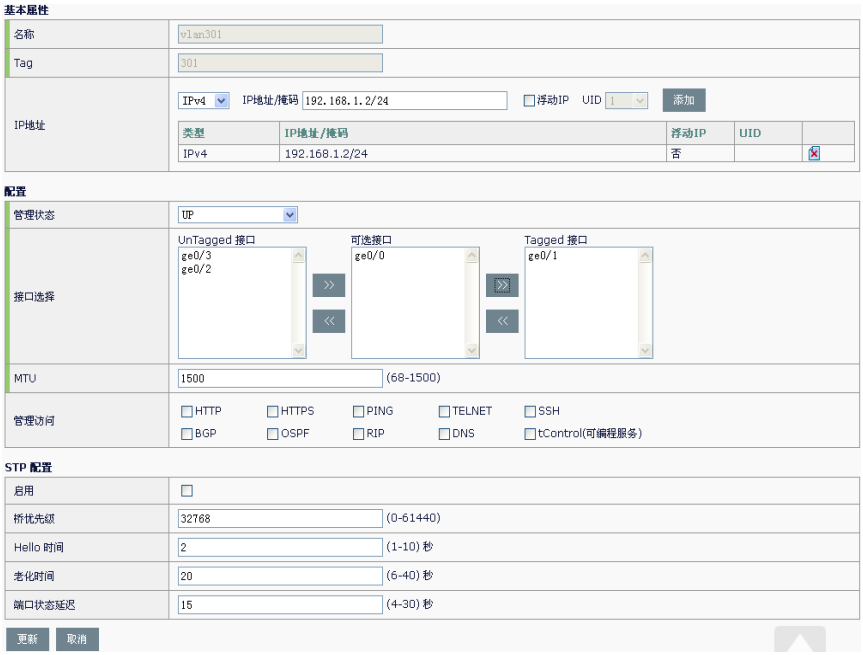

端口状态变换的时延是指：开启 STP 后，端口从 listening 到 learning 到 forwarding 各状态变化的时间间隔。

### 43.3.2 修改VLAN

1. 进入**网络配置>接口>VLAN 列表**，如下图：




2. 点击 vlan **名称**，修改 VLAN，如下图：



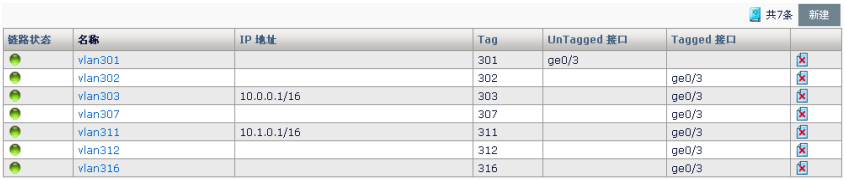

修改 vlan 的 **IP 地址、管理状态、UnTagged 接口、Tagged 接口、MTU、STP 配置**等信息

3. 点击**更新**完成修改。


不能修改 vlan 本身的名称、Tag 值。

### 43.3.3 删除VLAN

1. 进入**网络配置>接口>VLAN 列表**，如下图：




2. 点击  删除 VLAN。


3. 点击**确定**删除 VLAN。

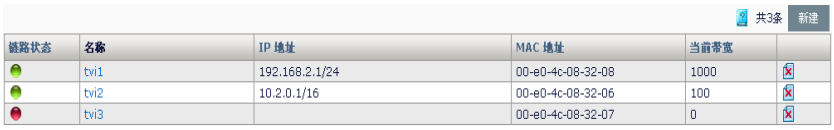
提示 被其他功能引用的 VLAN 不能被删除。

## 43.4 链路聚合配置管理

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

### 43.4.1 添加链路聚合

1．进入**网络配置>接口>链路聚合列表**，如下图：




**链路状态：**链路聚合的状态

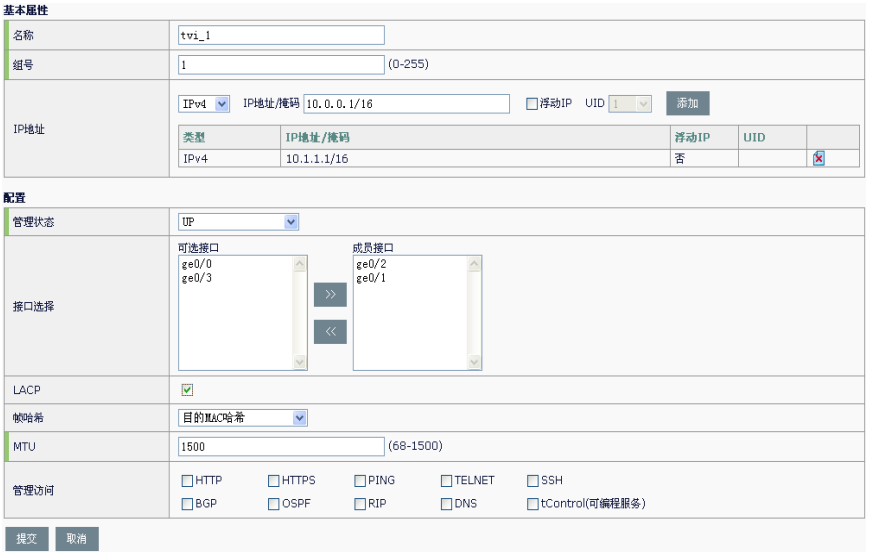
**名称：**链路聚合名称

**IP 地址：**链路聚合的 IP 地址

**MAC 地址：**链路聚合的 MAC 地址

**当前带宽：**所聚合的链路总带宽，单位 M

2．点击**新建**创建链路聚合，如下图：




**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，可选目的 MAC 哈希/源目的 IP 哈希

**MTU**：链路聚合 mtu 值，范围为 68-1500

**管理访问**： 配置可通过该链路聚合地址，访问设备提供的服务类别

**HTTP**:可通过访问该链路聚合的地址，访问设备提供的 HTTP 服务

**HTTPS**: 可通过访问该链路聚合地址，访问设备提供的 HTTPS 服务

**PING**: 该链路聚合地址允许响应 PING

**TELNET**: 可通过该链路聚合地址 TELNET 到设备本地

**SSH**: 可通过该链路聚合地址 SSH 连到设备本地

**BGP**: 可通过该链路聚合地址访问设备提供的 BGP 服务

**OSPF**: 可通过该链路聚合地址访问设备提供的 OSPG 服务

**RIP**：可通过该链路聚合地址访问设备提供的 RIP 服务

**DNS**: 可通过该链路聚合地址访问设备提供的 DNS 服务

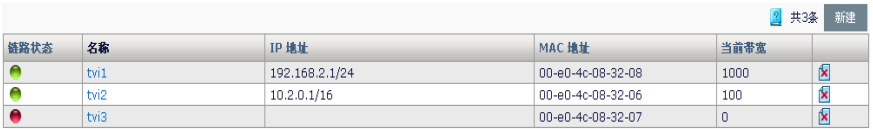
**tControl**: 可通过该链路聚合地址，访问设备提供的可编程服务

注意

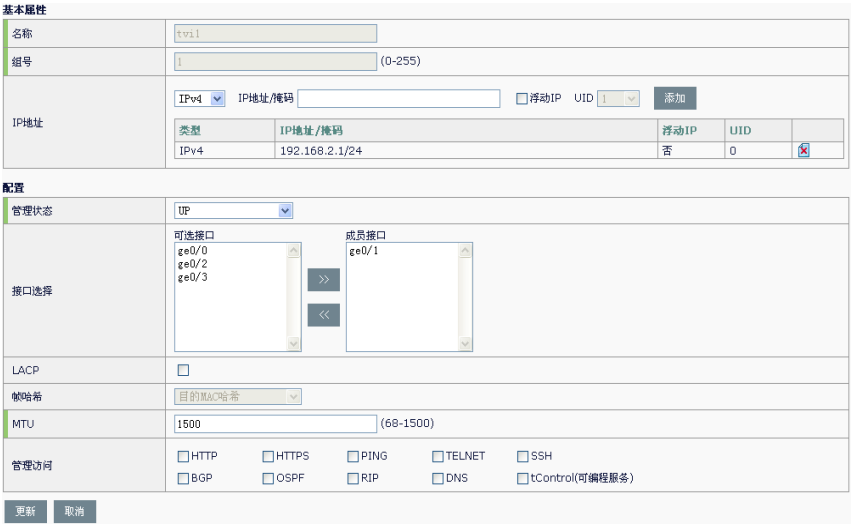
不开启 LACP 模式则静态轮询收发报文，开启 LACP 则可以达到动态链路聚合与备份。

### 43.4.2 修改链路聚合

1. 进入**网络配置>接口>链路聚合列表**，如下图：




2. 点击链路聚合**名称**修改。

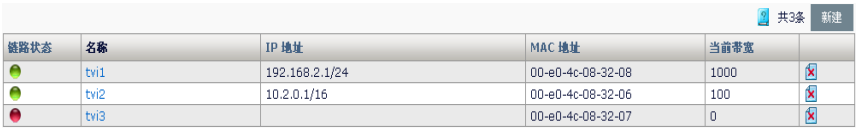



修改链路聚合 **IP 地址、管理状态、成员接口、LACP、帧哈希**等信息。

3. 点击**更新**完成修改。

### 43.4.3 删除链路聚合

1. 进入**网络配置>接口>链路聚合列表**，如下图：




2. 点击删除链路聚合。


3. 点击**确定**删除链路聚合。

提示 已经加入到 VLAN 中的链路聚合不能被删除。

## 43.5 LoopBack接口配置管理

loopback 接口是在设备上创建一个本地环回虚接口，用于动态路由协议配置 router id 和设备三层转发。

### 43.5.1 添加LoopBack接口

1、进入**网络配置>接口>LoopBack 接口**，如下图：


**IP 地址**：loopback 接口 IP

**掩码**：loopback 接口掩码

**接口**：loopback 接口，只有 lo 口可以配置 loopback 接口

2、点击**新建**，如下图：

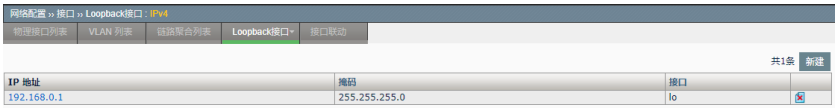

**IP 地址**：loopback 接口 IP

**掩码**：loopback 接口掩码

**接口**：loopback 接口，只有 lo 口可以配置 loopback 接口

### 43.5.2 修改LoopBack接口

1. 进入**网络配置>接口>LoopBack 接口**，如下图：

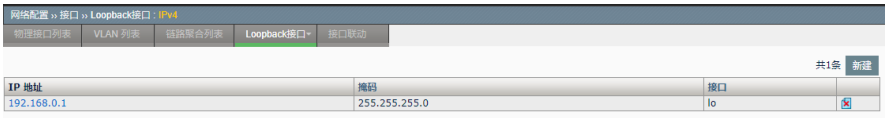



2. 点击**名称**修改，如下图：


修改掩码和接口

### 43.5.3 删除LoopBack接口

1. 进入**网络配置>接口>LoopBack 接口**，如下图：




2. 点击删除 LoopBack 接口。


3. 点击确定，删除 LoopBack 接口。

## 43.6 接口联动配置管理

接口联动是将多个物理接口绑定成一个接口联动组，以实现同一个联动组中所有接口链路状态一致的功能。接口联动只针对多个物理接口之间相互联动，已经加入联动组中的物理接口不能再被其它联动组引用。

### 43.6.1 添加接口联动组

1．进入**网络配置>接口>接口联动**，如下图：


**联动功能**：接口联动使能开关

**链路状态**：接口联动组中接口的状态

**名称**：接口联动组名称

**接口成员**：接口联动组中加入的物理接口成员

2．点击**新建**创建接口联动组，如下图：


**名称**：接口联动组名称

**接口成员**：勾选方式选择需要加入接口联动组的物理接口

注意 已经加入联动组中的物理接口不能再被其它联动组引用

### 43.6.2 修改接口联动

1. 进入**网络配置>接口>接口联动**，如下图：


2. 点击**名称**修改。


修改联动组中引用的接口成员。

3. 点击**更新**完成修改。

### 43.6.3 删除接口联动

1. 进入**网络配置>接口>接口联动**，如下图：


2. 点击删除接口联动。


3. 点击**确定**删除联动组。

# 43.7 配置案例

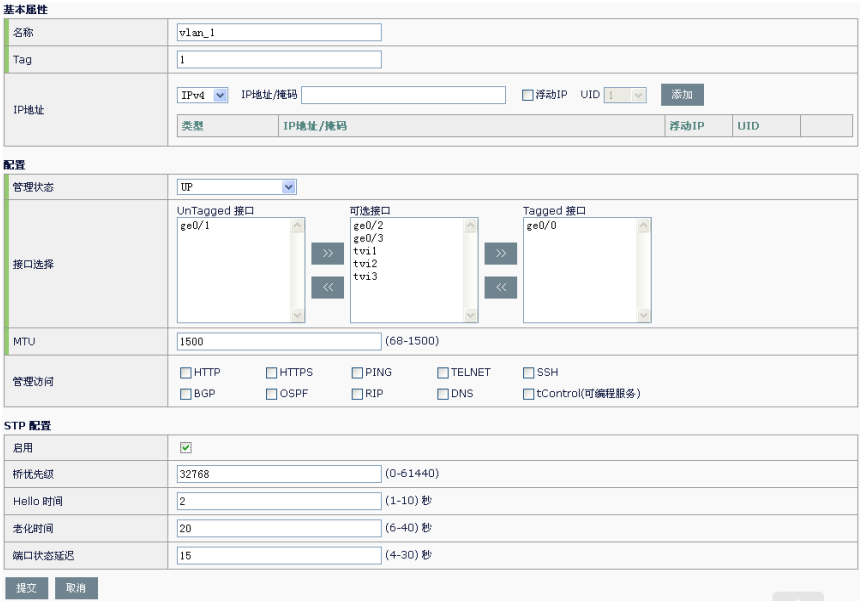
## 43.7.1 配置案例1：增加一个VLAN

**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**网络配置>接口>VLAN 列表**，点击**新建**，如下图：




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

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

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

5. 点击**提交**完成创建 VLAN。

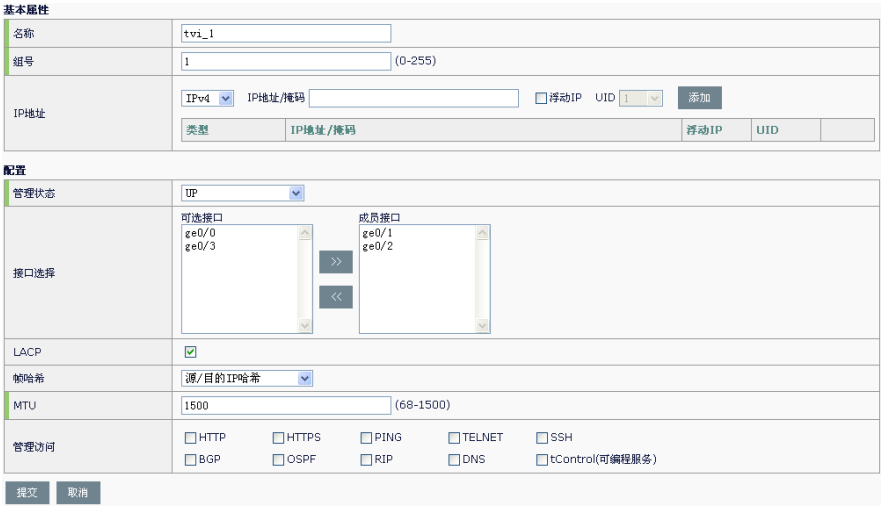
## 43.7.2 配置案例2：增加一个链路聚合

**案例描述**

创建一个链路聚合组，并在其中加入物理接口成员。

**配置步骤：**

1. 进入**网络配置>接口>链路聚合列表**，点击**新建**，如下图：




输入参数：名称 tvi1，组号 1，管理状态 UP。

2. **可选接口**中的接口 ge0/1、ge0/2 点击 >> 加入到链路聚合中。
3. **开启 LACP**，**帧哈希**选择源/目的 IP 哈希。
4. 点击**提交**完成创建链路聚合。

## 43.8 常见故障分析

### 43.8.1 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 聚合口配置，使两端聚合 LACP 协商成功 |

### 43.8.2 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 | 检查对端发送是否与 tag 相同的 802.1q 协议报文 |

# 44 第44章 静态路由

## 44.1 静态路由概述

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

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

## 44.2 配置静态路由

### 44.2.1 配置IPv4静态路由

**配置步骤：**

进入**网络>路由>静态路由：IPv4**，配置界面如下：


**IP 地址/掩码**：静态路由的目的网段。

**下一跳地址**：静态路由网关地址。

**出接口**：静态路由的出接口。

**权重**：路由权重，范围 1-100，等价路由情况下按照权重比例轮询转发。

**距离**：路由优先级，范围<1-255>。

**健康检查**：引用健康检查模板，支持 TCP 和 ICMP 两种健康检查方式。

点击**提交**，完成设置。

注意

静态路由健康检查的对象只能是路由的下一跳地址。

## 44.2.2 查看IPv4路由表

**配置步骤：**

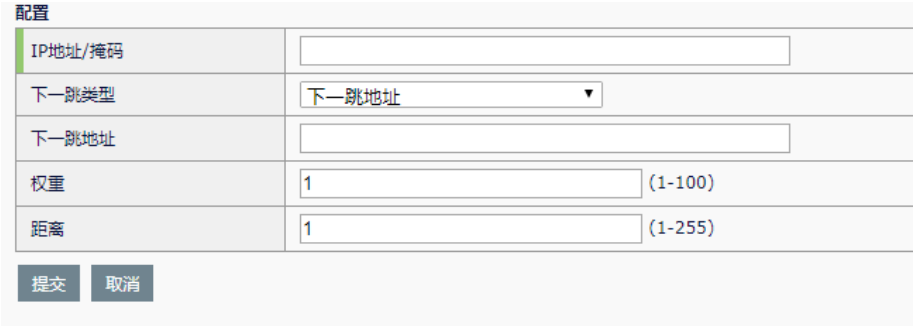
进入**网络>路由>路由表：IPv4**


此界面可以查看系统的路由信息，并且可以根据类型，目的地址及下一跳进行检索。

## 44.2.3 配置IPv6静态路由

**配置步骤：**

进入**网络>路由>静态路由：IPv6**




**IP 地址/掩码**：目的 IPv6 地址及掩码。

**下一跳类型**：下一跳地址、出接口、下一跳地址和出接口

**下一跳地址**：路由网关地址。

**出接口**：数据转发的出接口。

**下一跳地址和出接口**：路由网关地址和数据转发的出接口。

**权重**：路由权重，范围 1-100。

**距离**：路由优先级，范围<1-255>。

点击**提交**，完成设置。

### 44.2.4 查看IPv6路由表

**配置步骤：**

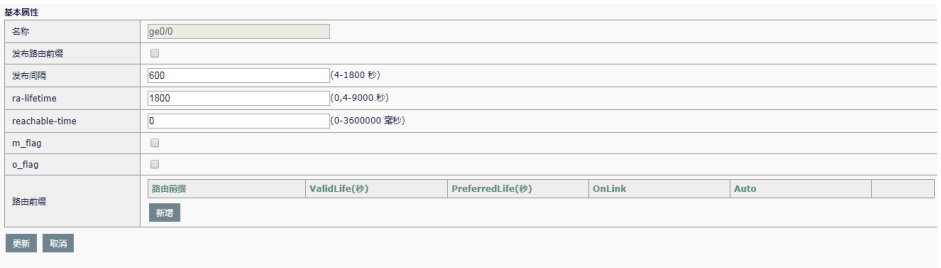
进入**网络>路由>路由表>IPv6**


此界面可以查看系统的路由信息，并且可以根据类型，目的地址及下一跳进行检索。

### 44.2.5 IPv6前缀公告

**配置步骤：**

进入**网络>路由> IPv6 前缀公告**




**名称：**发生路由前缀的 vlan 接口名称

**发布路由前缀：**启用/关闭前缀公告

**发布时间间隔：**每发布一次路由前缀的时间间隔

**ra-lifetime：**路由前缀生存时间

**reachable-time：**路由器可到达时间

**m_flag：**管理地址配置标示

**o_flag：**其他状态配置标示

**路由前缀：**所要发布的路由前缀

**ValidLife：**路由前缀有效生存时间

**PreferredLife：**路由前缀首选生存时间

点击**更新**完成设置。

## 44.3 配置案例

### 44.3.1 配置案例1：对多条路由配置路由监控

**案例描述：**

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

用户需求如下：

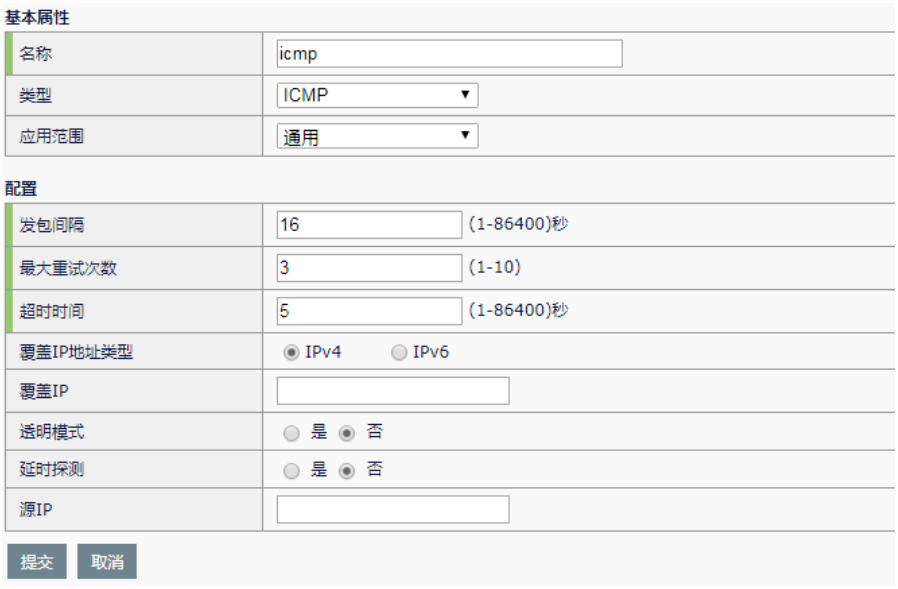
1. 配置两条默认路由，同时需要对下一跳的可用性进行健康检查。当健康检查失败，则将路由状态置为失效，以保证业务可以转发到其他可用下一跳上。

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

**配置步骤：**

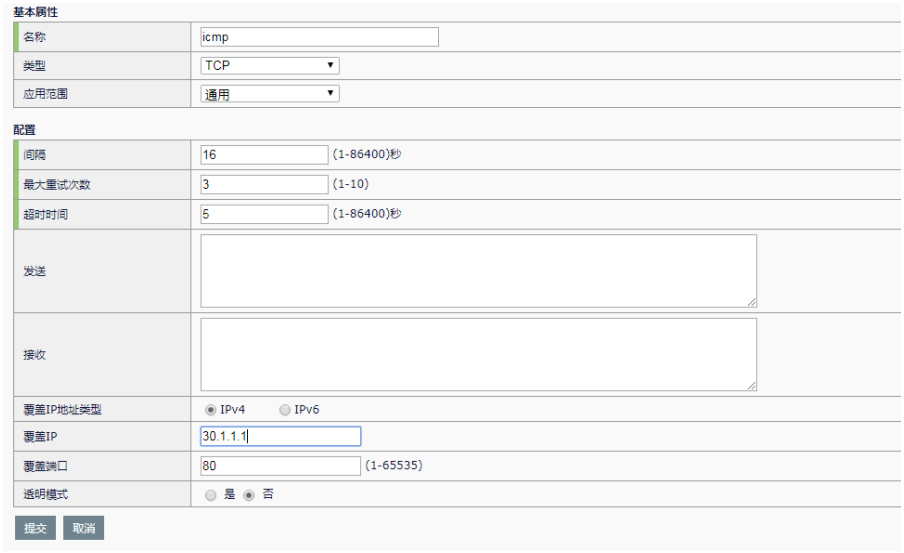
1. 进入**模板和对象>健康检查**，创建 ICMP 类型的健康检查。覆盖 IP 不填写则自

动选择路由的下一跳作为健康检查的对象。



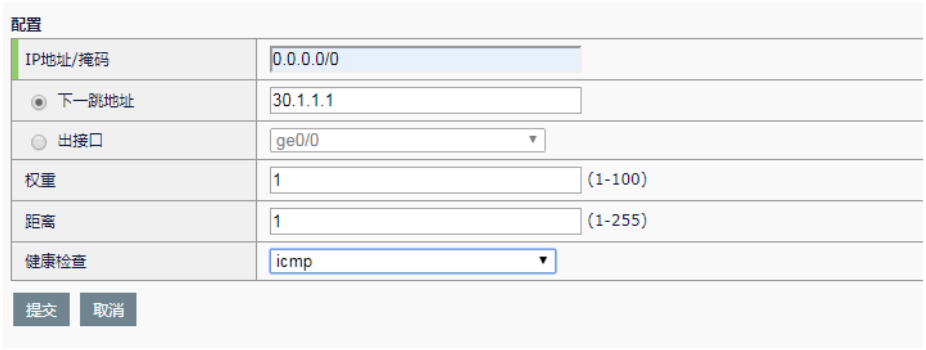

2. 进入模板对象>健康检查，创建 TCP 类型的健康检查。覆盖 IP 填写路由下

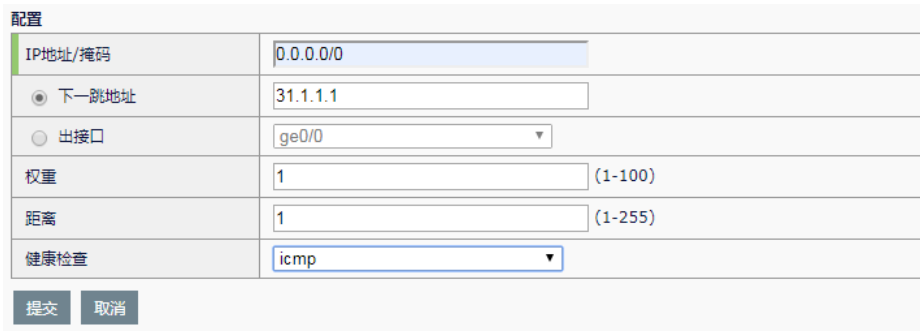
一跳地址，覆盖端口填写下一跳开放的端口。

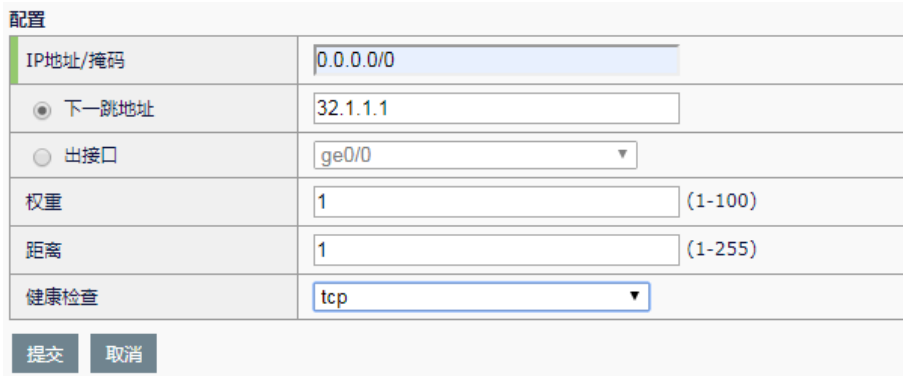



3. 进入**网络>路由>静态路由**，配置添加三条默认路由，30.1.1.1 和 31.1.1.1

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






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

为有效。若健康检查失败，则路由会显示为失效状态。

## 44.4 常见故障分析

### 44.4.1 路由状态为失效状态

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

# 45 第45章 静态路由 BFD

## 45.1 BFD概述

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

## 45.2 配置说明

### 45.2.1 配置静态路由BFD

进入**网络>路由>静态路由 BFD**


**源地址**：静态路由 BFD 的源地址。

**下一跳地址**：静态路由 BFD 的目的地址，即静态路由的下一跳地址。

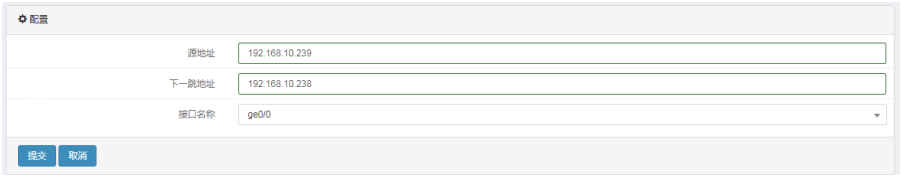
**接口名称**：与下一跳连接的接口名称。

**新建**：新建一条静态路由 BFD。

：删除该条静态路由 BFD。

**配置静态路由 BFD：**

点击**新建**按钮。




**源地址**：静态路由 BFD 的源地址。

**下一跳地址**：静态路由 BFD 的目的地址，即静态路由的下一跳地址。

**接口名称**：与下一跳连接的接口名称。

**提交**：新建该条静态路由 BFD。

**取消**：取消本次配置。

## 45.3 配置案例

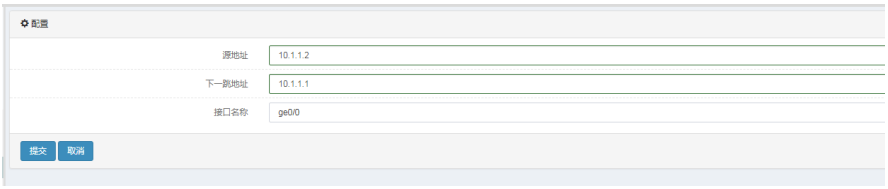
### 45.3.1 配置BFD与静态路由联动

**案例描述：**

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


**FWA 的配置步骤：**

1、进入**网络>路由>静态路由 BFD**，点击新建，如下图：




**源地址**：静态路由 BFD 的源地址为 10.1.1.2。

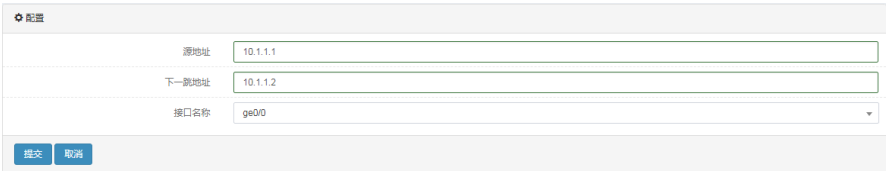
**下一跳地址**：静态路由 BFD 的目的地址，即静态路由的下一跳地址为 10.1.1.1。

**接口名称**：与下一跳连接的接口名称是 ge0/0。

2、点击**提交**完成设置。

**FWB 的配置步骤：**

1、进入**网络>路由>静态路由 BFD**，点击新建，如下图：




**源地址**：静态路由 BFD 的源地址为 10.1.1.1。

**下一跳地址**：静态路由 BFD 的目的地址，即静态路由的下一跳地址为

10.1.1.2。

**接口名称**：与下一跳连接的接口名称是 ge0/0。

2、点击**提交**完成设置。

## 45.4 故障分析

### 45.4.1 BFD邻居建立失败

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

# 46 第46章 配置 RIP

## 46.1 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。

## 46.2 配置RIP协议

### 46.2.1 缺省配置信息

ADC 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 |

### 46.2.2 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**网络配置>路由>动态路由>RIP**：


**参数说明：**

**RIP 版本：**RIP 的版本 1 或者 2

2. 点击**提交：**完成对版本的设置，并按默认值提交高级选项。

### 46.2.3 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**网络配置>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。

### 46.2.4 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**网络配置>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。

### 46.2.5 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**网络配置>路由>动态路由>RIP**：


2. 点击**新增**：进入接口配置页面。


**接口**：需要进行配置的接口名

**发送版本**：接口的发送报文版本

**接收版本**：接口的接收报文版本

**认证算法**：接口的认证类型

点击**提交**：完成对接口的配置

点击**取消**：取消对接口的配置

3. 按上图配置，点击**提交**


点击**接口名称**：对已有的接口配置进行编辑。

点击  ：删除对应接口的配置。

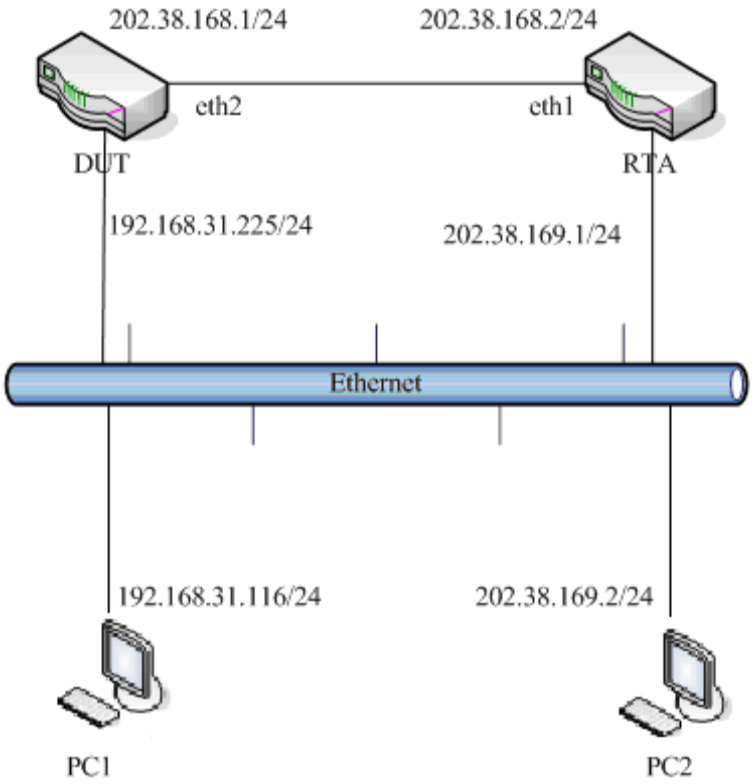
## 46.3 配置案例

### 46.3.1 配置案例：配置两台ADC设备互连

**案例描述**

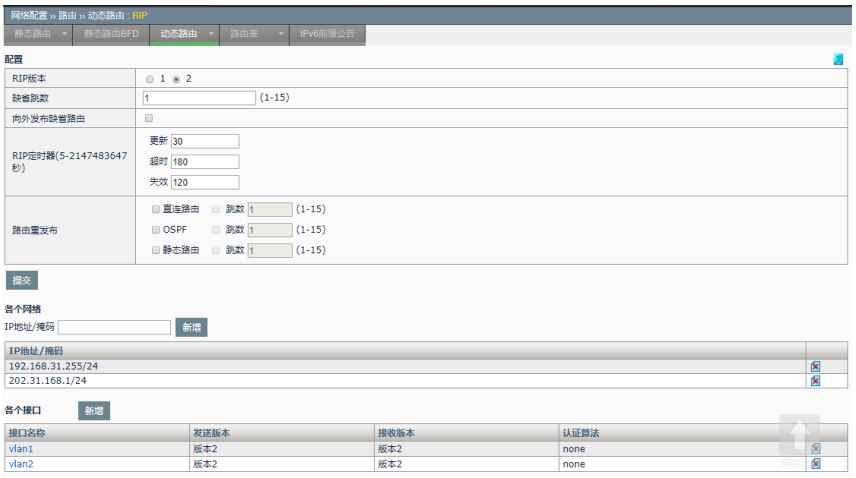
DUT 和 RTA 都为 ADC 设备，IP 地址配置如图，DUT 在 vlan0 和 vlan2 接口上启用了 RIP，RTA 在接口 vlan0 和 vlan1 上启用了 RIP，两个设备互连的接口收发报文的版本都设置为 2）。

**案例组网图：**

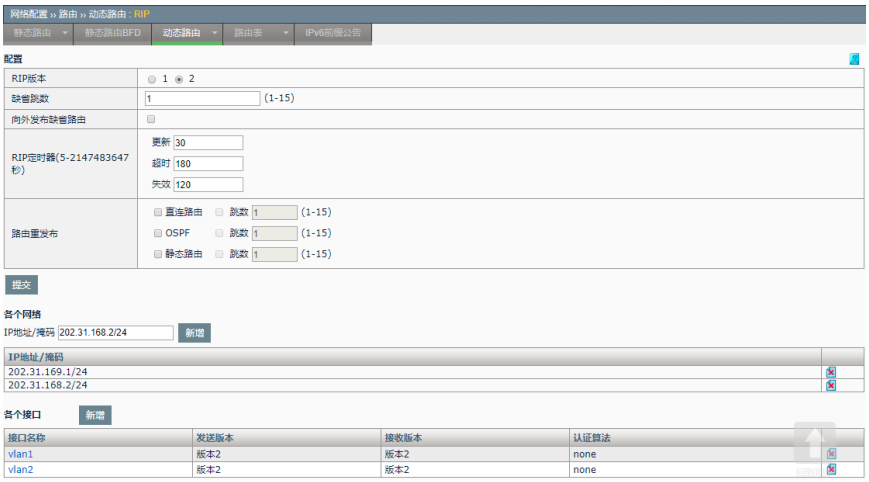



**配置步骤：**

1. 配置 DUT 的基本信息。




2. RTA 的基本配置。

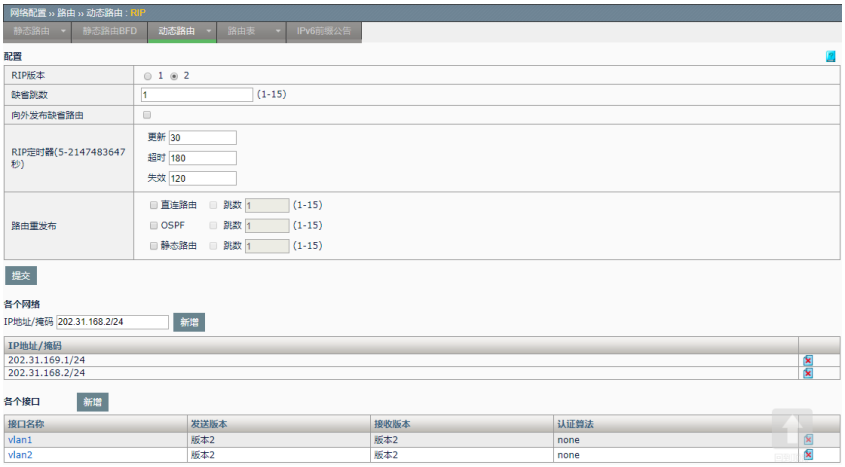



3. 配置 PC1 的网关为 192.168.31.225，配置 PC2 的网关为 202.38.169.1。从 PC1PING 向 PC2，可以 PING 通。

## 46.4 查看RIP配置信息

### 46.4.1 查看RIP配置信息

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




## 46.5 常见故障分析

### 46.5.1 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 |

# 47 第47章 配置 OSPF

## 47.1 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。

## 47.2 配置OSPF协议

### 47.2.1 缺省配置信息

ADC 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 | 不认证 | 可更改设置 |

| | | |
|---|---|---|
| （none/text/md5） | | |
| 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 |

### 47.2.2 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**网络配置>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。

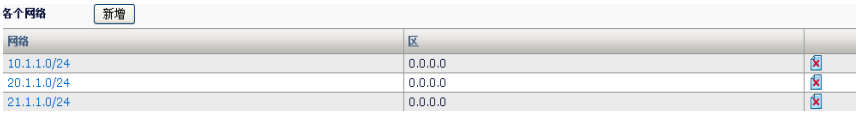
**权重：**三种重发布类型重发布的权重。

2. 点击**提交：**完成对 OSPF 的设置。

### 47.2.3 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**网络配置>路由>动态路由>OSPF**




2. 点击**新增**：


**IP 地址/掩码**：网络地址和网络地址掩码

**区域**：区域 ID

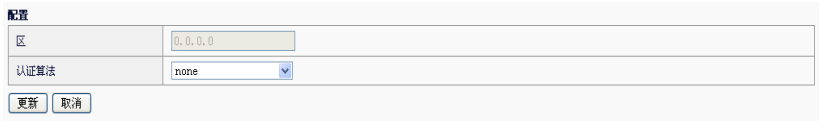
3. 点击**提交**。

### 47.2.4 编辑区域属性

编辑区域的认证方式：

1. 进入**网络配置>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**。

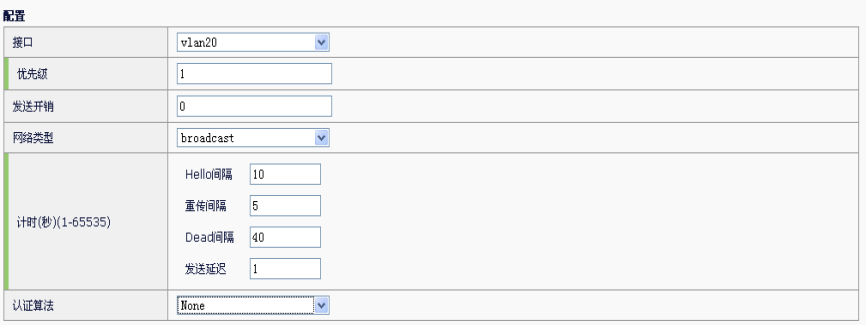
### 47.2.5 配置OSPF接口

配置接口收发报文的版本和认证类型。

**配置步骤：**

1. 进入**网络配置>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。

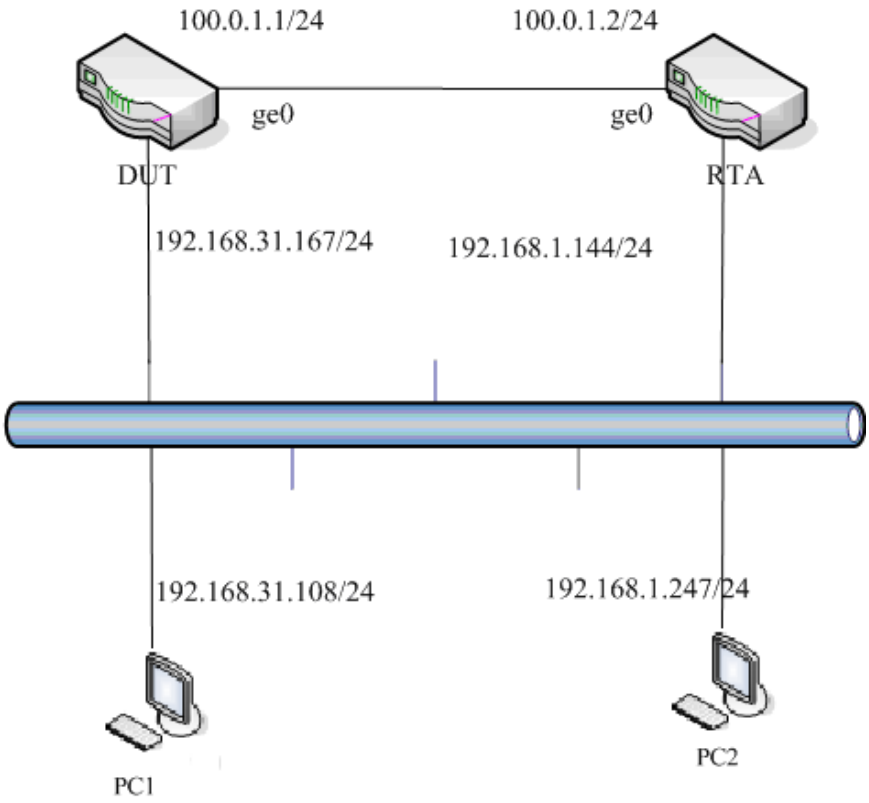
## 47.3 配置案例

### 47.3.1 配置案例：配置两台ADC设备互连

**案例描述**

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

**案例组网图：**

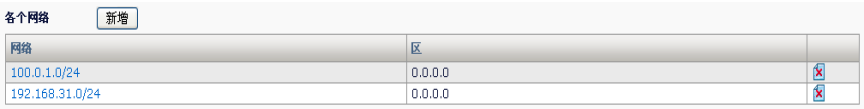



**配置步骤：**

1. 配置 DUT 的基本信息。


路由器 ID 自动选举产生，所以可以不输入路由器 ID，直接**提交**。

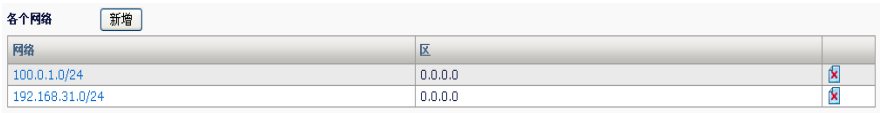
2. 配置 DUT 发布的网络。




3. 配置 RTA 的基本信息：

路由器 ID 自动选举产生，所以可以不输入路由器 ID，直接**提交**。

4. 配置 RTA 发布的网络：




## 47.4 OSPF监控与维护

### 47.4.1 查看邻居路由器状态信息

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


## 47.5 常见故障分析

### 47.5.1 故障现象：两台设备不能建立邻接关系

| | |
|---|---|
| 现象 | 两台设备不能建立邻接关系 |
| 分析 | 1. 区域ID不匹配<br>2. 认证类型不匹配<br>3. 密钥不匹配<br>4. 网段（网络掩码匹配）<br>5. Hello-interval不匹配<br>6. Dead-interval不匹配<br>7. 两台设备间是否需要建立邻接关系？ |
| 解决 | 1. 检查接口上OSPF参数的配置<br>2. 是否应该和邻居路由器建立一个邻接关系，满足下列条件中的一个或者多个，那么将建立邻接关系：<br>A、 网络类型是点对点的<br>B、 网络类型是点到多点的<br>C、 网络类型是虚链路<br>D、 本地路由器是邻接路由器所在网络的 DR<br>E、 本地路由器是邻接路由器所在网络的 BDR<br>F、 邻居路由器是 DR<br>G、 邻居路由器是 BDR |

# 48 第48章 配置 OSPFv3

## 48.1 OSPFv3协议概述

OSPFv3(Open Shortest Path First)是动态路由协议,其功能是实现网际间的路由。

OSPFv3(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，OSPFv3 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。

OSPFv3 是自治系统内部使用的链路状态路由协议，OSPFv3 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，OSPFv3 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 OSPFv3 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，OSPFv3 协议支持 IPV6 子网结构。

OSPFv3 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 OSPFv3 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。

## 48.2 配置OSPFv3协议

### 48.2.1 缺省配置信息

ADC 设备关于 OSPFv3 的缺省设置信息如以下表所示：

OSPF 缺省配置信息

| 5. 内容 | 6. 缺省设置 | 7. 备注 |
|---|---|---|
| 使能/禁止状态（enable/disable） | disable | 可更改设置 |
| LSA重传时间 | 5秒 | 不可更改 |

| | | |
|---|---|---|
| LSA发送延迟 | 1秒 | 不可更改 |
| Hello-interval值 | 10秒 | 不可更改 |
| Dead-interval值 | 4* Hello-interval | 不可更改 |
| 接口选举DR的优先级 | 1 | 不可更改 |

### 48.2.2 配置OSPFv3

OSPFv3 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。设备不支自动选取路由器 ID，必须需要手动配置。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**网络配置>路由>动态路由>OSPFv3**


**路由器 ID：**在路由器 ID 后输入路由器 ID。

**直连路由：**设置是否重发布直连路由。

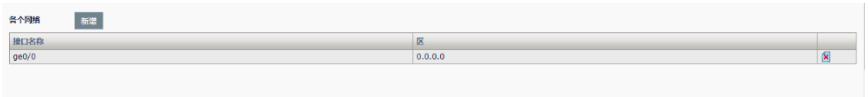
**静态路由：**设置是否重发布静态路由。

2. 点击**提交：**完成对 OSPFv3 的设置。

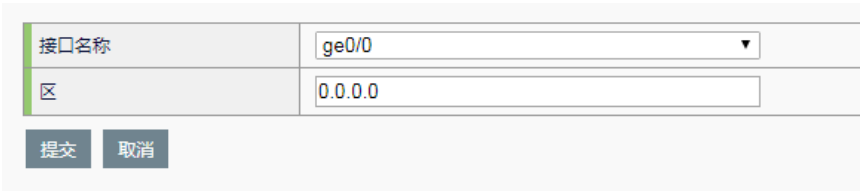
### 48.2.3 配置OSPFv3的接口区域

配置运行 OSPFv3 的接口以及其所属的区域。

1. 进入**网络配置>路由>动态路由>OSPFv3**




2. 点击**新增：**




**接口名称：**需要进行配置的接口名。

**区：**区域 ID

3. 点击提交

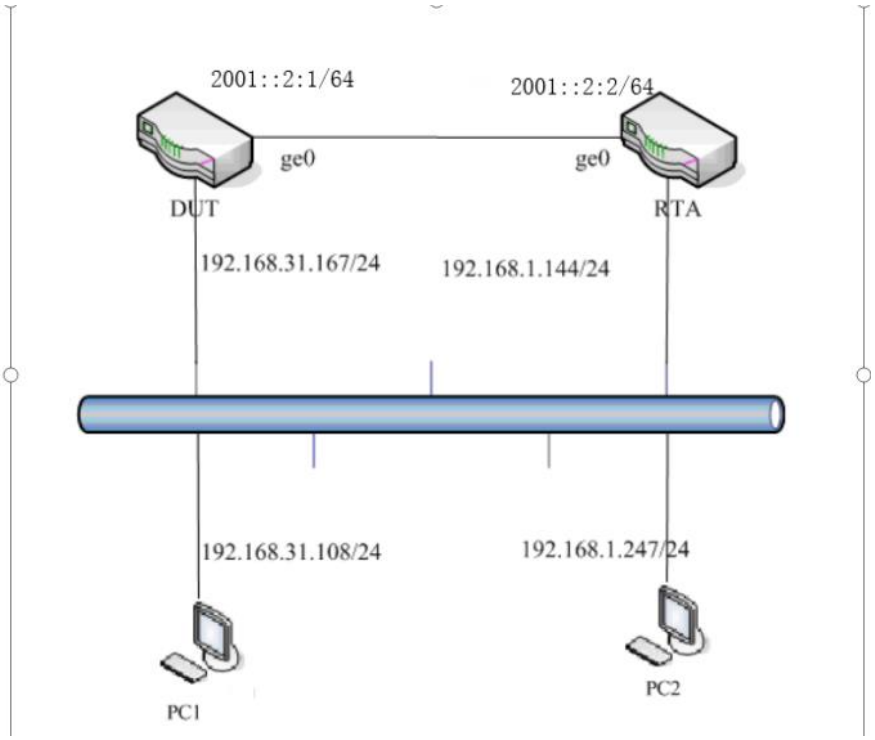
## 48.3 配置案例

### 48.3.1 配置案例：配置两台ADC设备互连

**案例描述**

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

**案例组网图：**

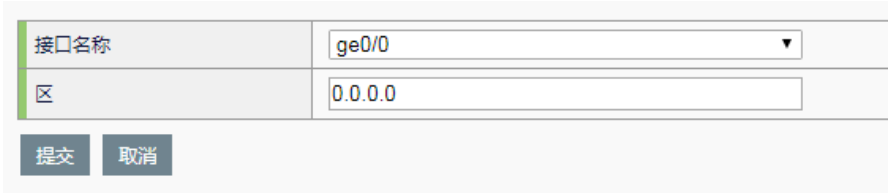



**配置步骤：**

1. 配置 DUT 的基本信息。


输入路由器 ID，点击**提交**。

2. 配置 DUT 接口信息与区域。




3. 配置 RTA 的基本信息：


输入路由器 ID，点击**提交**。

4. 配置 RTA 接口信息与区域：


## 48.4 常见故障分析

### 48.4.1 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 | 1. 区域ID不匹配<br>2. 认证类型不匹配<br>3. 密钥不匹配<br>4. 网段（网络掩码不匹配）<br>5. Hello-interval不匹配<br>6. Dead-interval不匹配<br>7. 两台设备间是否需要建立邻接关系？ |
| 解决 | 1. 检查接口上OSPF参数的配置<br>2. 是否应该和邻居路由器建立一个邻接关系，满足下列条件中的一个或者多个，那么将建立邻接关系：<br>3. 网络类型是点对点的<br>4. 网络类型是点到多点的<br>5. 网络类型是虚链路<br>6. 本地路由器是邻接路由器所在网络的DR<br>7. 本地路由器是邻接路由器所在网络的BDR<br>8. 邻居路由器是DR |

| | |
|---|---|
| | 9. 邻居路由器是BDR |

# 49 第49章 配置 BGP4

## 49.1 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。

## 49.2 配置BGP协议

### 49.2.1 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 |

### 49.2.2 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**网络配置>路由>动态路由>BGP4


**参数说明：**

**BGP 设置**：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。

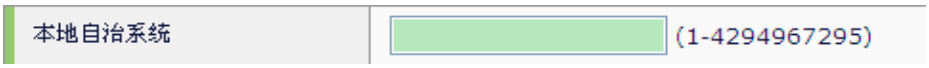
2. 点击**提交**：完成对路由器 ID 设置，并且按照高级选项的默认值进行配置。

### 49.2.3 配置运行BGP

配置启动 BGP

**配置步骤：**

1. 进入网络配置>路由>动态路由>BGP4




**参数说明：**

**本地自治系统号：**1 到 4294967295

2. 点击**提交：**运行 BGP。

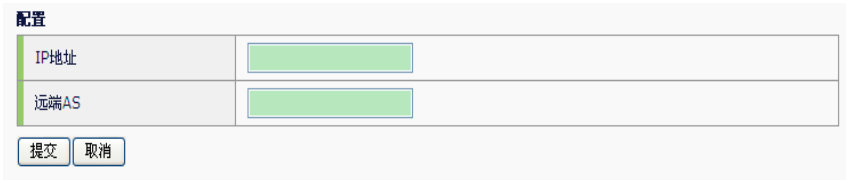
### 49.2.4 配置指定BGP的对等体

配置指定 BGP 的对等体

**配置步骤：**

**1. 进入**网络配置>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。

### 49.2.5 配置宣告网络

配置宣告网络：

**配置步骤：**

**1.**进入**网络配置>路由>动态路由>BGP4：**


**IP 地址：**对应要宣告的地址和子网掩码

2.点击**新增：**完成添加。

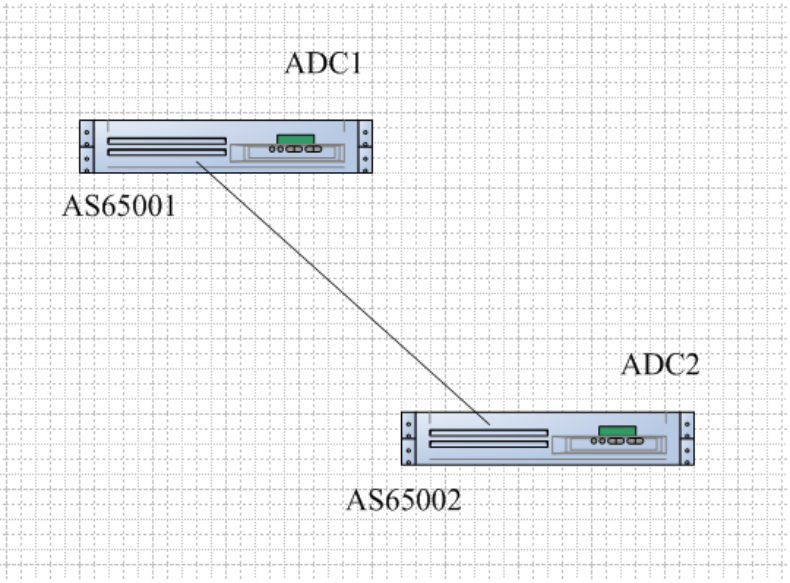
## 49.3 配置案例

### 49.3.1 配置案例1：配置两台ADC设备互连

**案例描述：**

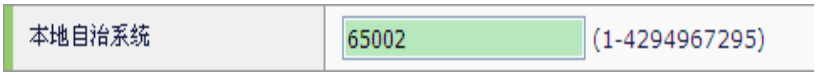
ADC1 和 ADC2 同为 ADC 设备，ADC1 属于 AS65001，ADC2 属于 AS65002，他们之间建立 EBGP 对等体。

**案例组网图：**

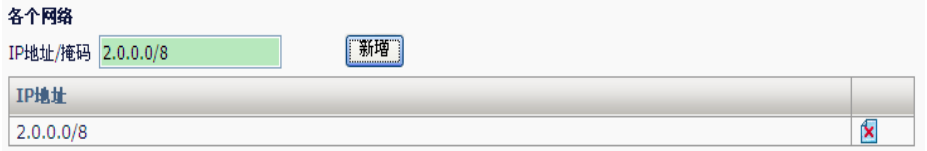



**配置步骤：**

1. 配置运行 BGP。




2. 配置 ADC1 发布的网络。




3. 配置 ADC1 的对等体。

## 49.4 BGP监控与维护

### 查看BGP路由信息

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


## 49.5 常见故障分析

### 49.5.1 故障现象1：两台设备不能建立邻接关系

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

# 50 第50章 静态 ARP

## 50.1 静态ARP概述

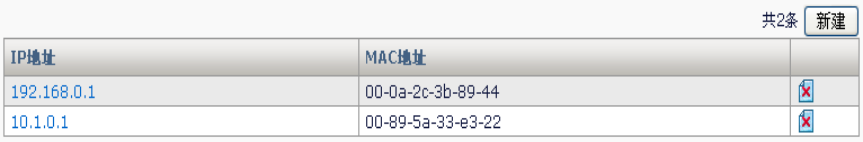
IP 数据包常通过以太网发送。以太网设备并不识别 32 位 IP 地址：它们是以 48 位以太网地址(MAC 地址)传输以太网数据包的。因此，IP 驱动器必须把 IP 地址转换成 MAC 地址。在这两种地址之间存在着某种静态的或算法的映射，常常需要查看一张表。地址解析协议(Address Resolution Protocol，ARP)就是用来确定这些映象的协议。

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。

## 50.2 静态ARP配置

### 50.2.1 添加静态ARP

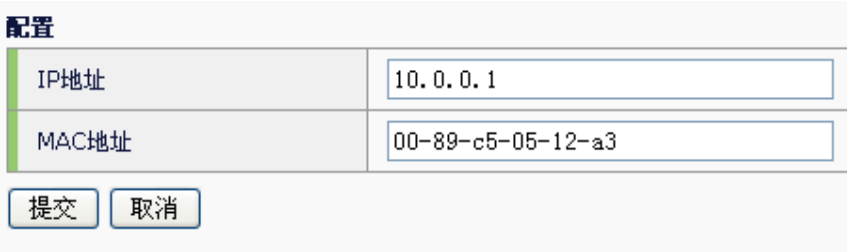
1. 进入**网络配置>ARP>静态 ARP**，如下如所示：




**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

2. 点击**新建**添加静态 ARP，如下图所示：




**IP 地址**：静态 ARP 被绑定的 IP 地址

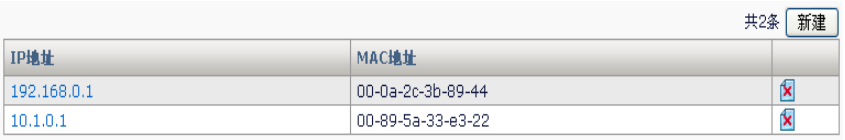
**MAC 地址**：静态 ARP 被绑定的 MAC 地址

3. 点击**提交**完成今天 ARP 的添加。

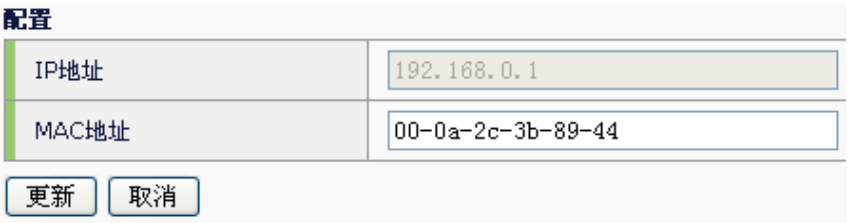

配置静态 ARP 时，MAC 地址可以重复添加，但 IP 地址必须唯一。

### 50.2.2 修改静态ARP

1. 进入**网络配置>ARP>静态 ARP**，如下如所示：




2. 点击静态 ARP 的 **IP 地址**修改，如下图所示：




修改静态 ARP 的 MAC 地址信息。

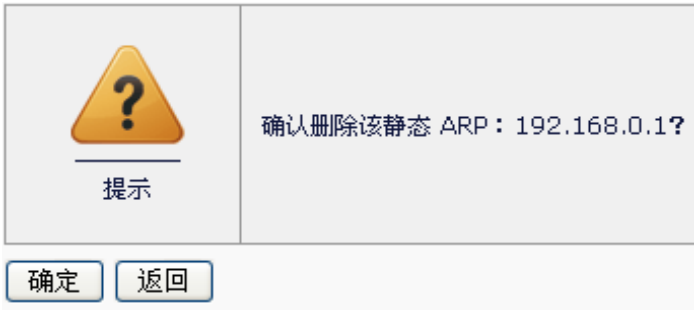
3. 点击**更新**完成修改。


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

### 50.2.3 删除静态ARP

1. 进入**网络配置>ARP>静态 ARP**，如下如所示：


2. 点击  删除静态 ARP，如下图所示：




3. 点击**确定**删除。

## 50.3 常见故障分析

### 50.3.1 故障现象：添加静态ARP后网络不通

| | |
|---|---|
| 现象 | 添加静态 ARP 对端网络不通 |
| 分析 | 可能是静态ARP 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 |

# 51 第51章 配置 NAT

## 51.1 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。

应用交付设备提供了源地址转换和静态地址转换功能。

## 51.2 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。


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。

### 51.2.1 配置地址池(NATPool)

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

在进行地址转换后，报文的真实地址将被转换为地址池中的地址。

**配置步骤：**

1. 进入**网络配置>NAT>NAT 地址池**，点击**新建。**


**名称：**NAT 地址池的名称，可以是中文，不得超过 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。

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

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

**下一跳地址：**向服务器 IP 发送报文时的下一跳 IP 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**。

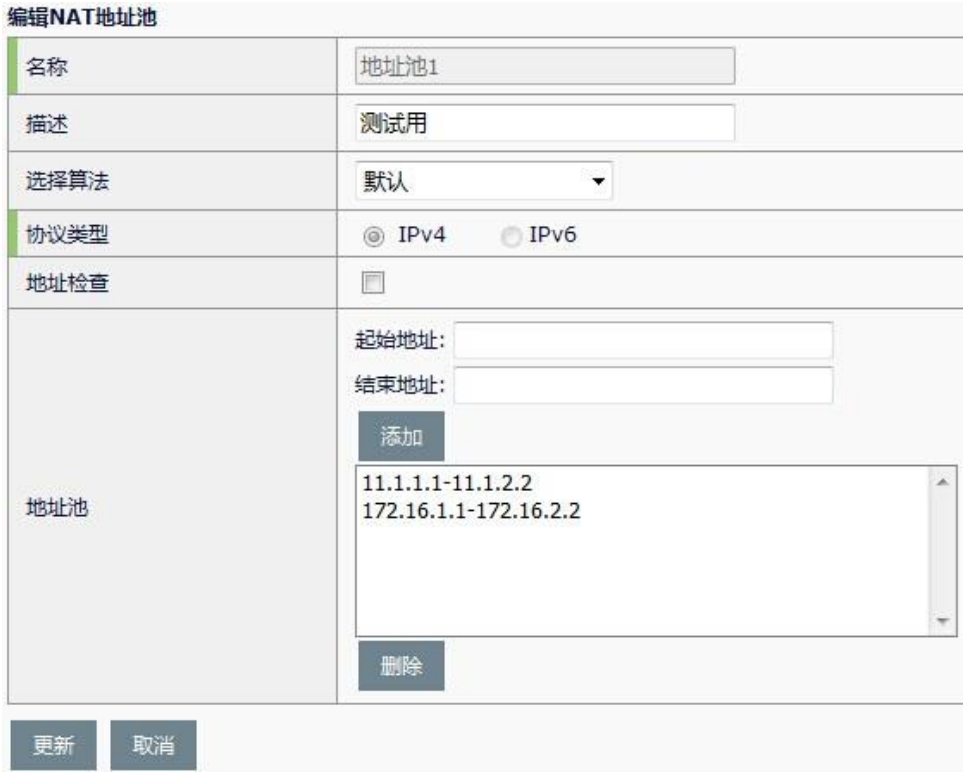
### 51.2.2 编辑地址池

已经创建的地址池可以编辑修改。

**编辑步骤：**

1. 进入**网络配置>NAT>NAT 地址池**。


点击地址池名称。




可以对地址池进行编辑修改。其中名称与协议类型是不允许变更的。

点击**更新**。

### 51.2.3 删除地址池

**地址池删除步骤：**

1. 进入**网络配置>NAT>NAT 地址池**。


2. 点击  ，删除选定的地址池。


当删除按钮为灰色时，表明该地址池正在被某处引用（可能是 NAT 规则，或者是虚拟服务，或者是虚拟链路），不能被删除。

### 51.2.4 配置源地址转换

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

**配置步骤：**

**1.** 进入**网络配置>NAT>NAT 规则>源地址转换**，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。

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

**描述**：对该转换规则的描述，最长不得超过 128 个字符。

**日志**：是否需要对该规则启用日志。

**2.** 点击**提交**。

### 51.2.5 配置目的地址转换

目的地址转换是一种单向的针对目的地址的映射，主要用于外网访问内网，隐藏内部设备地址。

配置步骤：

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


**源地址**：NAT 规则匹配的源地址，可以是地址对象或地址组。

**目标地址**：NAT 规则匹配的目的地址，可以是地址对象或地址组。

**服务**：NAT 规则匹配的服务名，可以是服务对象或服务组。

**入接口**：NAT 规则匹配的入接口。

**转换后的目的地址**：需要转换成的目的地址，可以选择地址池内的地址进行转换。

**转换后端口**：需要转换成的目的端口。

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

**描述**：对该转换规则的描述，最长不得超过 128 个字符。

**日志**：是否需要对该规则启用日志。

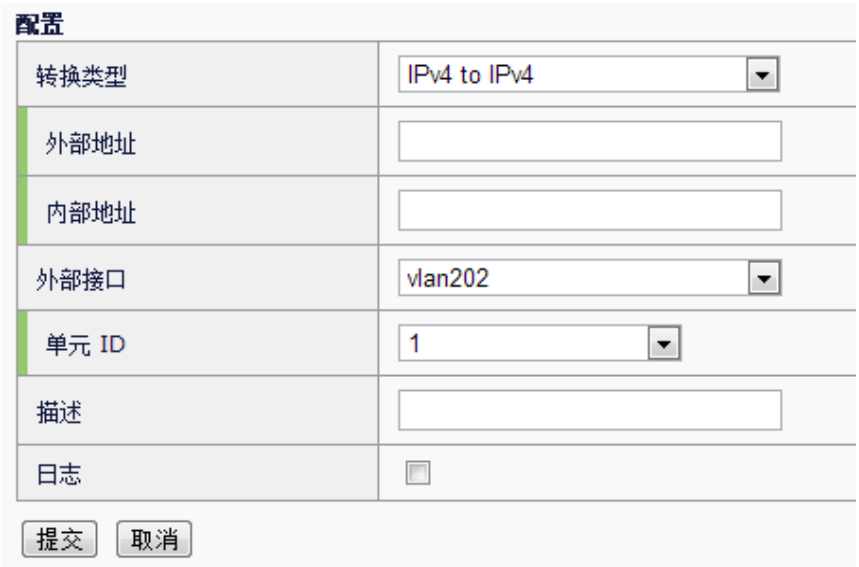
**2.** 击**提交。**

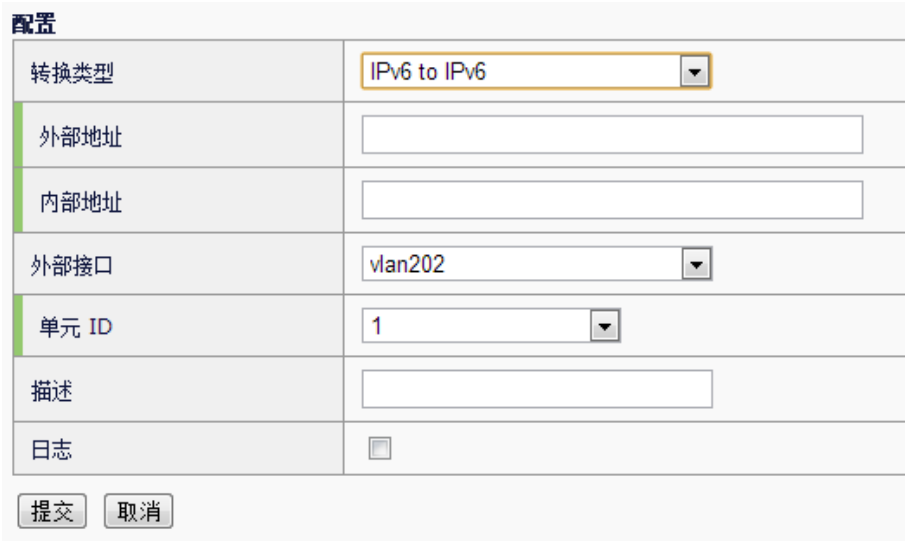
### 51.2.6 配置静态地址转换

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**网络配置>NAT>NAT 规则>静态地址转换**，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。

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

**描述**：对该转换规则的描述，不得超过 128 个字符。

**日志**：是否需要对该规则启用日志。

**2.** 点击**提交**。


配置静态 NAT，需要先配置相关的路由模式虚拟服务或者虚拟链路才会生效。

### 51.2.7 编辑NAT规则

已经创建的 NAT 规则可以编辑修改。

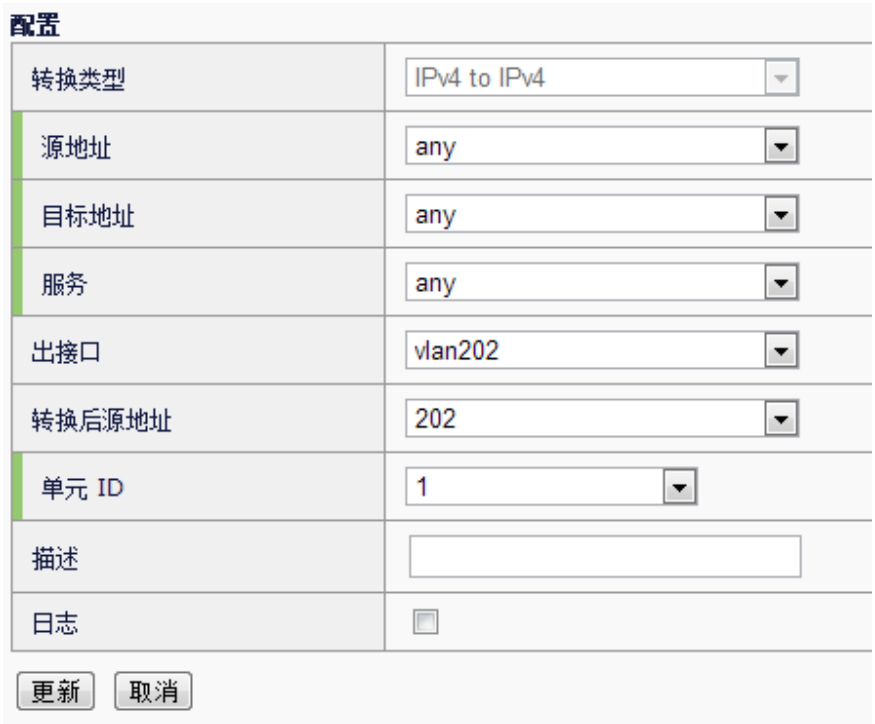
**源地址转换的 NAT 规则编辑步骤：**

1. 进入**网络配置>NAT>NAT 规则>源地址转换。**

| # | 转换类型 | 源地址 | 目标地址 | 服务 | 出接口 | 转换后源地址 | 日志 | 描述 | |
|---|---|---|---|---|---|---|---|---|---|
| 3 | IPv4 to IPv4 | 10.1.1.2 | 192.168.3.2 | any | vlan202 | 202 | 禁用 | | |

| # | 转换类型 | 源地址 | 目标地址 | 服务 | 出接口 | 转换后源地址 | 日志 | 描述 | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | IPv6 to IPv6 | IPv6 | 2001:192::2 | any | vlan202 | 出接口地址 | 禁用 | | |

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。

**2.** 点击**提交。**

### 51.2.8 删除NAT规则

源地址转换的 NAT 规则删除步骤：

1. 进入**网络配置>NAT>NAT 规则>源地址转换。**

| # | 转换类型 | 源地址 | 目标地址 | 服务 | 出接口 | 转换后源地址 | 日志 | 描述 | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | IPv6 to IPv6 | IPv6 | 2001:192::2 | any | vlan202 | 出接口地址 | 禁用 | | |

2. 点击  ，删除选定的 NAT 规则。

### 51.2.9 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**网络配置>NAT>NAT 规则>源地址转换。**

| # | 转换类型 | 源地址 | 目标地址 | 服务 | 出接口 | 转换后源地址 | 日志 | 描述 | |
|---|---|---|---|---|---|---|---|---|---|
| 2 | IPv4 to IPv4 | any | any | any | 电信 | 出接口地址 | 禁用 | | |
| 3 | IPv4 to IPv4 | any | any | aol | vlan1 | 出接口地址 | 禁用 | | |

2. 点击规则后的  ：


**规则 ID：**移动的目标规则 ID。

**移动到：**指定要移动的位置。

注意

规则移动时，只能在相同转换类型的规则之间移动。比如 IPv4 to IPv4 类型的规则只能移动到 IPv4 to IPv4 类型的规则前后，Pv6 to IPv6 类型的规则只能移动到 IPv6 to IPv6 类型的规则前后。

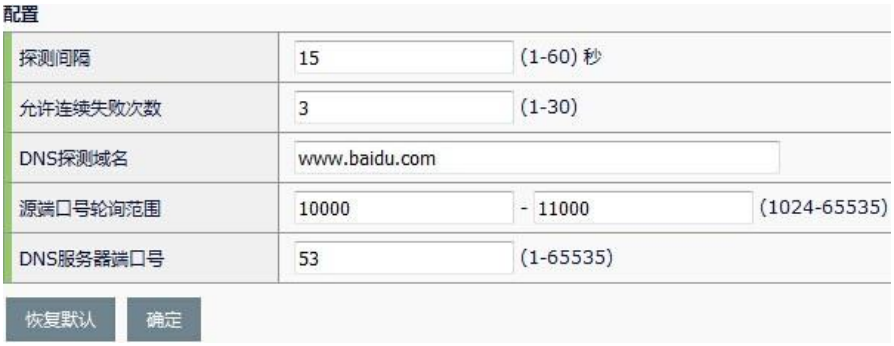
## 51.3 配置NAT地址池（NAT Pool）检查功能

### 51.3.1 配置地址池检查功能

该配置应用于检查地址池中的地址可用性。有默认配置。

配置步骤：

1. 进入**网络配置>NAT>NAT 地址池检查。**




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

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

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

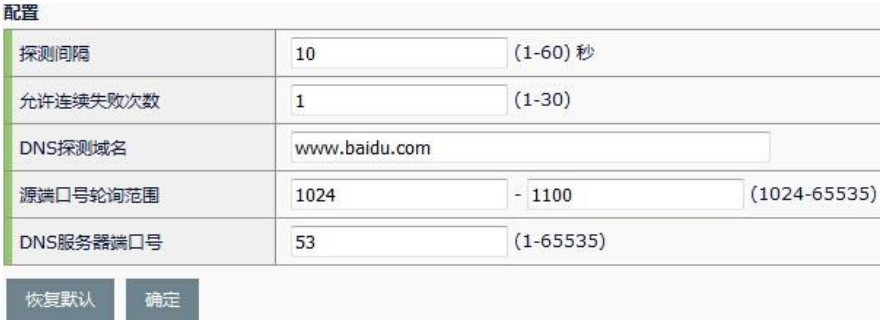
**源端口号轮询范围：**默认的范围为 10000~11000。源端口号轮询允许的范围为 1024~65535。

**DNS 服务器端口号：**默认值为 53。DNS 服务器端口号允许的范围为 1~65535。


注意

地址池检查功能仅限于 IPv4 协议类型。

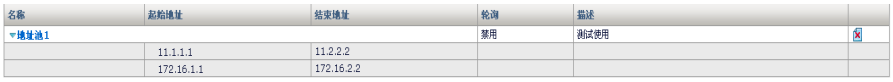
### 51.3.2 修改地址池检查功能



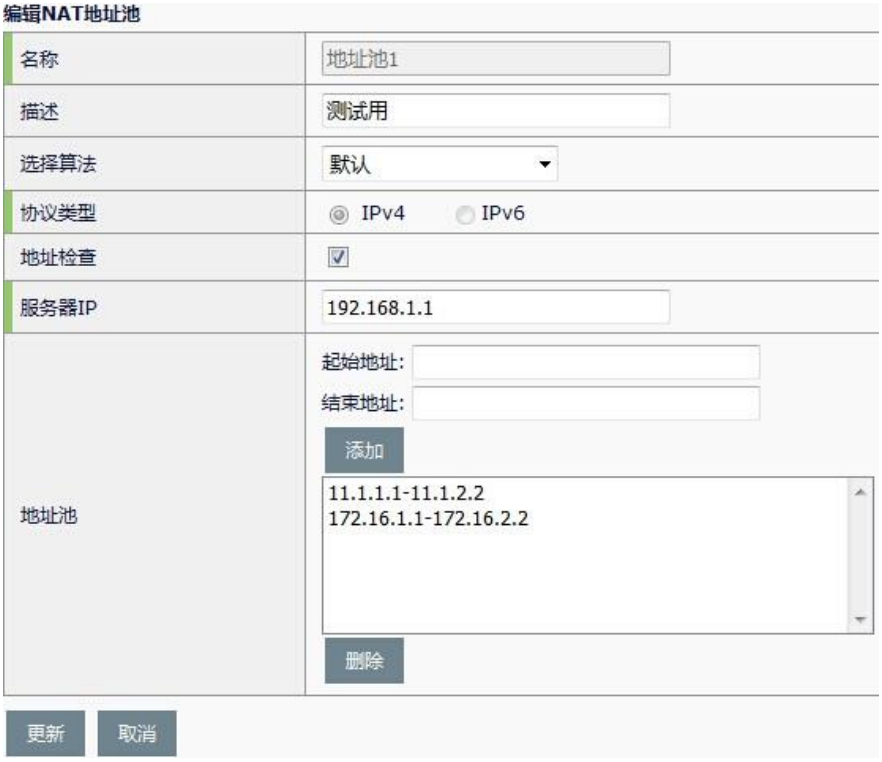

在相应的选项后面进行修改，完成后，按**确定键**。若想要恢复到默认配置，则按**恢复默认**键，再按**确定**。

### 51.3.3 开启地址池检查功能

**1.** 进入**网络配置>NAT>NAT 地址池。**




新建或选择需要开启检查功能的地址池。




2. 选中**地址检查**选项，填入需要的服务器 IP。点击确定即可。地址检查仅限于 IPv4 协议。

### 51.3.4 关闭地址池检查功能

**1.** 进入**网络配置>NAT>NAT 地址池。**


2. 选择需要关闭检查功能的地址池。


3. 勾选掉**地址检查**这一项。再点击**更新**即可。

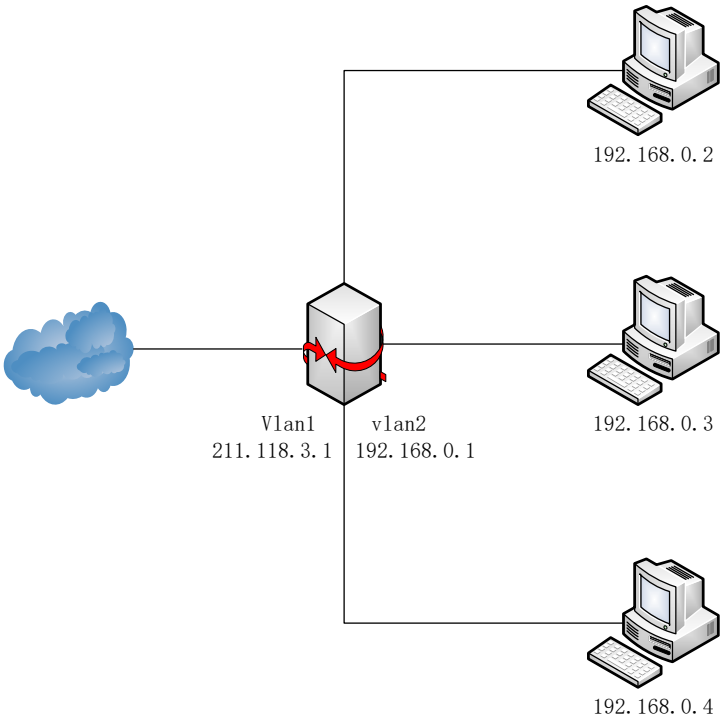
## 51.4 配置案例

### 51.4.1 配置源地址转换

**案例描述：**

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

**案例组网图：**

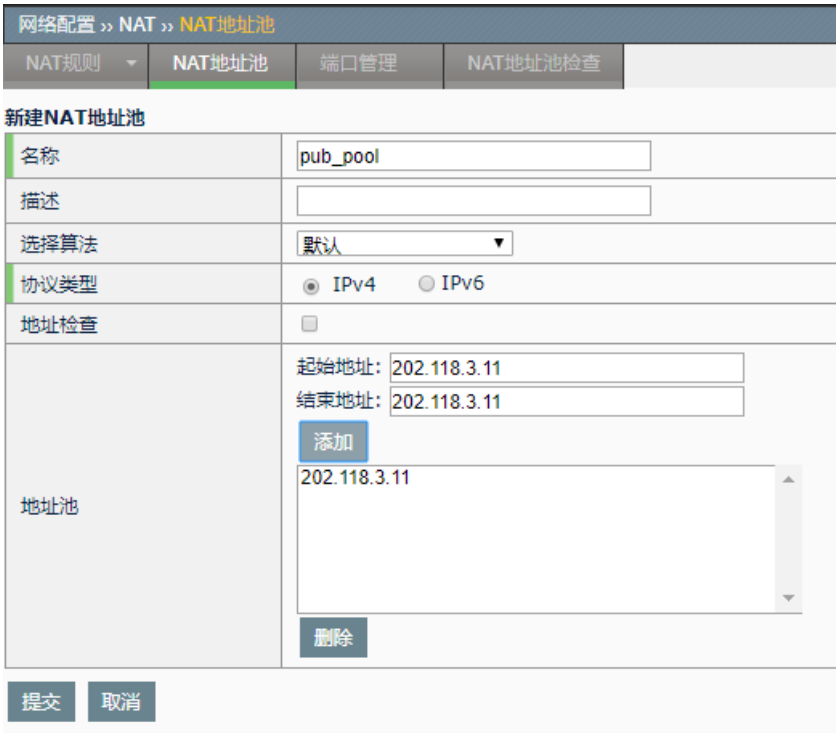



**配置步骤：**

1. 进入**模板和对象->对象管理->地址对象**，创建 IPv4 类型的地址对象“inside-net”。

| 名称 | 成员 | 引用 | 描述 | |
|---|---|---|---|---|
| any | 0.0.0.0/0 | 5 | | |
| Intranet | 10.1.1.0/24 | 0 | | |
| Extranet | 192.168.11.0/24 | 0 | | |
| inside-net | 192.168.0.0/24 | 0 | | |

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




点击**提交**。

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

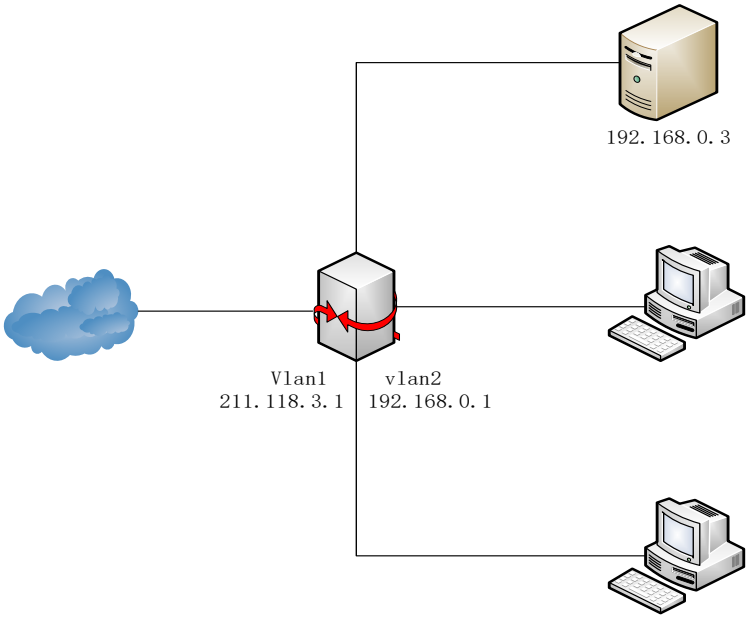

4．点击**提交**。

## 51.4.2 配置静态地址转换

**案例描述：**

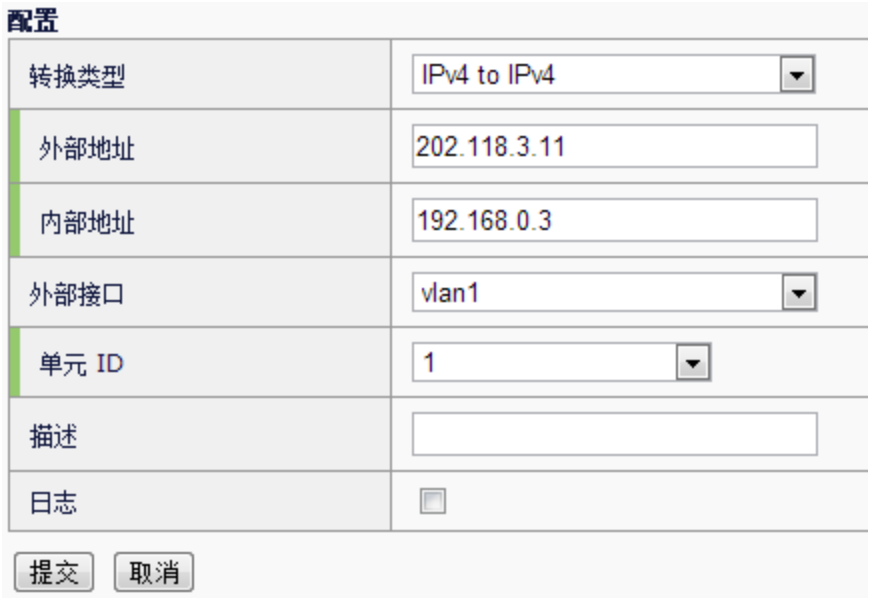
内网有一台服务器对外提供服务，服务器的内网地址为 192.168.0.3，映射的公网地址为 202.118.3.1。

**案例组网图：**




**配置步骤：**

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




2. 点击**提交**，显示如下界面。

## 51.5 NAT监控与维护

### 51.5.1 查看地址池和NAT规则

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

## 51.6 常见故障分析

### 51.6.1 连接时通时断

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

# 52 第52章 跨协议转换

## 52.1 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。

目前应用交付设备实现了 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。

## 52.2 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。

### 52.2.1 配置IVI转换方式

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

IVI 转换方式支持 NAT46 和 NAT64。

**配置步骤：**

1. 进入**网络配置>NAT>NAT 规则：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。

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

**描述：**添加对该规则的描述，最多可为 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**。

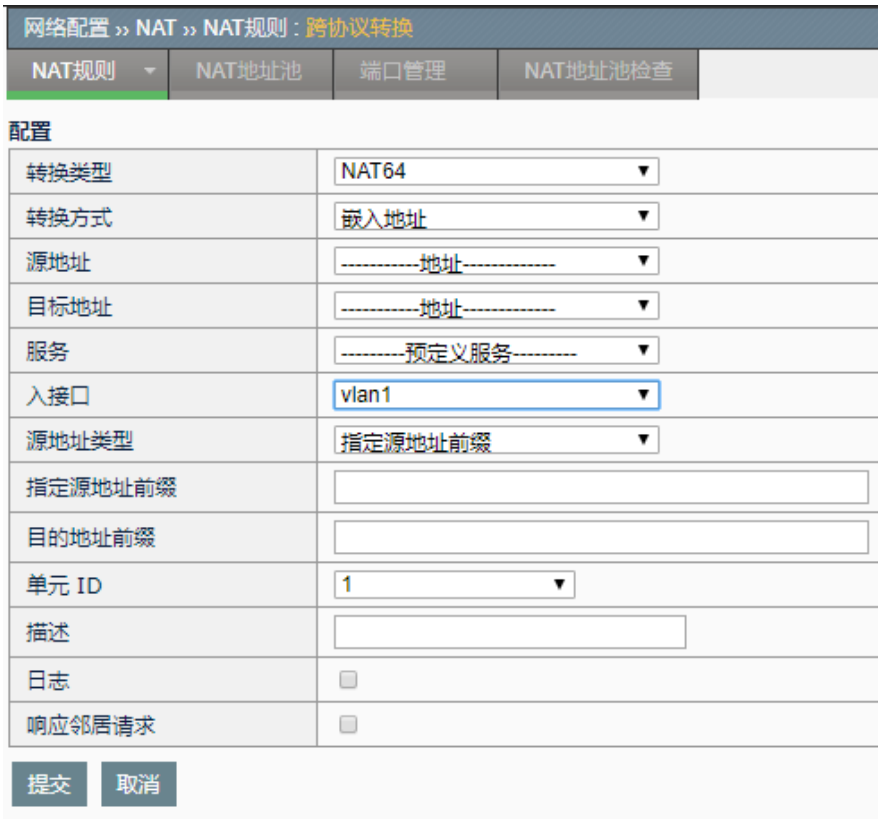
### 52.2.2 配置嵌入地址转换方式

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**网络配置>NAT>NAT 规则：跨协议转换**，点击**新建**，**转换类型**选择

**“NAT64”，转换方式**选择**“嵌入地址”。**




**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）。

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

**描述：**添加对该规则的描述，最多可为 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)。

注意

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。

### 52.2.3 配置地址池转换方式

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

**配置步骤：**

进入**网络配置>NAT>NAT 规则：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。

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

**描述：**添加对该规则的描述，最多可为 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

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。

### 52.2.4 编辑跨协议转换规则

已经创建的跨协议转换规则可以进行编辑修改。

**编辑步骤：**

1.进入**网络配置>NAT>跨协议转换。**


2.点击规则编号。


3.对原有的规则进行编辑，其中**转换类型**不允许修改。

4.点击**更新。**

### 52.2.5 删除跨协议转换规则

**删除步骤：**

1. 进入**网络配置>NAT>跨协议转换。**

| # | 所有 | 源地址 | 目的地址 | 服务 | 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 | any | any | dhcp | vlan3 | | | IVI | 禁用 | | |
| 2 | NAT64 | test | test_2 | any | vlan3 | pool_1 | | 嵌入地址 | 禁用 | | |
| 1 | NAT46 | abc | def | bootpc | vlan3 | 出接口地址 | pool_2 | 地址池 | 禁用 | | |

2. 点击规则编号后对应的  ，删除该条跨协议转换规则。

### 52.2.6 移动跨协议转换规则

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

**配置步骤：**

1. 进入**网络配置>NAT>跨协议转换。**

| # | 所有 | 源地址 | 目的地址 | 服务 | 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 | any | any | dhcp | vlan3 | | | IVI | 禁用 | | |
| 2 | NAT64 | test | test_2 | any | vlan3 | pool_1 | | 嵌入地址 | 禁用 | | |
| 1 | NAT46 | abc | def | bootpc | vlan3 | 出接口地址 | pool_2 | 地址池 | 禁用 | | |

2. 点击要移动的规则编号后对应的  ，可移动该规则。

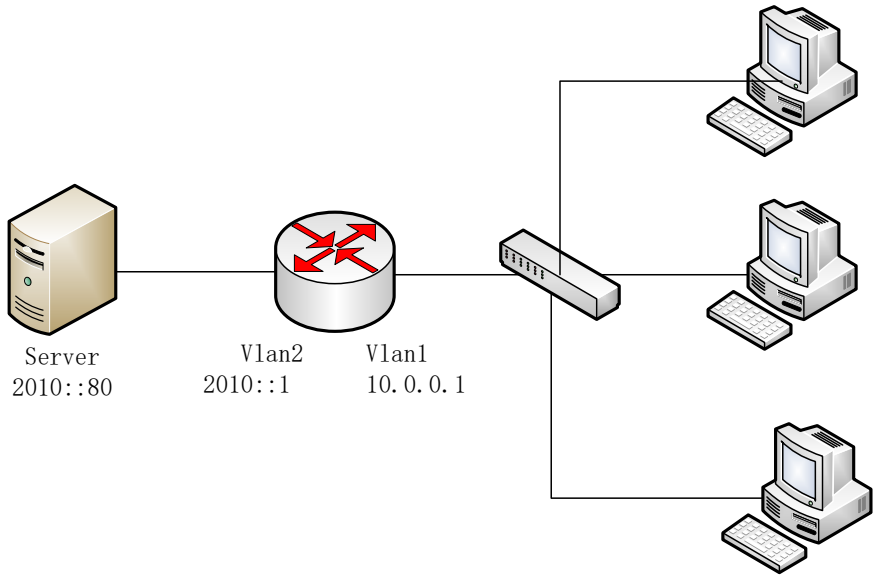
## 52.3 配置案例

### 52.3.1 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。应用交付设备作为核心路由，串行接入网络。

**NAT46 配置案例组网图：**




**配置步骤：**

1. 进入**模板和对象->对象管理->地址对象，**创建 IPv4 类型的地址对象“inside-net”。
2. 进入**模板和对象->对象管理->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 |
|---|---|---|
| any | 0.0.0.0/0,::/0 | 1 |
| inside-net | 10.0.0.0/24 | 0 |
| inside-ftp | 10.0.0.100 | 0 |

3. 进入**网络配置->NAT->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 |
|---|---|---|---|
| ftp-server | | | 默认 |
| | 2010::80 | 2010::80 | |

4. 进入**网络配置->NAT->跨协议转换，**创建 NAT46 规则。


注意

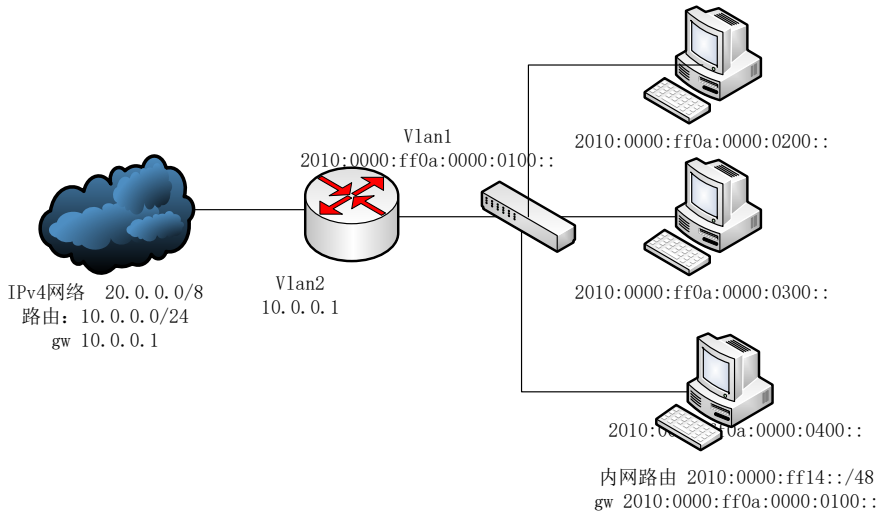
这种环境下，设备会代理 IPv6 服务器的业务，所以配置时要勾选响应 ARP，以保证 IPv4 内网向代理服务器地址 10.0.0.100 发出的请求能被发送至设备上。

### 52.3.2 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。应用交付设备作为核心路由，串行接入设备。

**配置案例组网图：**




**配置步骤：**

1. 进入**模板和对象->对象管理->地址对象**，创建 IPv6 类型的地址对象“ivi-addr”和“dest-addr”。

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

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

**配置**

| | |
|---|---|
| 转换类型 | NAT64 |
| 转换方式 | IVI |
| 源地址 | ivi-addr |
| 目标地址 | dest-addr |
| 服务 | any |
| 入接口 | vlan1 |
| 源地址类型 | 指定源地址前缀 |
| 指定源地址前缀 | 2010::/32 |
| 指定目的地址前缀 | 2010::/32 |
| 单元 ID | 1 |
| 描述 | |
| 日志 | |
| 响应邻居请求 | |

提交 取消


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

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

## 52.4 常见故障分析

### 52.4.1 用户发现网络中一直有地址冲突的情形

| | |
|---|---|
| 故障现象 | 用户发现PC一直有地址冲突的情形。 |
| 分析与解决 | 可查看NAT64/NAT46规则是否开启响应邻居/ARP请求，如果开启了，设备会响应入接口收到的匹配的目的地址的邻居/ARP请求。如果用户配置的匹配目的地址为”any”，建议不要轻易开启响应邻居/ARP请求。 |

### 52.4.2 用户发送的请求报文无法到达设备

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

### 52.4.3 地址转换失败

| | |
|---|---|
| 故障现象 | 用户在设备出口抓包发现，地址没有进行任何转换 |
| 分析与解决 | 如果是NAT64转换，可查看配置：<br>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<br>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<br>3. 嵌入地址转换方式，如果配置的匹配规则的目的地址对象，与配置的目的地址前缀有冲突，则不会进行任何转换 |

如果转换后的目的地址路由失败，那么报文也不会进行转换。

# 53 第53章 端口管理

## 53.1 端口管理概述

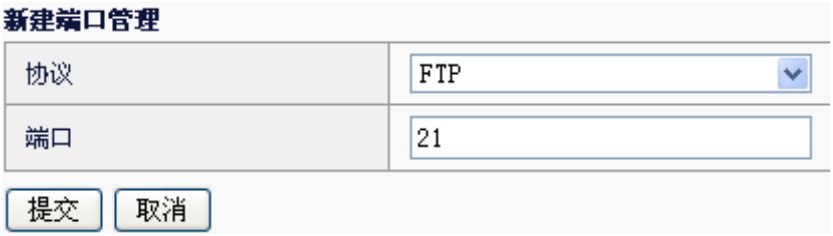
针对服务器有时会改变或者添加所提供服务对应的监听端口号的情况，设备需要改变或添加预置的 ALG 端口号，使设备能正确识别报文中端口号所对应的服务类型。

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

## 53.2 端口配置

### 53.2.1 设置ALG端口号

进入**网络配置>NAT>端口管理**，点击“新建”按钮。如下图：



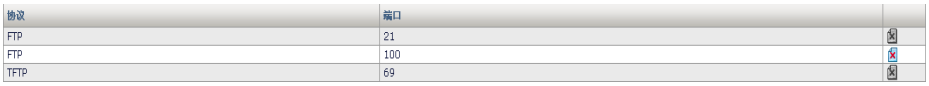

**协议**：ALG 协议类型，目前仅支持 FTP 和 TFTP。

**端口**：要添加的 ALG 协议的监听端口号。

注意 每个协议，除了默认端口，最多可以添加 7 个端口号。

### 53.2.2 删除ALG端口号

进入**网络配置>NAT>端口管理.**

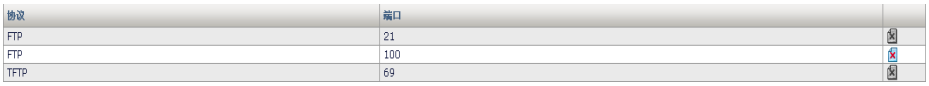


点击最后一列的图标，即可删除配置的端口号。

注意 协议对应的默认端口号无法改变或删除。

### 53.2.3 查看ALG端口号

进入**网络配置>NAT>端口管理**，可查看到配置的所有端口号。




## 53.3 配置案例

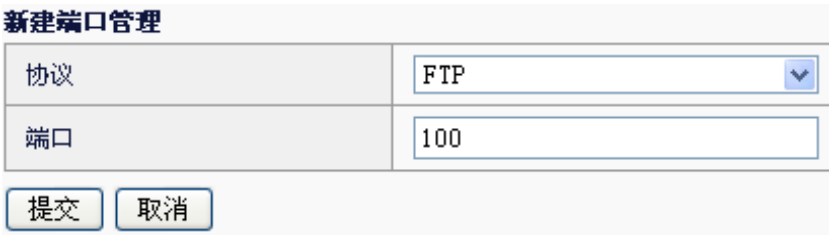
**配置案例 1**

**案例描述：**

添加一个 FTP 协议的监听端口号 100。

**配置步骤：**

**网络配置>NAT>端口管理**，点击“新建”按钮。如下图：




点击“**提交**”提交配置。

注意 不同的协议添加的 ALG 端口可以相同。

# 54 第54章 IPsec VPN

## 54.1 概述

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

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

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

**相关术语解释：**

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

## 54.2 IPSec VPN配置过程

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

配置 IPsec VPN 基本过程如下：

1. 配置 IKE 协商策略，主要配置对端地址，认证方式，协商参数等。

2. 配置 IPSEC 协商策略，主要配置 IPsec 加密算法，封装模式等。

3. 配置安全策略，通过配置 IPsec 类型的安全策略来指定需要加密数据的网络范围。

### 54.2.1 配置IKE协商策略

**配置步骤：**

进入**网络配置>IPsec VPN>IPSec VPN**，点击 新建


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

### 54.2.2 配置IPSEC协商策略

**配置步骤：**

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



2. 配置 IPSEC 协商的**通道名称**

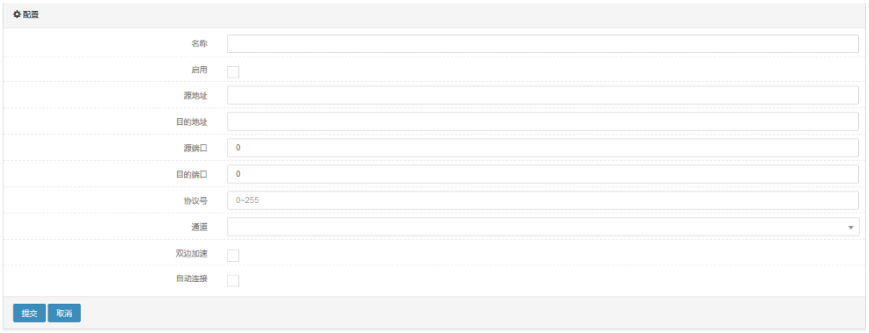
3. 配置 **IPSEC 协商的交互方案**。可以选择 ESP 封装算法，或 AH 的封装算法，和 IPSec 对端要保持一致。另外 Nat 穿越的情况下，不要使用 AH

封装。

4. 配置**工作模式**。网络到网络的 IPSec 传输使用隧道模式。L2tp 远程接入使用传输模式。与 IPSec 对端需要保持一致。

### 54.2.3 配置IPSEC策略

进入**网络配置>IPsec-VPN>IPsec 策略**，点击**新建**




1. 配置**源地址、源端口，目的地址、目的端口，协议号**。源地址是要保护的本地私网。目的地址是要保护的对端私网。

2. 通道选择上一节 IPSEC 协商策略配置的 IPSec 协商通道。

## 54.3 IPSec VPN配置参数

### 54.3.1 IKE协商参数

IKE 策略定义了 IKE 协商的一组参数。两端 VPN 设备通过 IKE 协议协商相同的策略建立 isakmp SA。

**配置步骤：**

1. 进入**网络配置>IPsec-VPN>IPsec**，点击 


**网关名称**：IKE 协商的名称。

**本地 IP 地址**：本地用来接受或发起协商的地址。

**远程网关**：

静态 ip 地址：由用户输入 ip 地址。

动态地址

**模式**：IKE 协商的协商模式是野蛮模式还是主模式。

**认证方式**：在协商过程中所采用的认证方法，可选预共享密钥或证书。

**预共享密钥**：当采用预共享密钥的认证方法时要输入的密钥值。

**本地证书**：当采用证书认证方法时要选择的本地证书。

**IKE 协商的交互方案**：在协商过程中所采用加密算法和验证算法。

**DH 组**：在协商过程中做 DH 交换时采用的 group 值。

**密钥周期**：阶段 1 的 SA 的生存时间。

**NAT 穿越保持连接的频率**：设置 NAT 穿越的保活时间。

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

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

**对等体状态检测**：是否启用 DPD 功能。

**DPD 穿越保持连接的频率**：设置对等体检测时间。

**配置步骤**：

1. 输入网关名称
2. 输入本地 IP 地址
3. 选择远程网关的类型

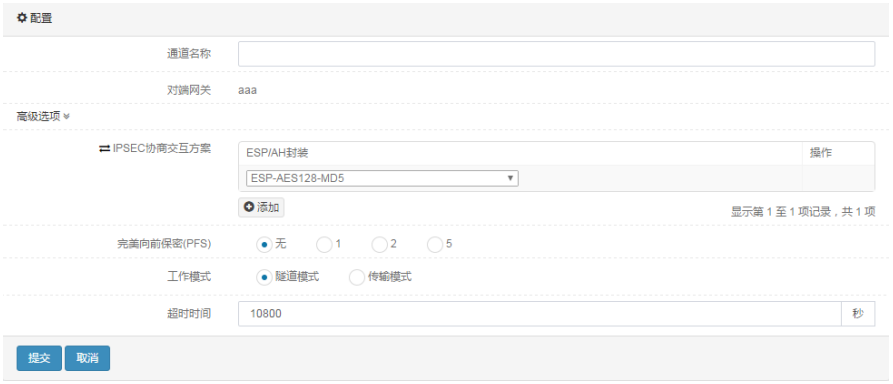
4. 配置远程网关的 IP 地址
5. 选择 IKE 协商模式
6. 输入预共享密钥值
7. 选择 IKE 协商的加密认证算法
8. 选择 DH 交换的 group 值
9. 输入 SA 的生存时间值
8. 输入 NAT 穿越的连接频率
9. 输入本地身份的 IP 地址
10. 选择是否启用状态检测以及输入连接频率
11. 点击**提交。**

### 54.3.2 IPSEC协商参数

两端 VPN 设备通过 IKE 协议协商后，这些参数用于建立 ipsec SA。

**配置步骤：**

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




**通道名称：**IPSEC 协商的名称

**对端网关：**IKE 协商的网关名称

**IPSEC 协商的交互方案：**协商 IPSEC 的封装方式以及算法

**完美向前保密（PFS）：**是否需要在 IPSEC 协商过程中采用 DH 交换

**工作模式：**协商 IPSEC 封装时工作方式

**超时时间：**可以以秒数或者字节数决定 IPSEC SA 的生存时间

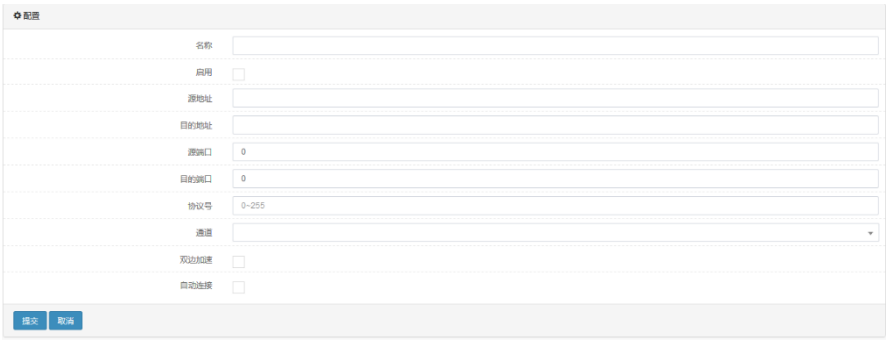
1. 输入通道名称
2. 选择 IPSEC SA 的封装方式以及算法
3. 选择是否使用 PFS 功能

4. 选择 IPSEC SA 的工作模式
5. 设置 IPSEC SA 的超时时间
6. 点击**提交。**

### 54.3.3 IPSEC策略

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

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




**名称：**IPSEC 策略的名称

**启用：**是否启用当前策略

**源地址：**需要保护的本地子网的地址

**目的地址：**需要保护的对端子网的地址

**源端口：**需要保护的本地发出流量的源端口

**目的端口：**需要保护的本地发出流量的目的端口

**协议号：**需要保护的本地发出流量的目的协议号

**通道：**保护当前流量的阶段二

**双边加速：**是否开启双边加速功能

**自动连接：**启用后立即主动发起连接

1. 配置名称
2. 启用
3. 配置源地址、目的地址、源端口、目的端口、协议号
4. 选择阶段二隧道
5. 点击**提交。**

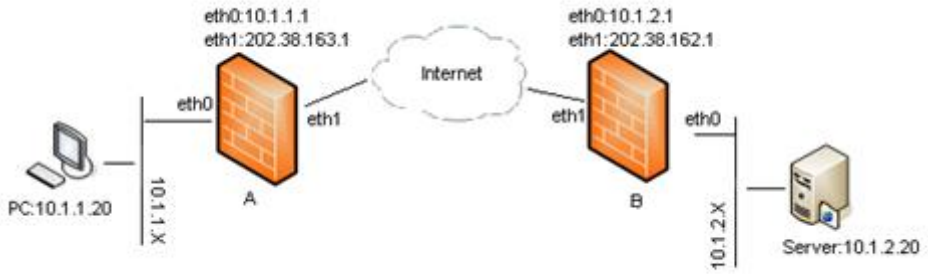
## 54.4 配置案例

### 54.4.1 配置案例1：配置IPSEC基本组网

**案例描述**

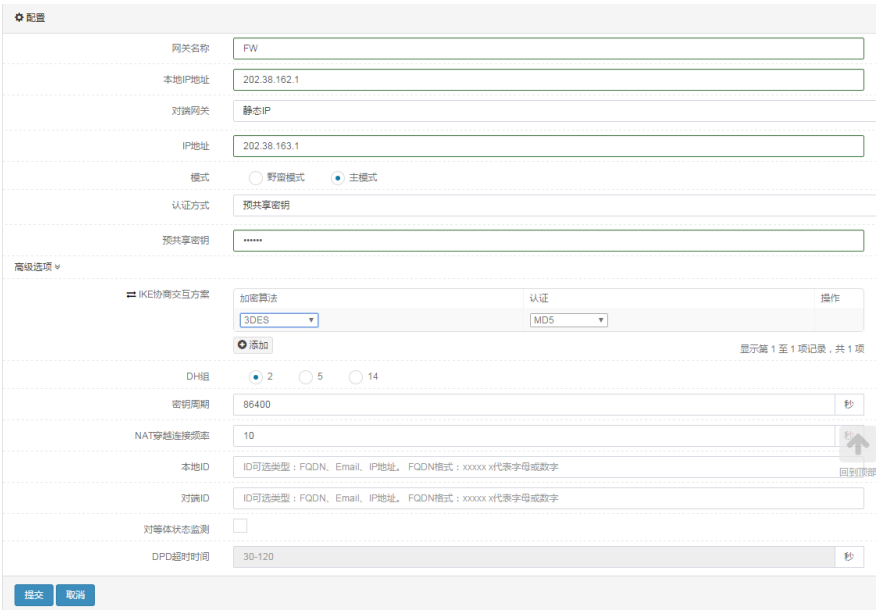
假定网络环境如下图所示，PC 机到 Server 的流量需要经过各自的 FW 设备后在 Internet 上传输，为了保证流量在 Internet 传输过程中的安全性，有必要在 FW_ A 和 FW_B 之间建立 IPSec 的 VPN 隧道以保障通信安全。

**图54-1** 案例组网图



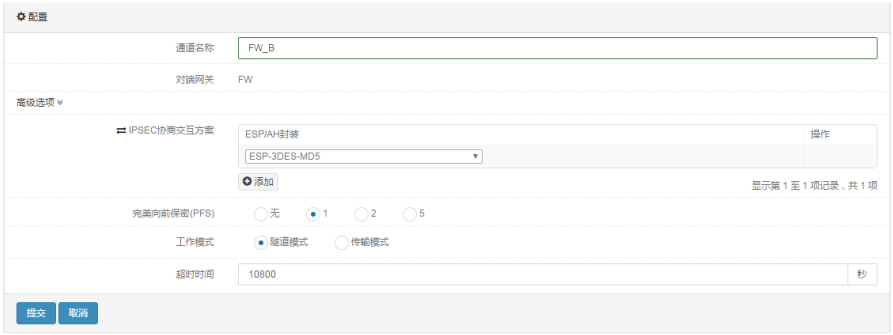

**FW_B 配置步骤：**

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



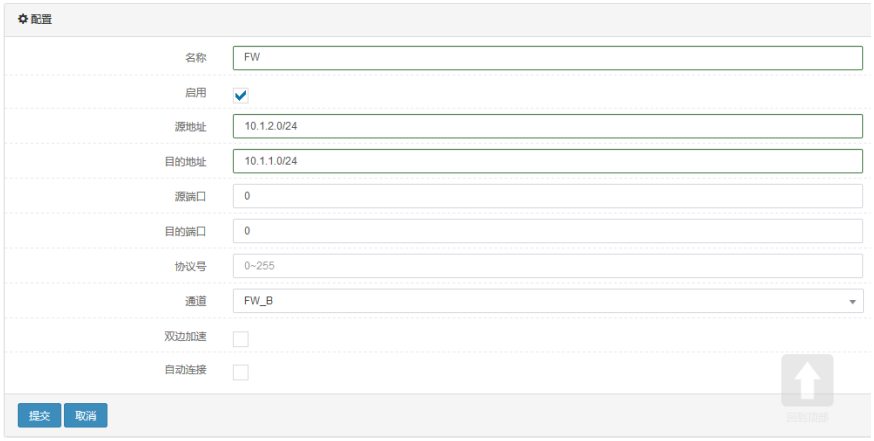

2. 点击**提交**完成设置。

3. 进入**网络配置>IPsec-VPN>IPsec**，点击 **新建 IPSEC 协商**，如下图：




4. 点击**提交**完成设置。

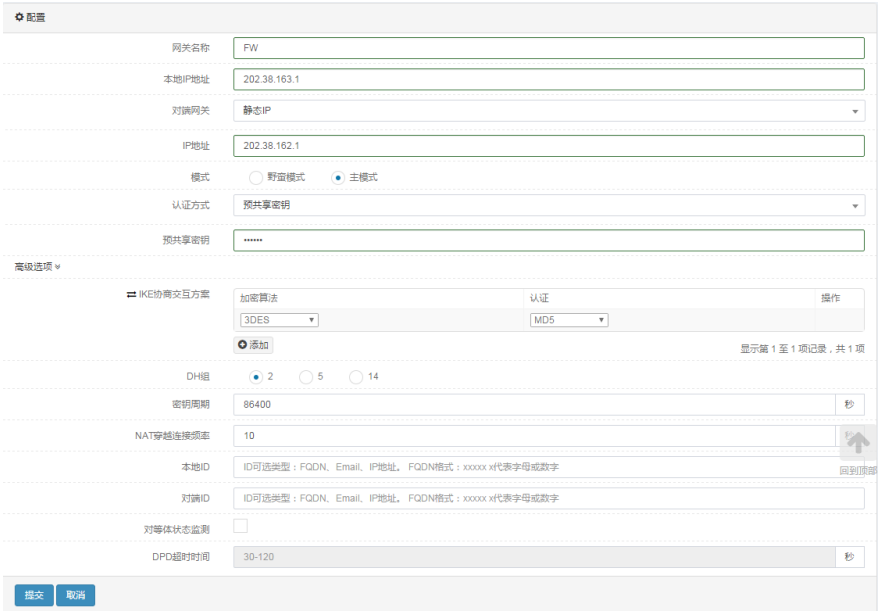
5. 进入**网络配置>IPsec-VPN>IPsec 策略**，建立 IPsec 策略，如下图：




6. 点击**提交**完成设置。

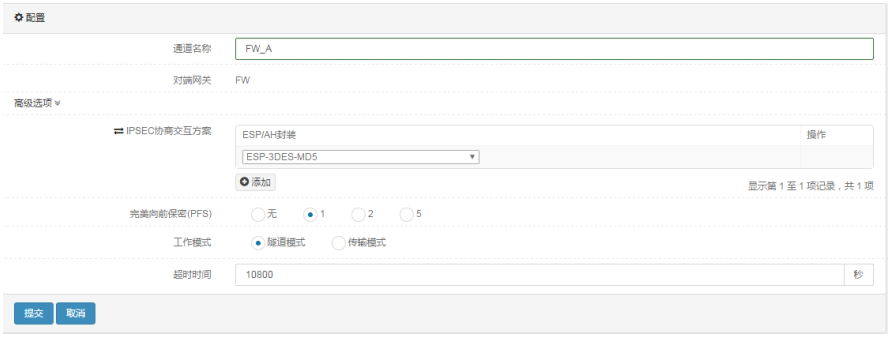
**FW_A 配置步骤：**

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



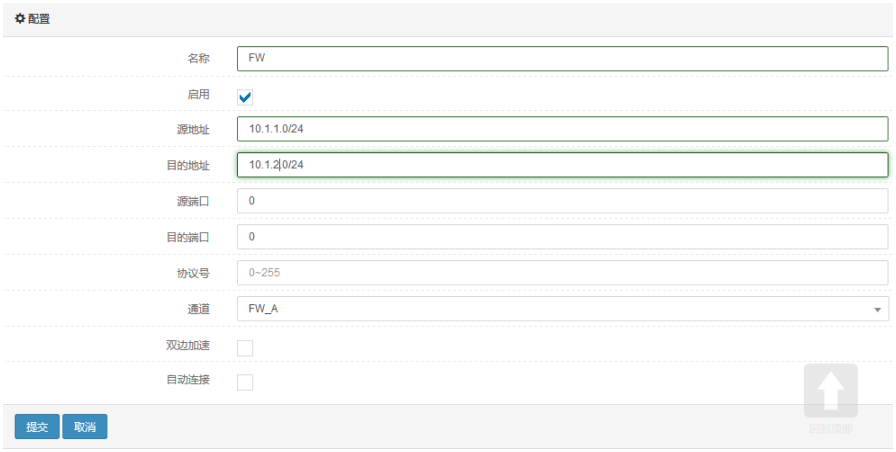

2. 点击**提交**完成设置。

3. 进入进入**网络配置>IPsec-VPN>IPsec**，点击 **新建 IPSEC 协商**，如下图：




4. 点击**提交**完成设置。

5. 进入**网络配置>IPsec-VPN>IPsec 策略**，建立 IPsec 策略，如下图：



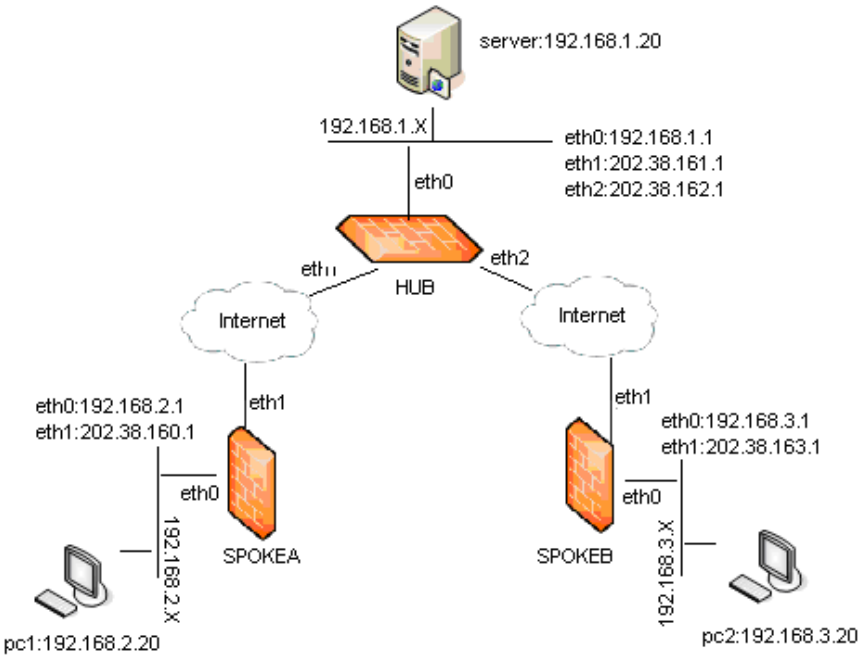

6. 点击**提交**完成设置。

## 54.4.2 配置案例2：配置IPSEC HUB_SPOKE

**案例描述**

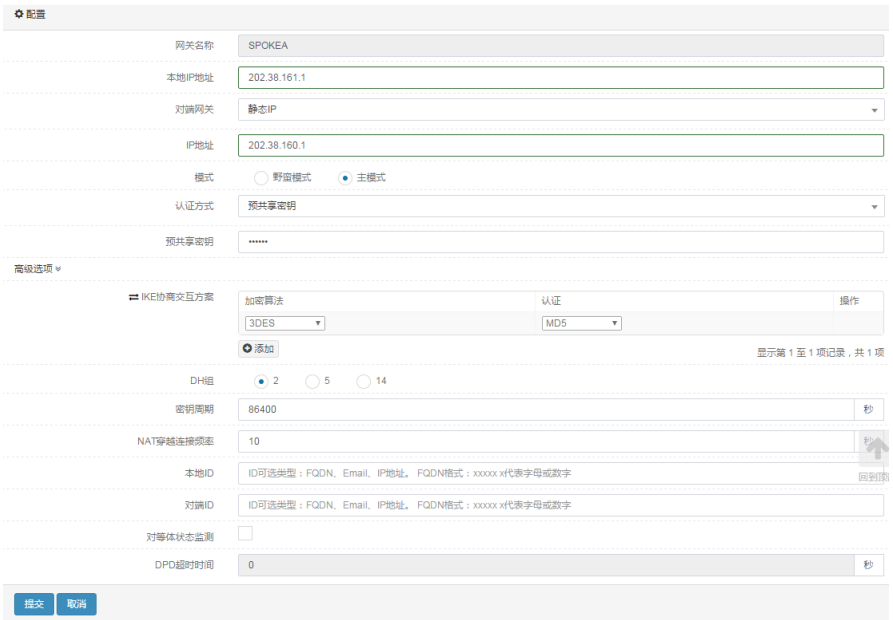
假定网络环境如下图所示， SPOKEA 想要访问 SPOKEB，但是他们之间没有网络连接。必须通过 HUB 进行转发。

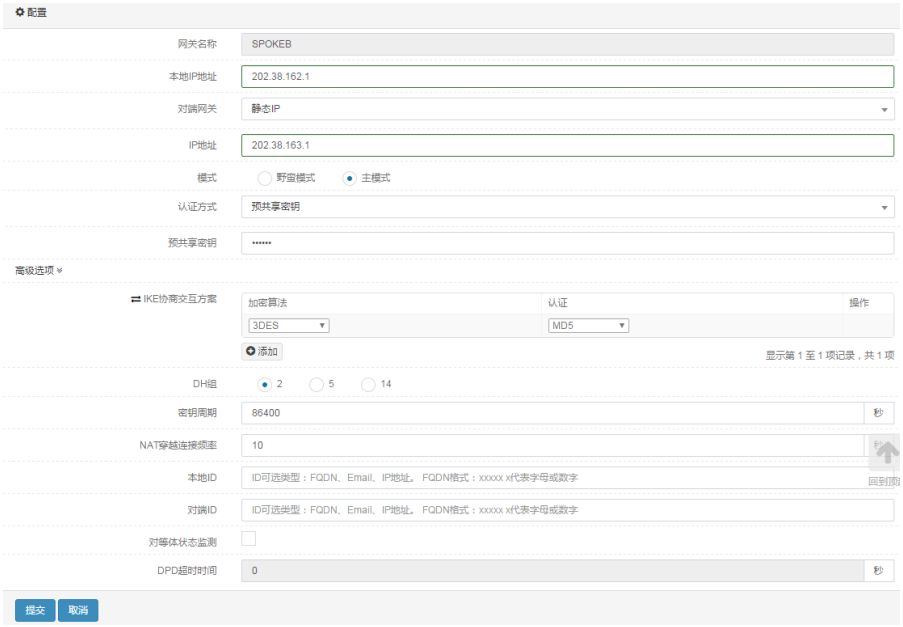
**图54-2** 案例组网图




**HUB 配置步骤：**

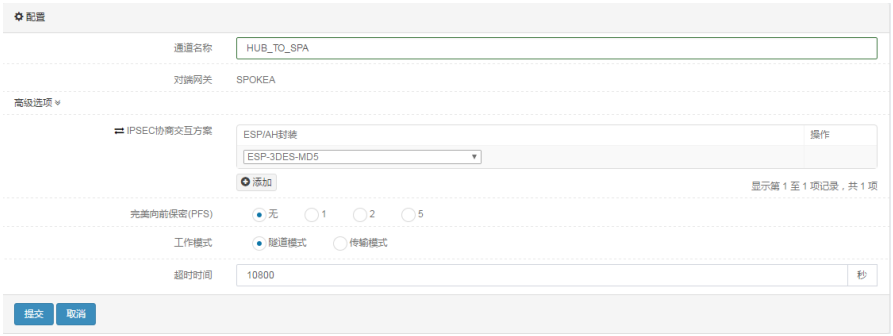
1. 进入**网络配置>IPsec-VPN>IPsec**，点击**新建**，如下图：

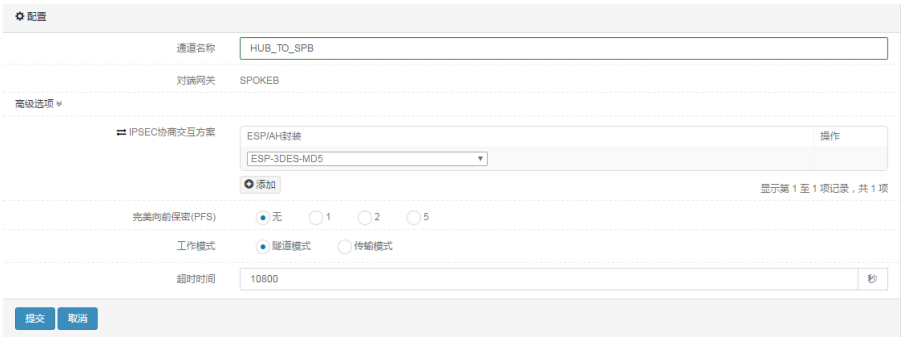





2. 分别点击**提交**完成配置。

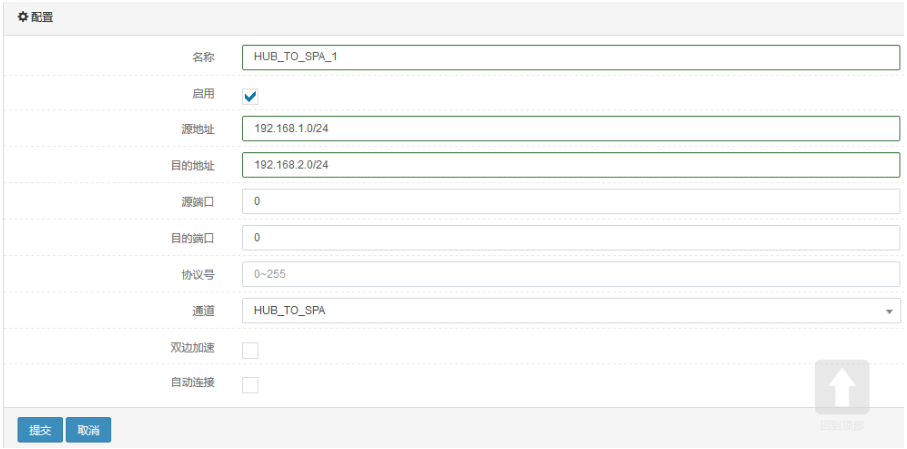
3. 进入进入**网络配置>IPsec-VPN>IPsec**，点击 新建 IPSEC 协商，如下图：

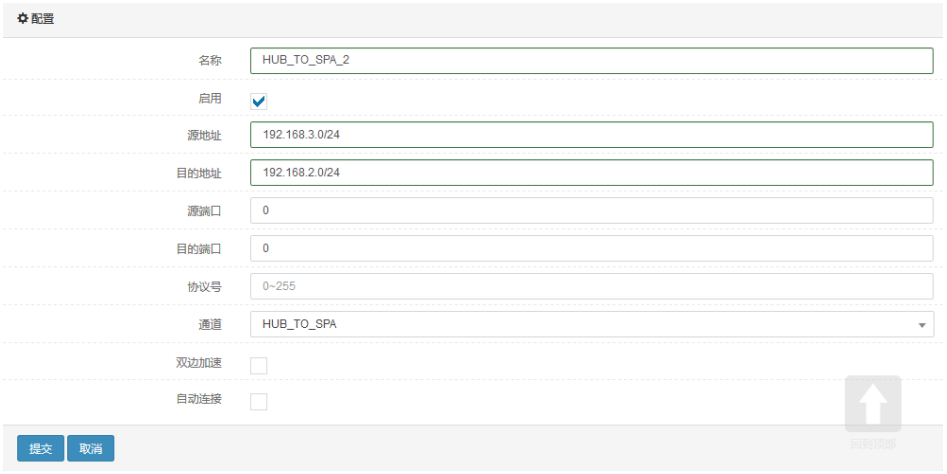


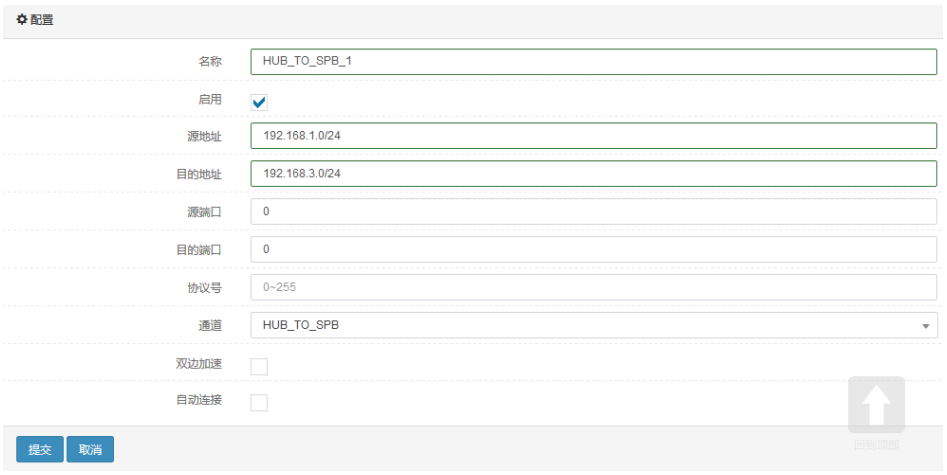



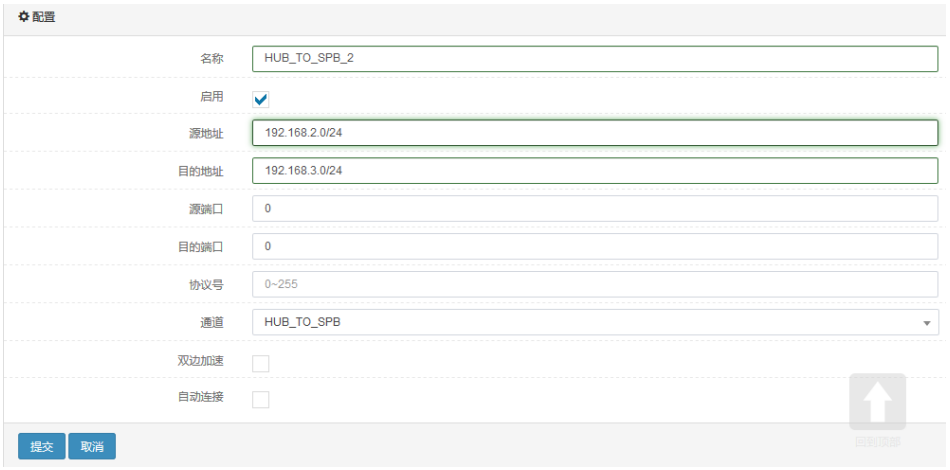

4. 分别点击**提交**完成配置。

5. 进入**网络配置>IPsec-VPN>IPsec 策略**，建立 IPsec 策略，如下图：


配置
名称
HUB_TO_SPA_1
启用
源地址
192.168.1.0/24
目的地址
192.168.2.0/24
源端口
0
目的端口
0
协议号
0~255
通道
HUB_TO_SPA
双边加速
自动连接
提交
取消


配置
名称
HUB_TO_SPA_2
启用
源地址
192.168.3.0/24
目的地址
192.168.2.0/24
源端口
0
目的端口
0
协议号
0~255
通道
HUB_TO_SPA
双边加速
自动连接
提交
取消

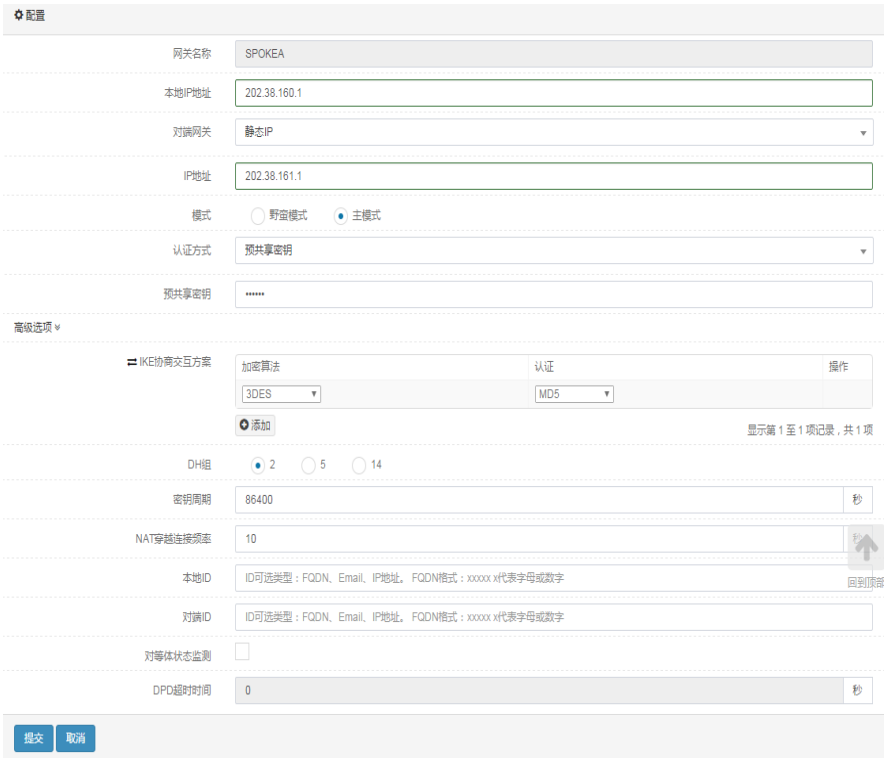

配置
名称
HUB_TO_SPB_1
启用
源地址
192.168.1.0/24
目的地址
192.168.3.0/24
源端口
0
目的端口
0
协议号
0~255
通道
HUB_TO_SPB
双边加速
自动连接
提交
取消




6. 分别点击**提交**完成配置。

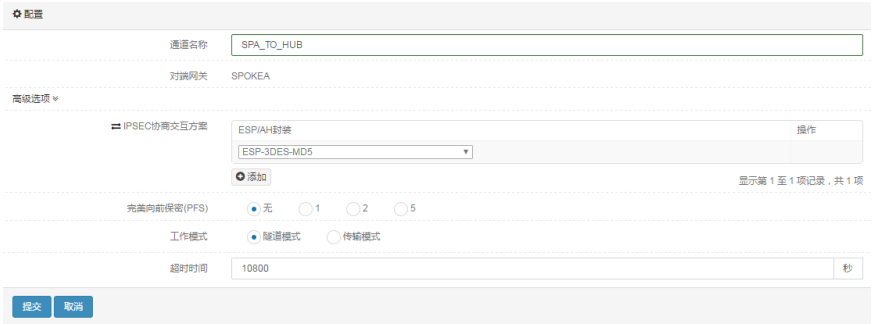
**SPOKEA 配置步骤：**

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



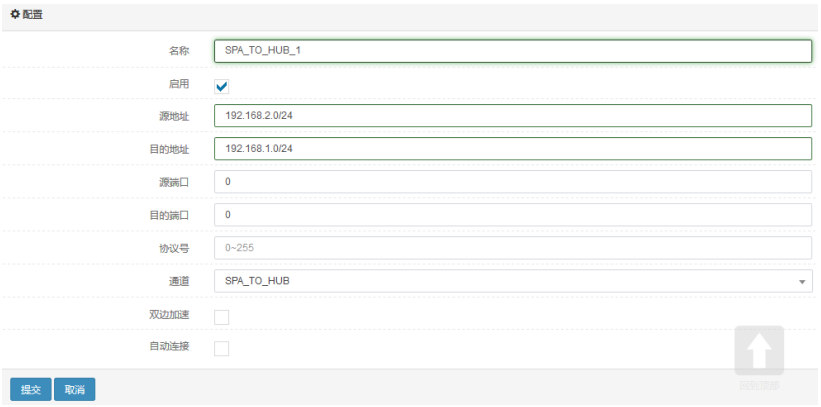

2. 点击**提交**完成配置。

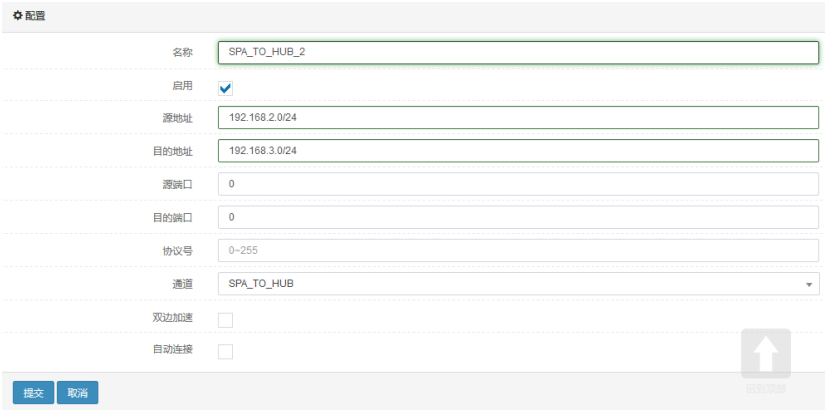
3. 进入进入网络配置>IPsec-VPN>IPsec，点击 新建 IPSEC 协商，如下图：




4. 点击**提交**完成配置。

5. 进入**网络配置>IPsec-VPN>IPsec 策略**，建立 IPsec 策略，如下图：

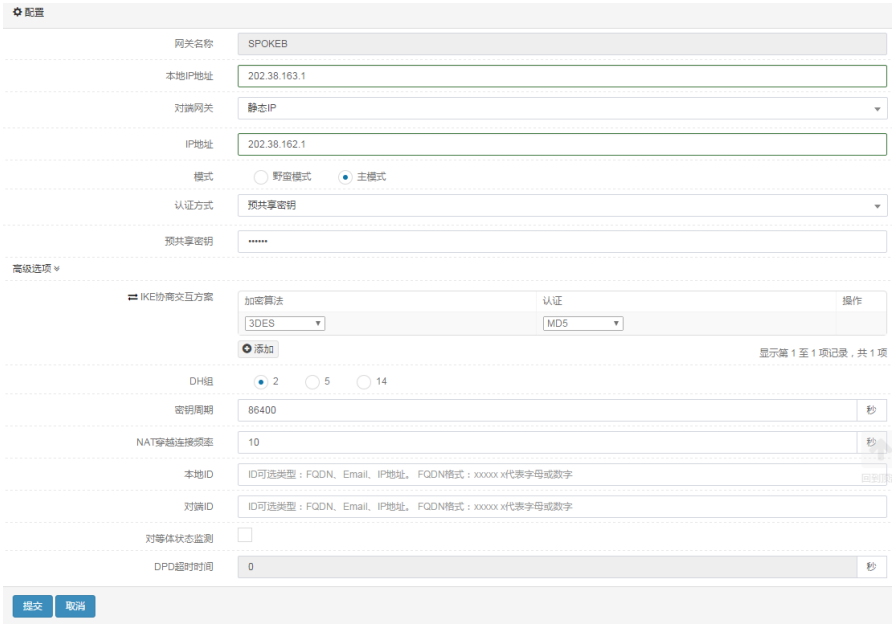



6. 分别点击**提交**完成设置。

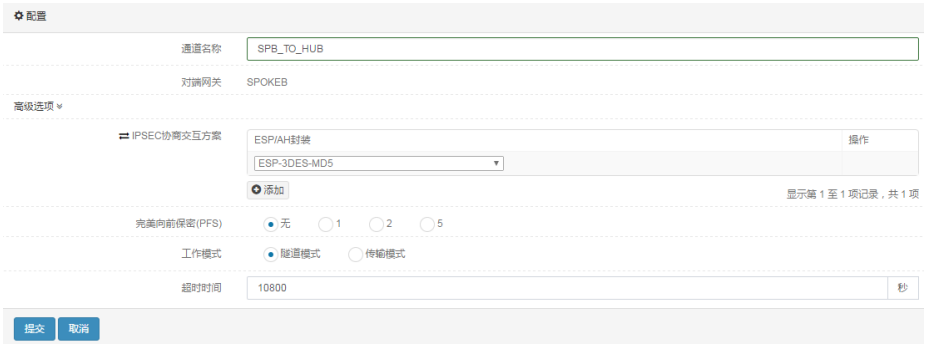
**SPOKEB 配置步骤：**

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



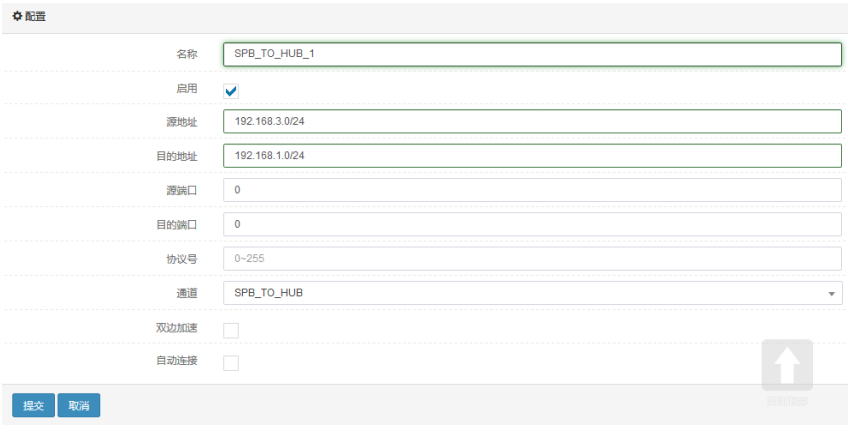

2. 点击**提交**完成配置。

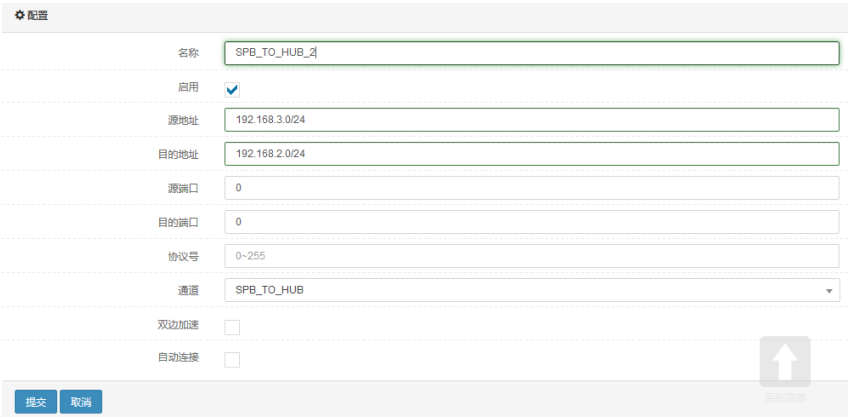
3. 进入进入网络配置>IPsec-VPN>IPsec，点击 新建 IPSEC 协商，如下图：




4. 点击**提交**完成配置。

5. 进入**网络配置>IPsec-VPN>IPsec 策略**，建立 IPsec 策略，如下图：




6. 分别点击**提交**完成设置。

## 54.5 IPSEC VPN监控与维护

### 54.5.1 查看SA是否建立

点击**网络配置>IPsec-VPN>>监视器**，如下图：





### 54.5.2 删除建立的SA

点击 删除两个协商的 SA。

点击 查看 IPSEC 阶段 SA 的详细信息。

## 54.6 常见故障分析

### 54.6.1 故障现象：不能建立隧道

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

# 55 第55章 SSL 远程接入

## 55.1 技术简介

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

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

天清 ADC 应用交付平台的 SSL VPN 分为两种工作模式：

- Web 模式。也叫做代理 Web 页面。它将来自远端浏览器的页面请求（采用 HTTPS 协议）转发给 Web 服务器，然后将服务器的响应回传给终端用户。支持 WEB 服务，FTP 服务，文件共享服务以及 OWA。
- Tunnel 模式。需要下载、运行客户端支持。客户端和天清 ADC 应用交付平台建立 SSL 隧道后，天清 ADC 应用交付平台为客户端分配 IP，客户端通过建立的虚接口直接通过 SSL 隧道连接到内部网络。该种方式可支持各种应用。

## 55.2 配置SSL VPN

SSL VPN 模块的配置主要包括以下几部分内容：

- 配置 SSL VPN 基本功能
- 配置 SSL VPN Web 访问配置
- 配置 SSL VPN 用户和用户组
- 配置 SSL VPN 资源和资源组
- 查看监视器

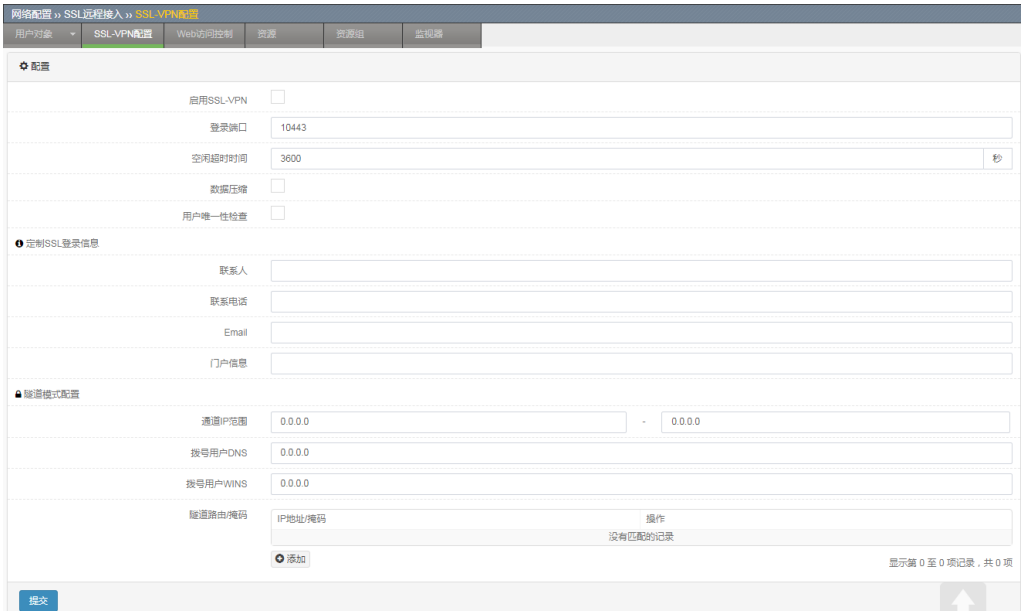
### 55.2.1 配置SSL VPN基本功能

#### 1. 基本配置

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

首先单击左侧功能栏网络配置→SSL 远程接入→SSL-VPN 配置，如下图：


点击进入 SSL VPN 基本功能配置页面，如下图：




- **启用 SSL VPN**：用以启用/关闭 SSL VPN 服务功能。
- **登录端口**：用于设置 SSL VPN 的服务端口，是客户端登录 SSL VPN 页面时

采用的端口号，客户端通过此端口和天清 ADC 应用交付平台建立 SSL VPN 连接。默认端口为 10443。用户登录地址可表述为：“https://开启 SSL VPN 服务的端口 IP 地址:登录端口号”。

- **空闲超时时间：**设置一段时间（秒）来控制用户超时。如果用户在登录 SSL VPN 后，在设定的时间内，没有使用 SSL VPN 传输数据，用户将自动退出。如果用户需要再次使用 SSL VPN，需要重新登录。
- **数据压缩：**是否启用数据压缩。
- **用户唯一性检查：**如果选定，检查是否存在已登录的同名用户，同名禁止登录。
- **定制 SSL 登录信息：**SSL-VPN 添加 SSL 客户端页面信息定制功能，使管理员可以根据团队的需要，来定制 SSL 客户端页面。包括以下配置：
- **联系人：**联系人的信息
- **联系电话：**联系人的电话
- **Email：**联系人的 Email。
- **门户信息：**用户自定义的 SSLVPN 门户信息。用户配置门户信息将显示在用户登录后的 SSLVPN PORTAL 页面上。
- **隧道模式配置**在用户使用 SSLVPN 隧道模式时才会生效。包括以下配置：
- 通道 IP 范围：指客户端通过隧道方式连接后分配到的 IP 地址范围。指定为 SSL VPN 隧道模式客户端分配的 IP 地址范围，输入 IP 地址范围的起始和结束地址即可。
- **拨号用户 DNS：**指定客户端通过隧道方式连接后使用的域名服务器，如果访问的资源均通过 IP 地址直接访问则可不填。
- **拨号用户 WINS：**指定客户端使用的 WINS 服务器。
- **隧道路由/掩码：**配置隧道模式用户可以访问的私有网络，指客户端通过隧道方式连接后，在客户端 PC 上设定的访问路由，可配置多条。

**2. 注意事项**

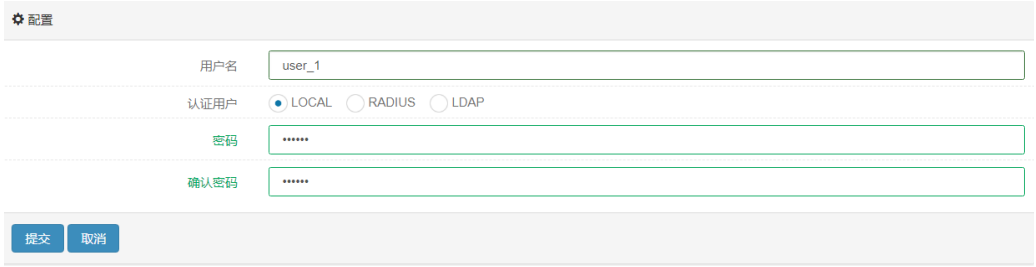
➢ 在配置登录端口时，不能与天清 ADC 应用交付平台其他服务所占用的端口冲突。

### 55.2.2 配置SSL VPN用户和用户组

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

**1. 配置用户**

配置用户账户：网络配置→SSL 远程接入→用户对象→用户，点击“新建”。如下图：




配置过程：

1. 输入远程用户的用户名（如 user_1）；

2. 选中启用；

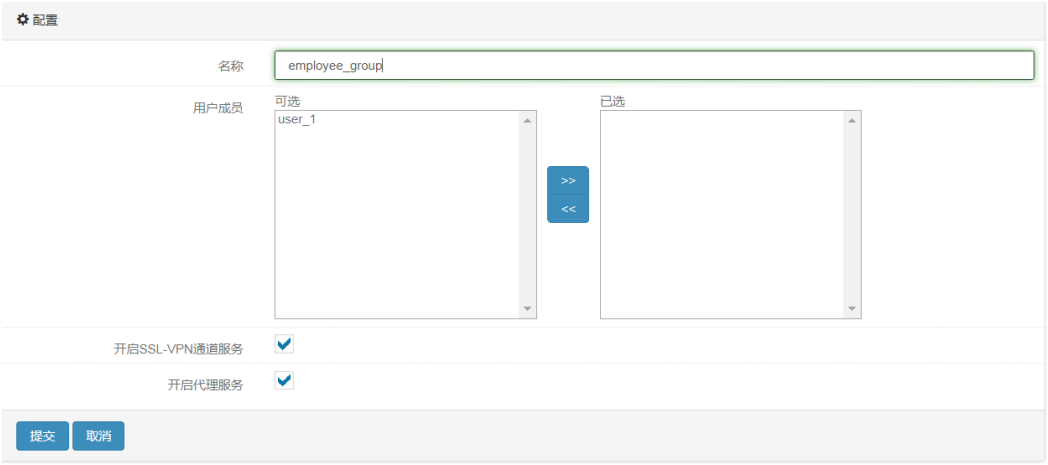
3. 如果使用本地密码验证，勾选 LOCAL，并输入密码和确认密码；如果使用 RADIUS 认证，勾选 RADIUS，并选择指定的 RADIUS 服务器；如果使用 LDAP 认证，勾选 LDAP，并选择指定的 LDAP 服务器；

4. 提交；

5. 重复以上过程，可以添加多个远程用户。

**2．配置用户组**

配置 SSL VPN 用户组：进入网络配置→SSL 远程接入→用户对象→用户组，点击“新建”。如下图：




配置过程：

1) 输入用户组名（如 employee_group）；
2) 要向该用户组中加入用户。从“可选”列表中选择用户，然后单击右箭头或双击用户名称，将该用户添加到组员列表中；
3) 选择开启 SSL VPN 通道服务，使该组用户可以使用 SSL VPN 隧道模式（可选）；
4) 选择开启代理服务，使该组用户可以使用 Web 代理模式（可选）；
5) 提交。

### 55.2.3 配置SSL VPN Web访问配置

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

#### 1. 配置 Web 访问配置

配置 SSLVPN Web 访问，进入**网络配置>SSL 远程接入>Web 访问控制配置**。如下图：


1. 配置需要过滤的 HTTP 方法：从 HTTP 方法列表中选择要过滤的方法，然后单击右箭头添加方法名到要过滤列表中。如要取消过滤只需从右侧已过滤

HTTP 方法列表中选择要取消过滤的方法，然后单击左箭头添加方法名到要未过滤列表中。

2. 启用 HTML 重写功能：选中即启用 HTML 重写功能。

3. 特殊改写功能：对页面中包含非标准 HTML 元素中的链接进行改写。

**2. 注意事项**

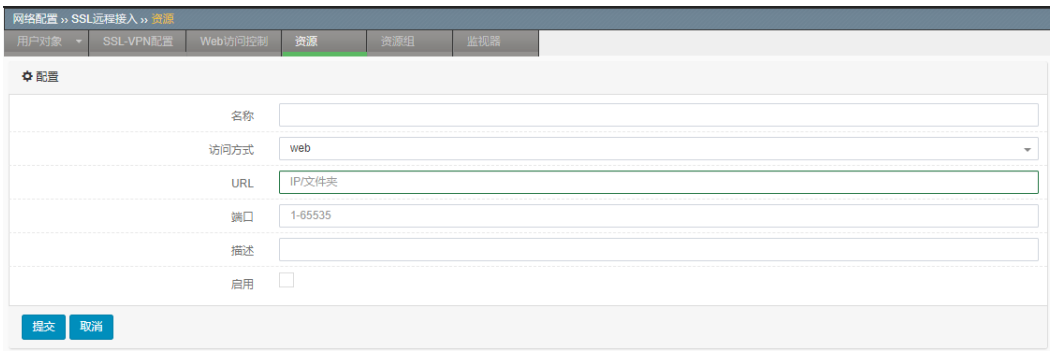
HTTP 方法过滤功能提供三类可以过滤的方法：基本方法、扩展方法和其他方法，如需要过滤的方法在基本方法和扩展方法中未给出，可以通过选择其他方法中的”other”进行过滤。

### 55.2.4 配置SSL VPN资源和资源组

天清 ADC 应用交付平台 V4.0 的 SSL VPN 支持根据用户组配置资源组，资源组是将现有的资源进行按类别组合，可以根据业务类型、用户权限级别等来对资源进行分类，如邮件访问，WEB 服务器访问，远程登录访问等。该功能可从设备上对客户端可访问的资源方便的进行控制，随时可将新建的资源加入资源组或从资源组删除已选资源，可以限定或取消限定访问某个资源组的用户组，还可以选择是否允许违反客户端安全检查的客户端对资源的访问等等。

**1. 配置可用的资源**

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




配置过程：

1. 输入资源名称；

2. 选择访问方式：如该资源为 WEB Server，则采用 WEB 方式，或根据不同资源类型选择对应的 Ftp，Fileshare ,Owa 方式；

3. 输入该资源的 IP 地址；

4. 输入该资源所提供服务的对应端口号，如 WEB Server 一般为 80；Ftp 一般为 21；

5. 输入资源描述（可选）；

6. 点击“启用”，以激活该资源；

7. 点击“提交”；

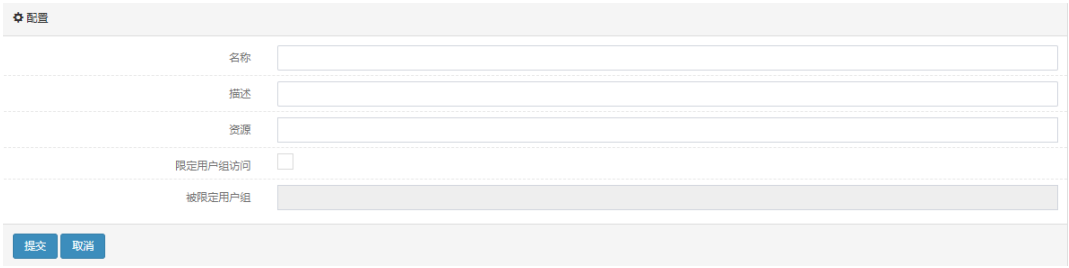
8. 重复以上过程，可以添加多个资源。

**2. 注意事项**

- 代理资源不支持域名；

**3. 配置 SSL VPN 的资源组**

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




配置过程：

1. 输入资源组名称；

2. 输入资源组描述（可选）；

3. 在资源列表栏中选择指定资源；

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

5. 点击“提交”；

6. 重复以上过程，可以添加多个资源组。

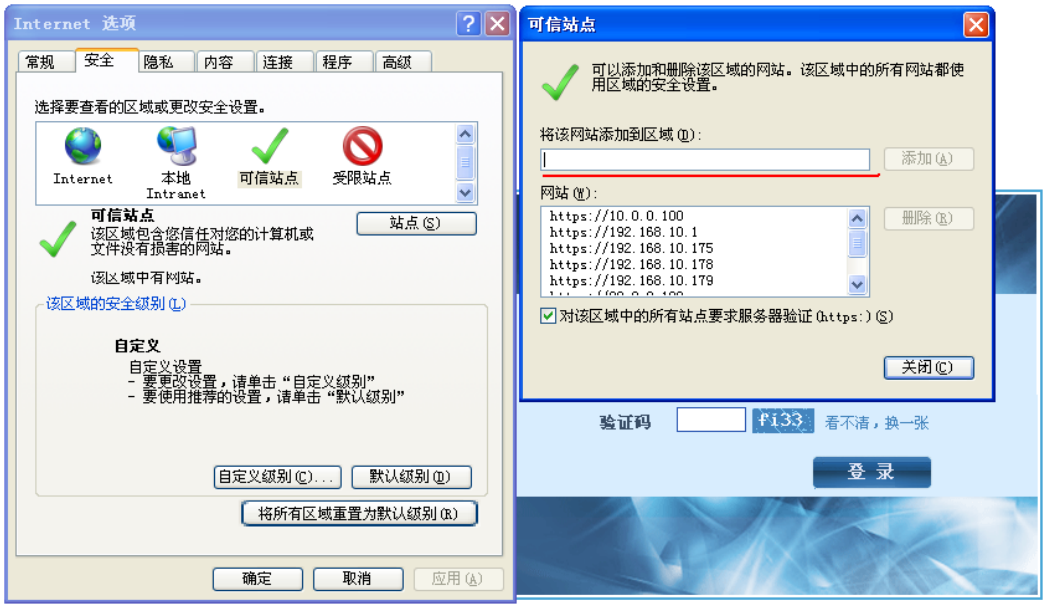
通过新建、编辑或删除资源组，可以很方便的将 SSL VPN 用户组与特定的内部资源联系起来。

## 55.3 SSL VPN登录

### 55.3.1 WEB模式

#### 1. 打开 SSL VPN 登录页面

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




SSL VPN 登录界面如下图所示：

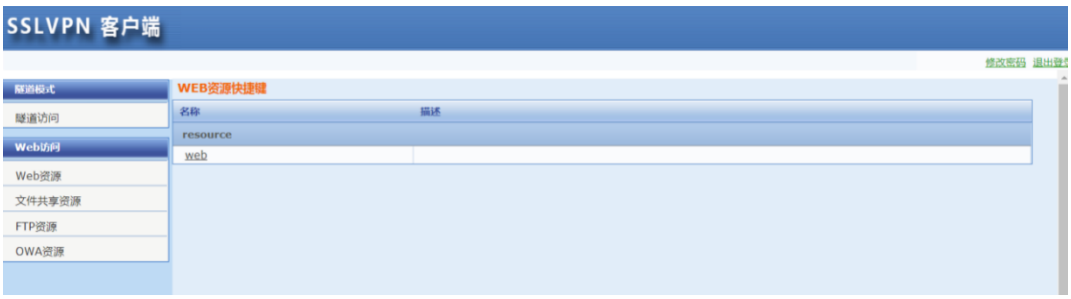
### 2. 输入用户名和密码

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

### 3. 成功登录

点击“登录”按钮，在输入正确用户名和密码情况下，登录成功，用户会看到如下页面。


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




同样还可以访问文件共享资源、FTP 资源和 OWA 资源。

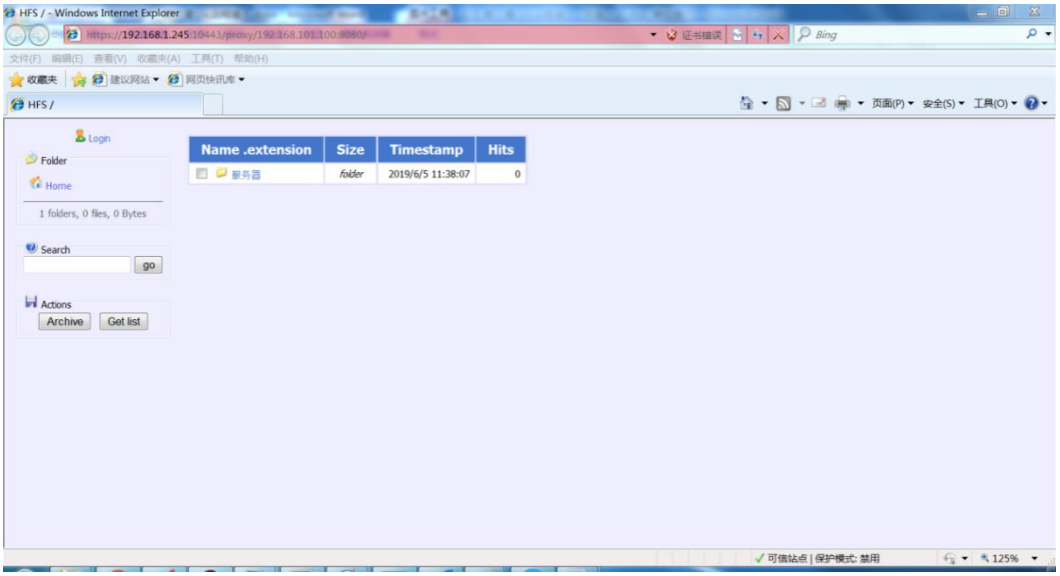
使用隧道模式访问的用户，第一次访问时需手工安装一个瘦客户端，隧道模式的使用方式下一章做专门介绍。

### 4. 访问内网资源

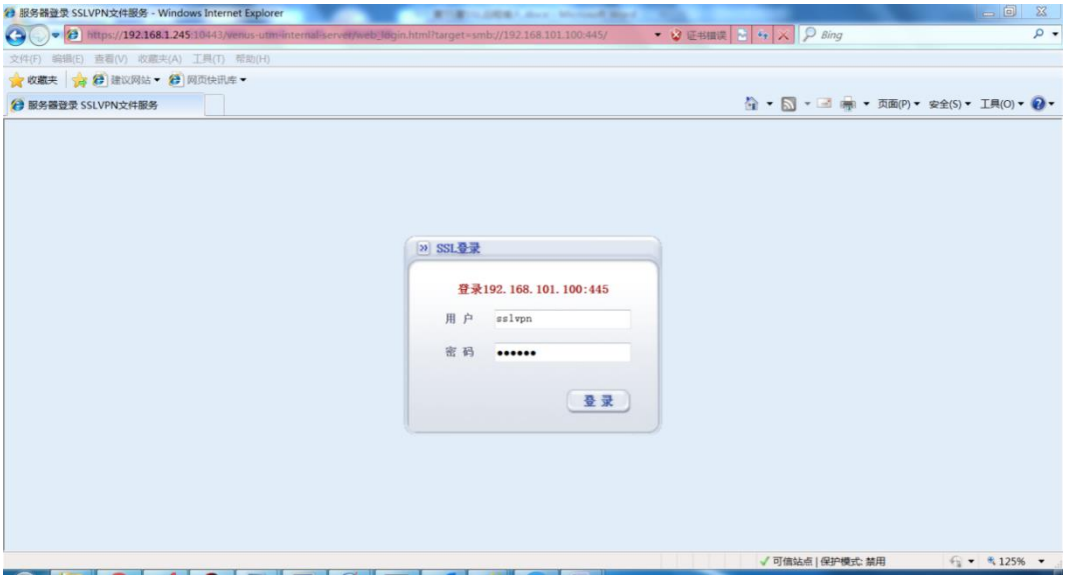
成功登陆后，用户可直接点击“WEB 资源、文件共享资源、FTP 资源、OWA 资源”下的链接跳转至内部服务器。

### 访问 Web 资源

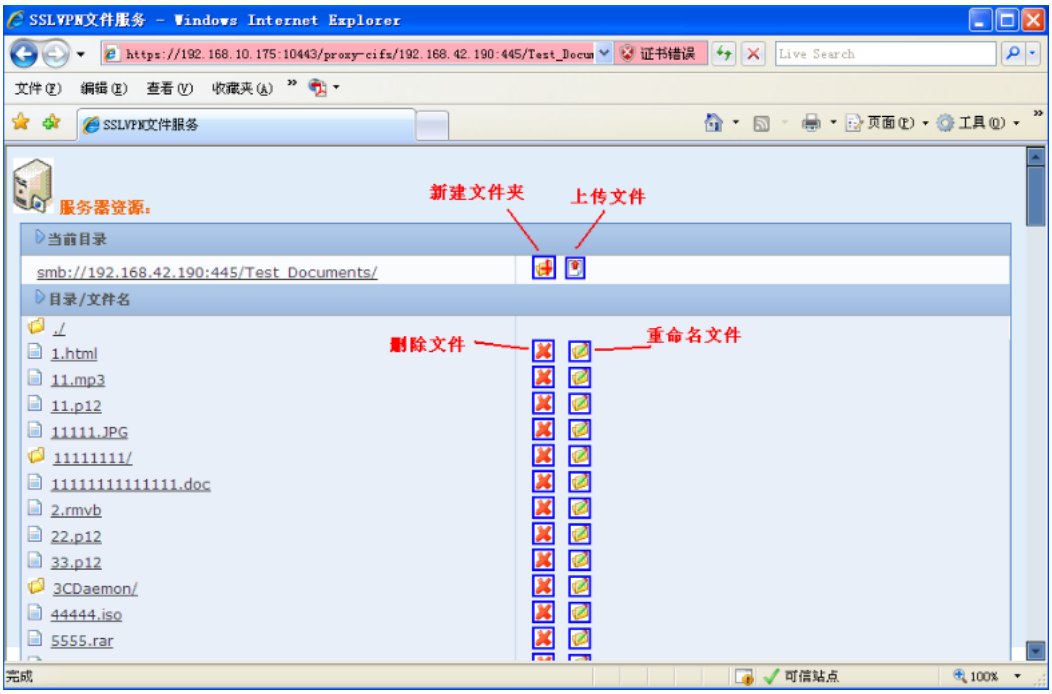
直接点击 web 资源列表中的链接即可：




### 访问文件共享资源

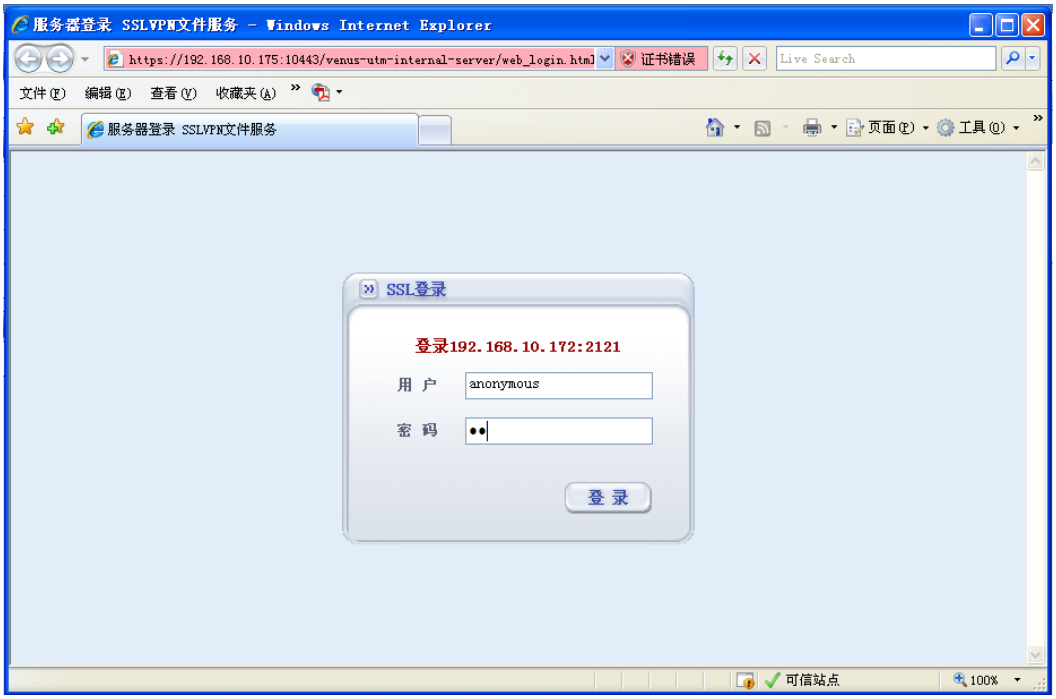



输入用户名和密码，登录：

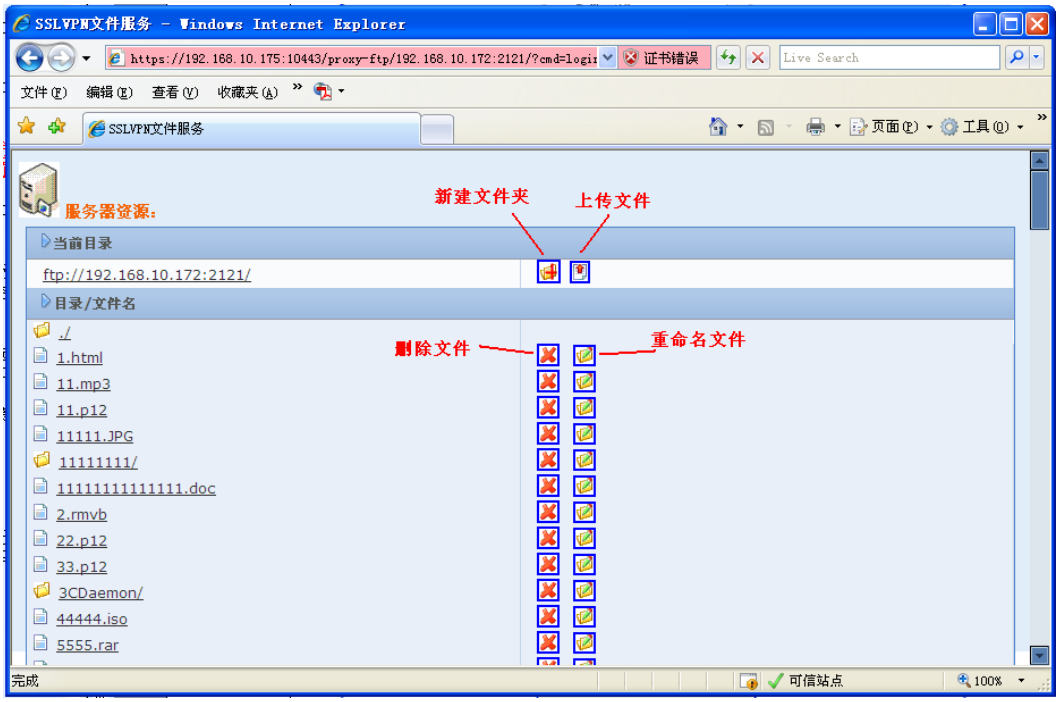



根据共享文件夹所设的属性，访问时可以新建文件夹、上传文件、直接点击下载文件、重命名文件和删除文件。

### 访问 FTP 资源

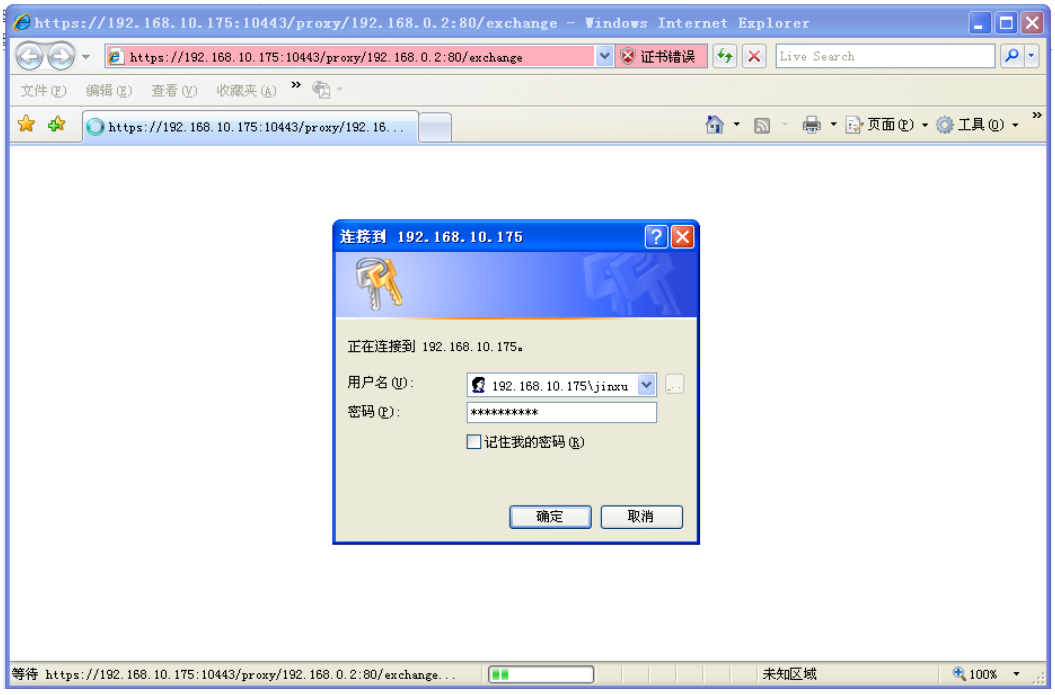



输入用户名和密码，如果允许匿名访问，可以在用户名处输入“anonymous”，密码任意即可登录，

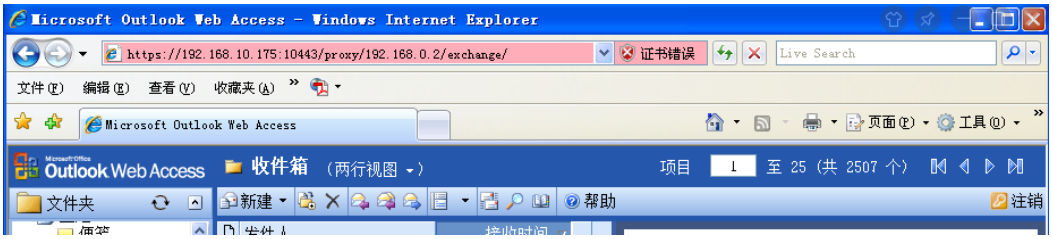



与文件共享访问类似，根据 FTP 服务器设置的不同访问权限，用户可以新建文件夹、上传文件、直接点击下载文件、重命名文件和删除文件。

### 访问 OWA 资源




需要输入邮箱的用户名和密码：




与正常使用 Outlook 收发邮件功能相同，可以正常进行收发邮件等操作。

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

#### 5. 注意事项

- 在登录页面中，存在设备本地的用户，用户名中填写的信息为“*用户名*”，需要到 RADIUS 或者 LDAP 服务器认证的用户，用户名中填写的信息为“*用户名@组名*”，其中用户名和组名分别为在 SSL VPN 配置阶段所创建的 SSL VPN 用户和 SSL VPN 用户组，详见“配置 SSL VPN 用户和用户组”部分内容。
- web ftp 和文件共享不支持非空文件夹删除，不支持文件夹整体上传和下载；
- web ftp 和文件共享下载时只能直接下载，或目标另存，无法用迅雷等下载工具下载；
- 直接访问 exchange 服务器，退出操作会导致已经登录的 sslvpn 退出，此问题在知名网站上都存在。

### 55.3.2 Tunnel模式

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

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

#### 1. 客户端的安装

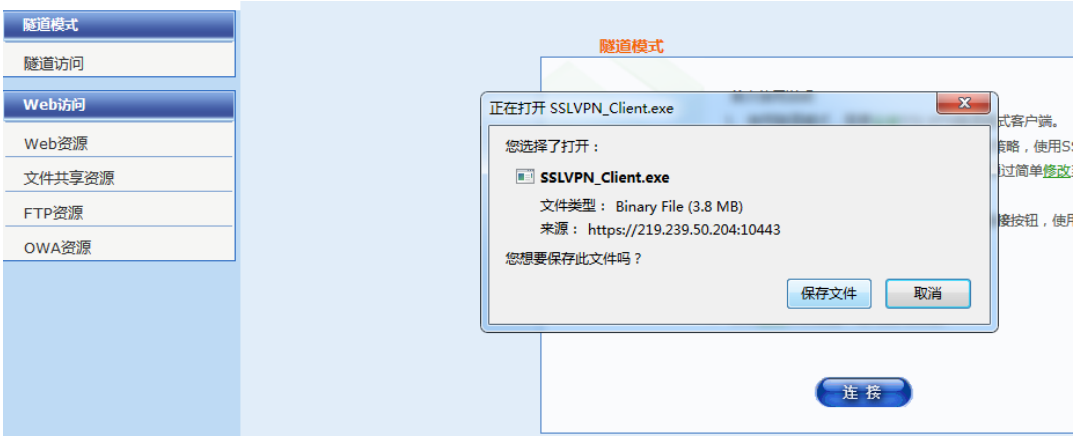
在 WEB 的登录成功页面中，点击“隧道访问”，如图：


点击第一行的“此处”可下载一个 SSL VPN 瘦客户端。

第二行的“此处”是可以避免使用证书登录或者链接隧道时浏览器弹出很多需要确认的提示信息，可以简化使用操作。

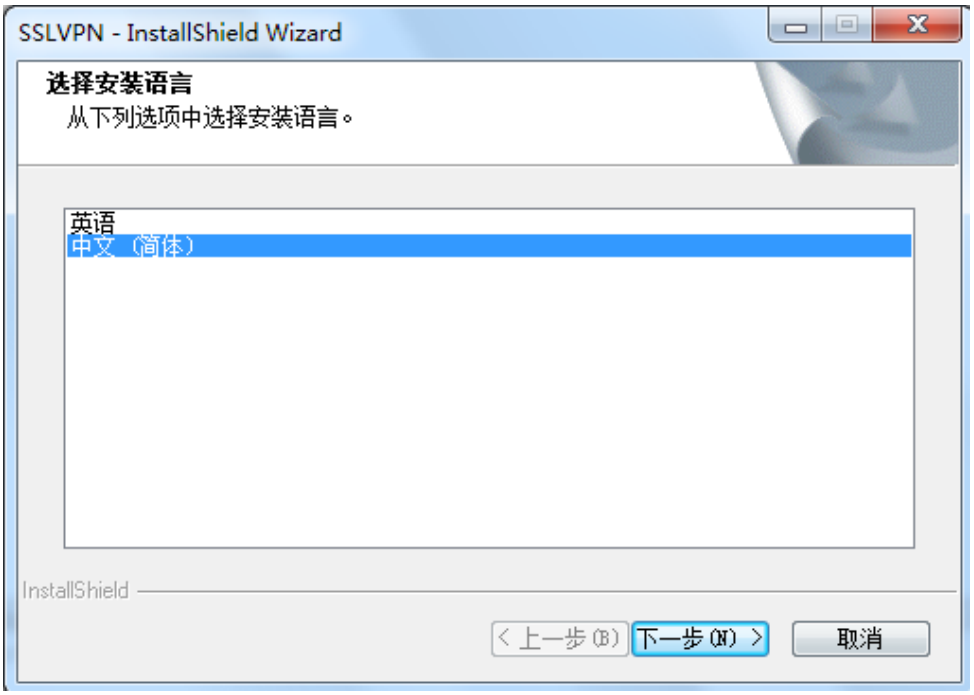
### 2. 安装客户端

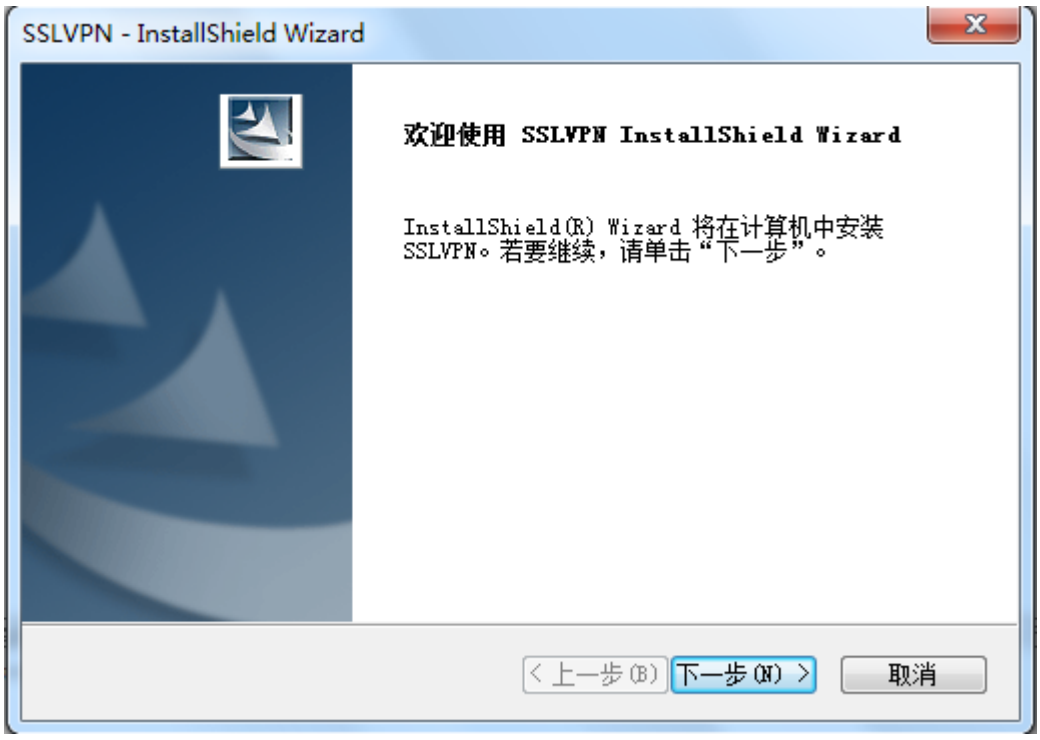
点击“此处”后浏览器会弹出文件下载提示，如下图：



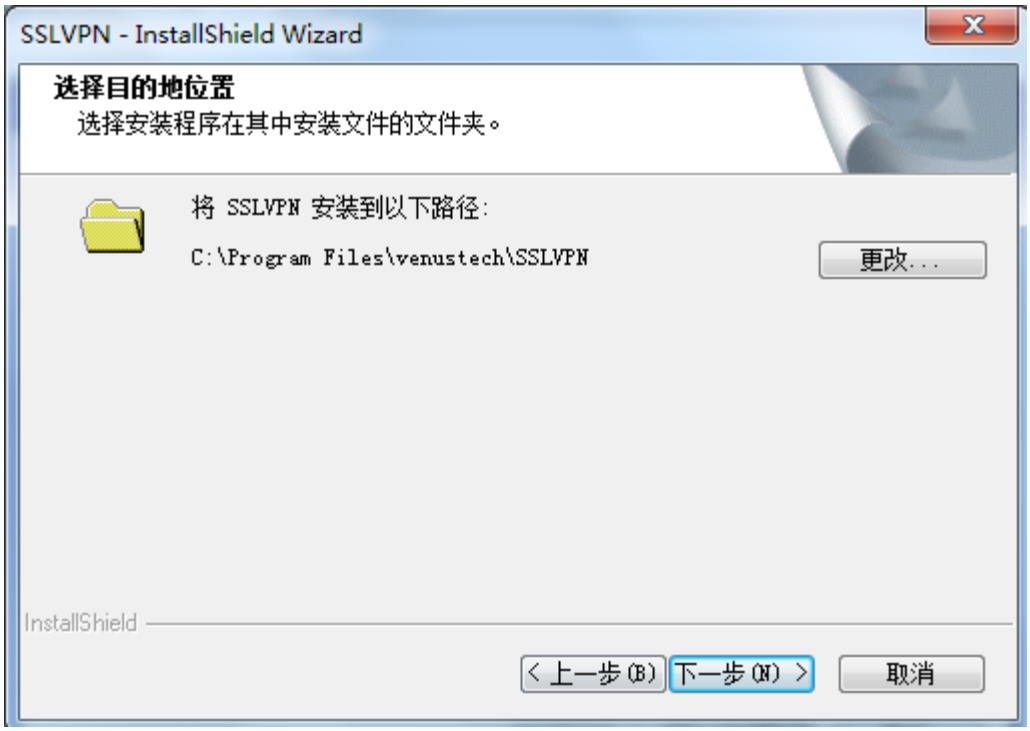

1. 选择“保存”，将 SSLVPN_Client.exe 文件下载至本机，然后双击运行该程序。某些浏览器由于捆绑了下载工具（如迅雷、FlashGet），也可用这些下载工具将 SSLVPN_Client.exe 文件下载至本地以管理员方式运行。

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

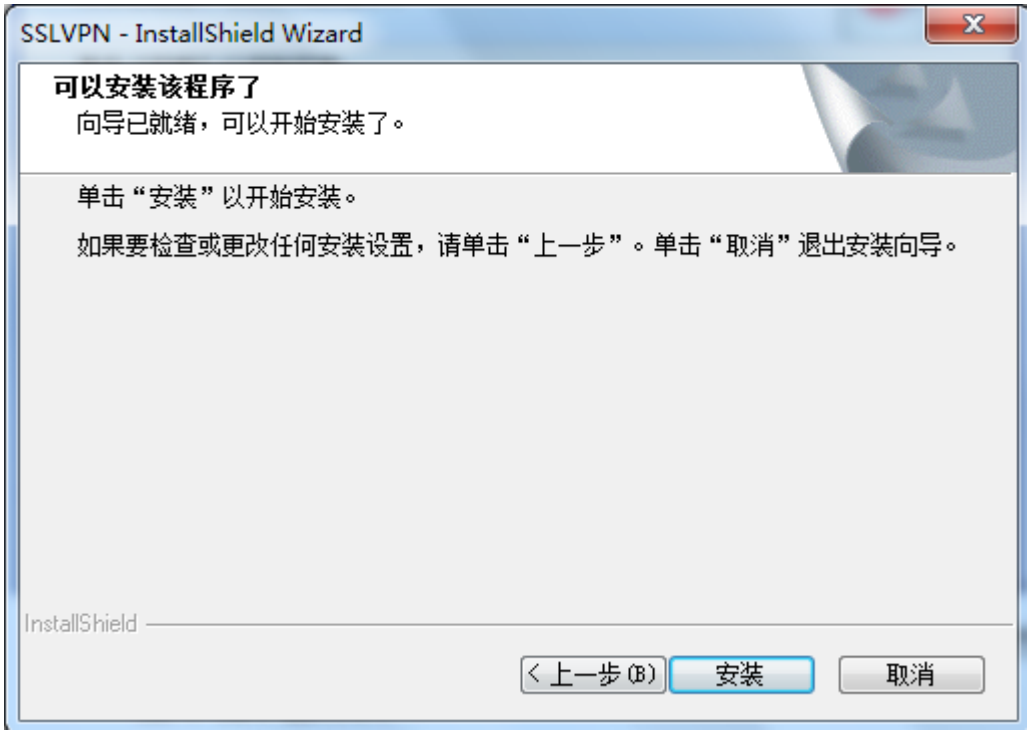


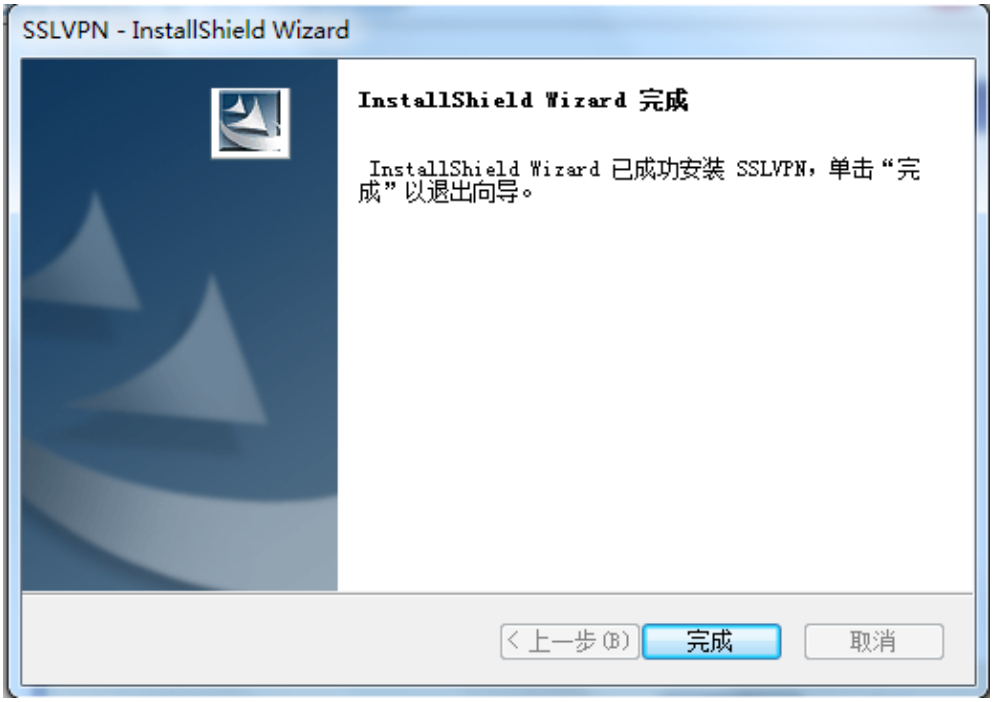

3. 此界面会提示用户选择该瘦客户端的安装路径。用户可自行选择安装目录，也可直接采用默认设置。选择好安装目录后，点击下一步。




4. 此界面提示用户安装已经就绪，点击“安装”。




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




### 3 . Tunnel 模式登录

瘦客户端安装完成后，返回到 WEB 认证界面，点击“连接”，如下图所示。


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


此时，即可开启相关软件访问 VPN 内的相关资源。

**4．注意事项**

- 隧道客户端安装时，需要注意，只安装 sslvpn 的虚拟网卡，其他选择停止安装，否则有可能会有硬件上的冲突等问题，甚至出现蓝屏；
- 任何终端用户，当完成第一次的 SSL VPN 瘦客户端安装后，下次进行 SSL VPN 连接时无需重新下载，直接点击 Tunnel 模式下的“连接”即可。即，WEB 模式登录之后直接点击“连接”，即完成了 SSL VPN 隧道方式的连接，可正常开展相关业务。
- 建议保持最初的登录页面，当需要断开 VPN 时，点击退出登录，即可完成 SSL VPN 的断开和注销工作，同时瘦客户端也会自动断开连接。
- 隧道模式一连接就断开，需要查看 pc 的服务中 DHCP 服务是否启用，所有需要使用虚拟网卡的功能都需要 pc 开启此服务；
- 隧道模式正常连接后，仍不能访问预期地址，cmd 下查看路由信息 route print，是否已经存在访问预期地址的完全匹配的一条默认路由，导致访问预期地址不走隧道路由；解决方法是禁用重新启用 pc 本地网卡，使旧的路由信息清除掉，或者手动删除该条路由信息 route delete 预期地址，确保访问预期地址走隧道路由；
- 隧道连接下发 dns 服务器，客户端有时是无法使用下发的 dns 访问，与 dns 本身

的机制有关；

- 在 win2000 上面使用隧道模式如果不通，查看一下路由表的默认网关的 metric 值，如果都是 1，需要手动修改使本地网关的 metric 值大一些，再连接隧道模式使之能通。
- 对于 Vista 系统，安装控件及瘦客户端时需要关闭账户控制 UAC 功能。隧道客户端安装时，出现如图所示，无法安装时：


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

- 对于 Win 7 或者 Win2008 操作系统，需要右键以管理员身份运行打开 ie 浏览器之后才能正常连接隧道进行访问；
- 使用 ie9 连接隧道时，会出现一连接页面就无法显示的问题，这是由于 ie9 老版本存在本身的问题，解决方法有两种：1、升级 ie9 补丁到编号为 KB2586448；2、采用右键打开新窗口的方法连接隧道。

## 55.4 SSL VPN监控与维护

### 55.4.1 SSL VPN监视器

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

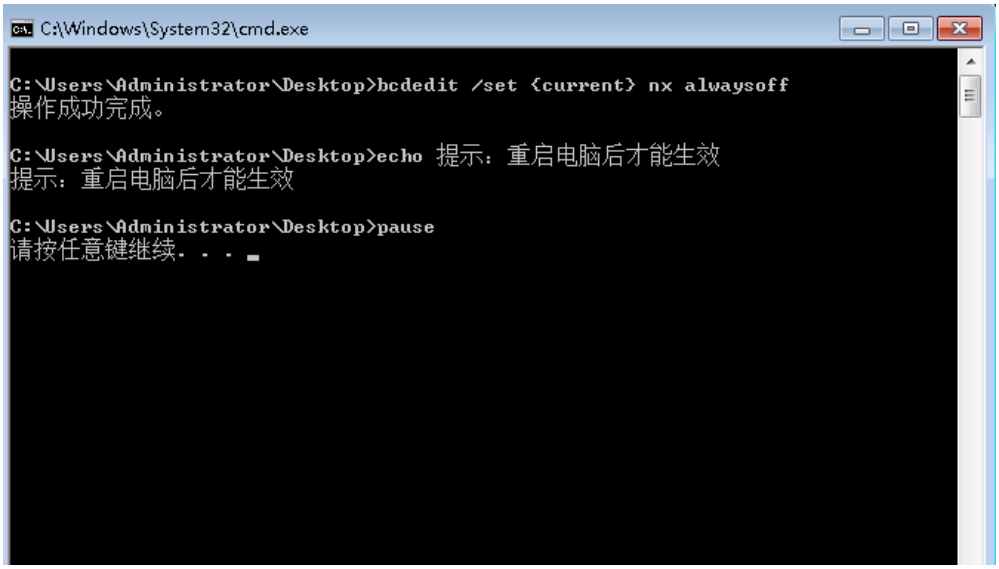
要显示在线用户 SSL VPN 用户信息，进入网络配置→SSL 远程接入→监视器。如下图：


点击用户列表最右侧的 ✖ 可以强制用户下线。

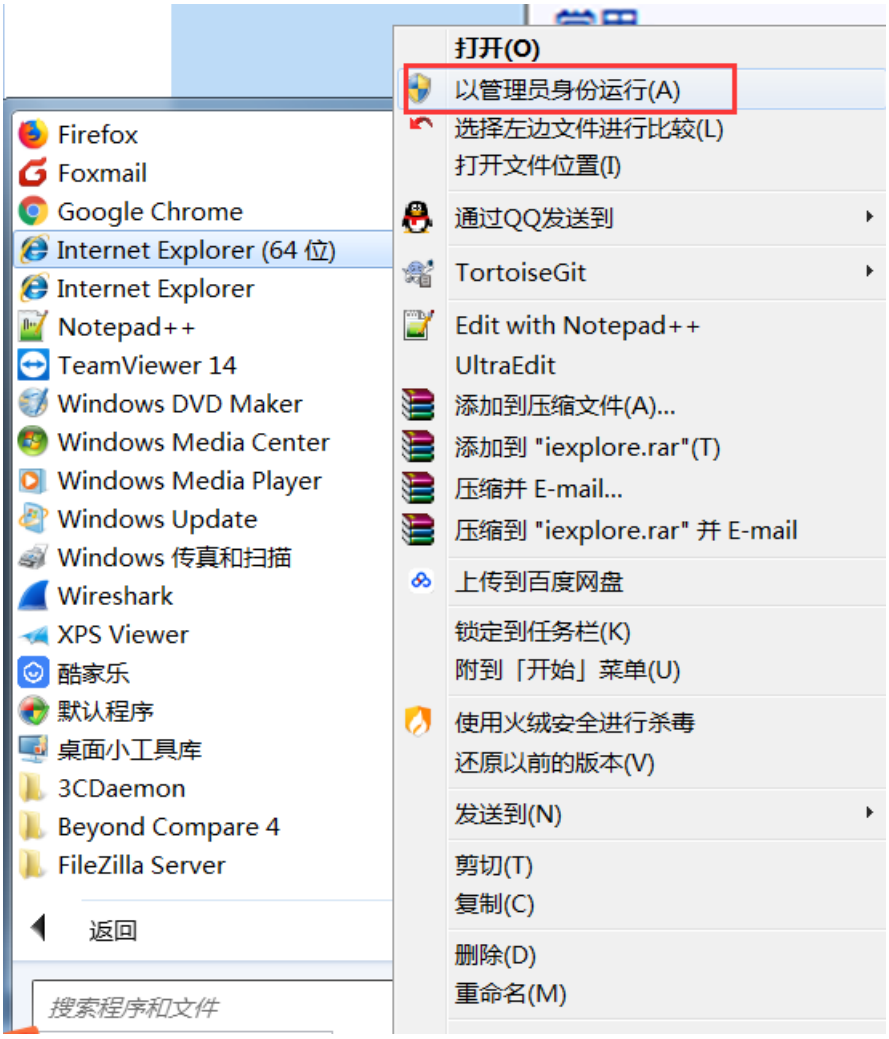
## 55.5 WINDOWS7 下的使用注意事项

配置过程：

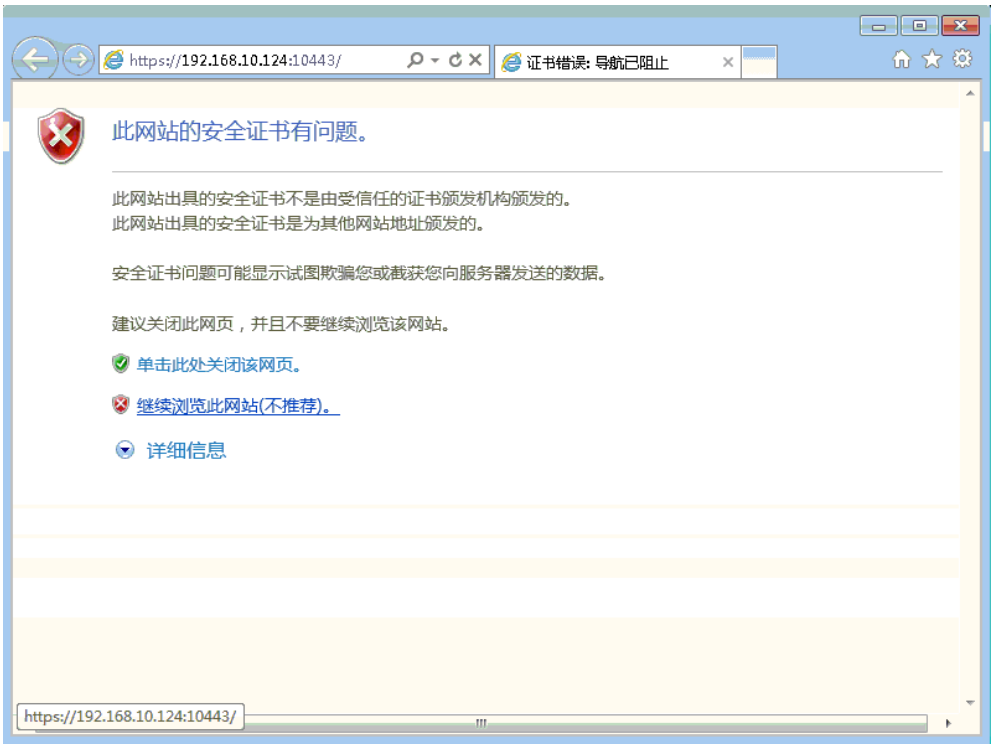
1. 安装 CloseDEP 的批处理文件并重启（安装时右键以管理员身份运行该文件）




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



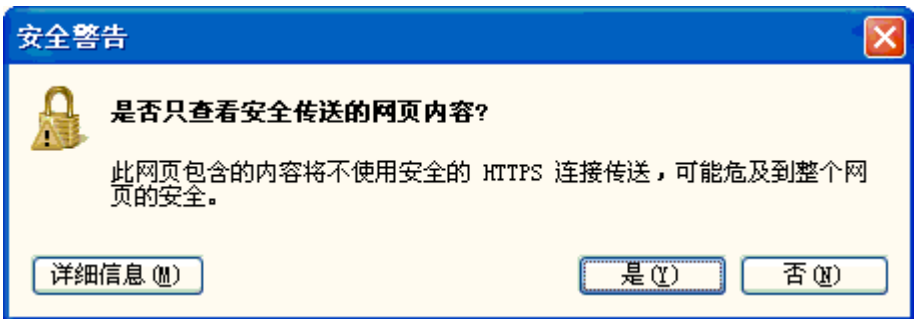

3. 输入连接的 SSL 服务的地址后选择“继续浏览此网站”




4. 输入用户名和密码、验证码并登录


5. 选择隧道模式下载安装 SSL-VPN 客户端


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

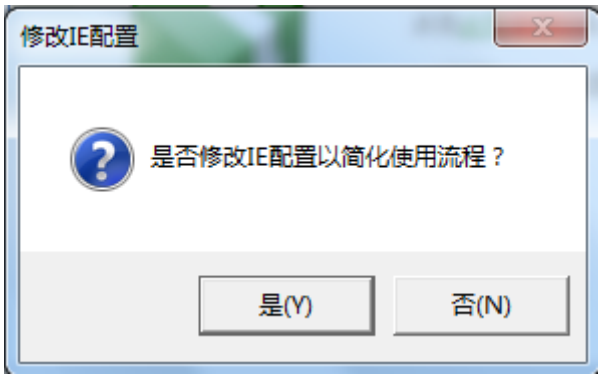


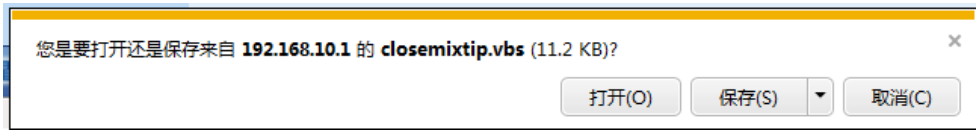

7. 出现下列选择单时选择“允许”

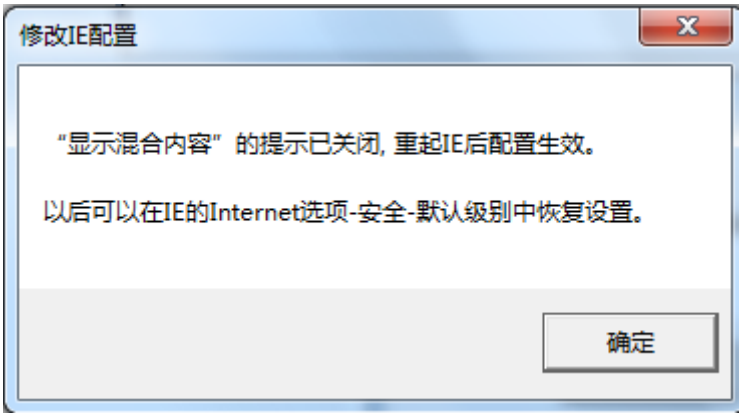

8. 出现下列图表则表明已成功连接上 SSL-VPN，可以通过 SSLVPN 隧道分到一个私网 ip，访问可达目标内的内网资源

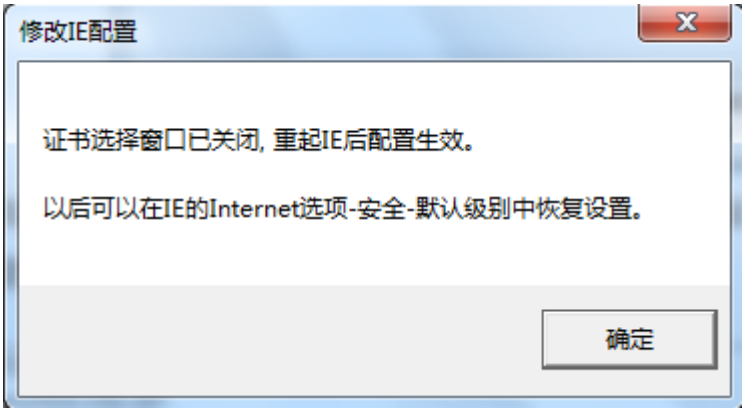

9. 对于不清楚自己 IE 版本的用户可以选择在隧道模式的界面下载一个控件用于跳过安全警告的提示，在下面的界面中选择“点击此处修改 IE 配置，简化使用流程”。

10. 点击后会下载一个名为“closemixtip.vbs”的控件，可以双击打开控件，并选择“是”来进行控件的安装




11. 如果需要恢复默认设置则在 IE 的 internet 选项中的安全中选择恢复默认级别即可

# 55.6 SSLVPN插件、客户端与操作系统兼容性问题的FAQ

## 55.6.1 共性问题

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

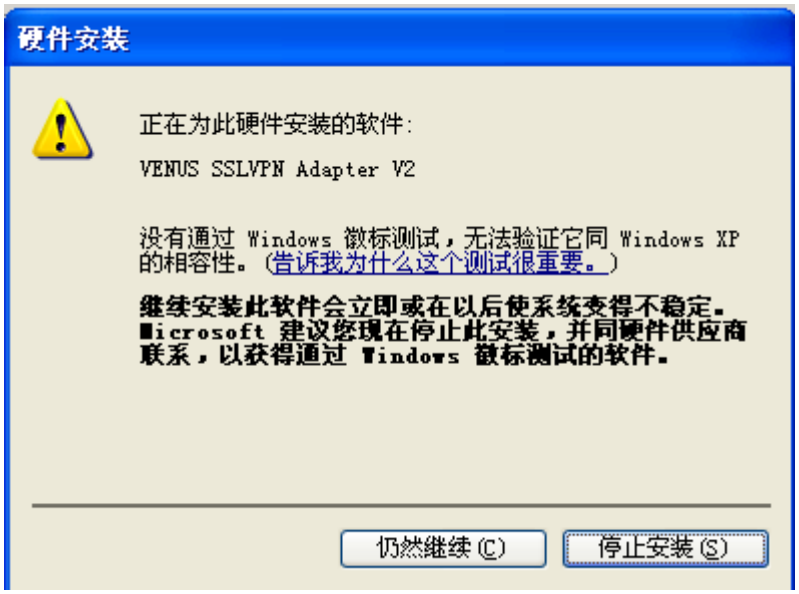
**解决方法：**需要查看 pc 的服务中 DHCP 服务是否启用，所有需要使用虚拟网卡的功能都需要 pc 开启此服务；

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

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

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

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




**现象描述 4：隧道客户端安装出现异常信息，**安装过程中出现如下图的错误信息；


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

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

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

**现象描述 6：隧道连接后，ftp 访问能够连接上，但是无法下载上传资源。**

**解决方法：**请关闭操作系统的防火墙功能。

### 55.6.2 针对Windows 2003和Windows XP-SP3操作系统

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

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

参照以下例子：

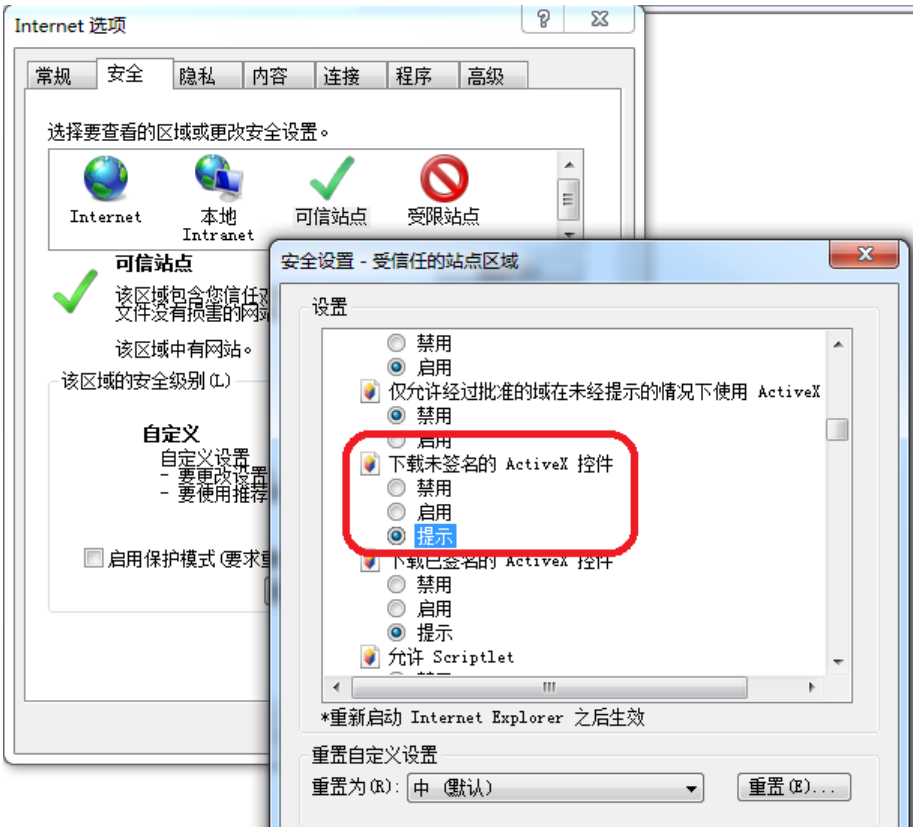
```
[boot loader]
timeout=5
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Server 2003, Standard" /fastdetect /NoExecute=OptIn
```

修改为：

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

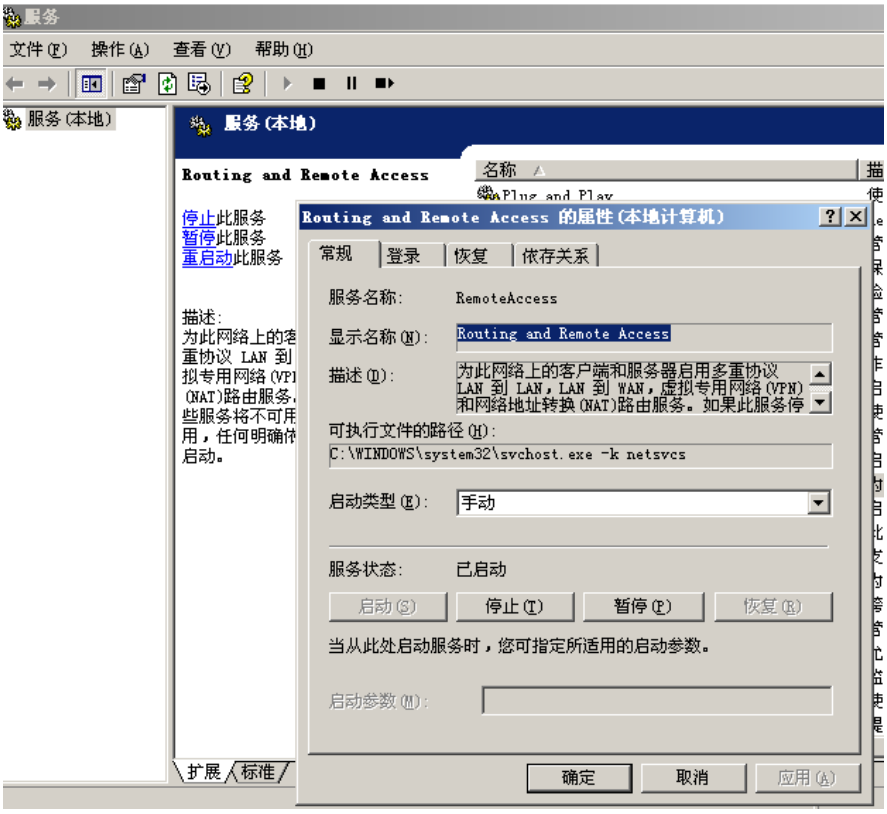
**现象描述 2：无法在 IE7 上安装插件，**设备配置正确，但是仍无法安装插件，被浏览器认为是未识别的发行者。

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




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


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




## 55.6.3 针对Windows Vista、Windows 7和Windows 2008操作系统

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

**解决方法：**以管理员身份执行 CloseDEP.bat 后，重新启动系统。

**现象描述 2：通过 ie9 安装插件，**无法安装成功

**解决方法：**同于使用 ie8 安装插件，必须右键以管理员身份运行 ie，

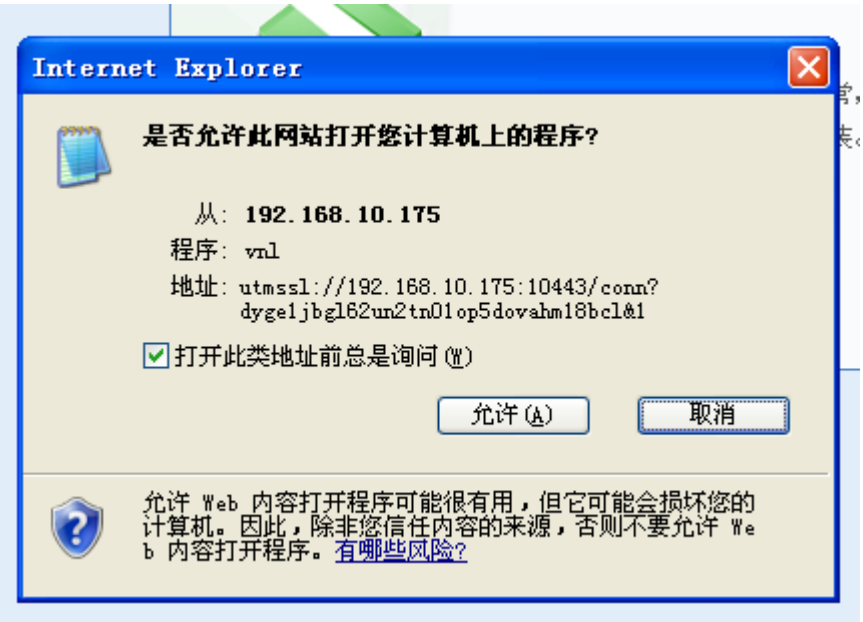
通过 ie9 安装插件过程中参考下图：


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

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

**解决方法：**首先**要确保以管理员的身份启动 IE**，之后在上图的安全警告下选

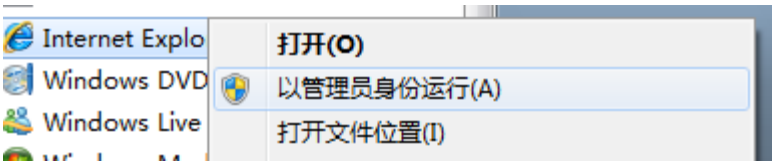

择否，就会看到下面的提示信息：




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

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

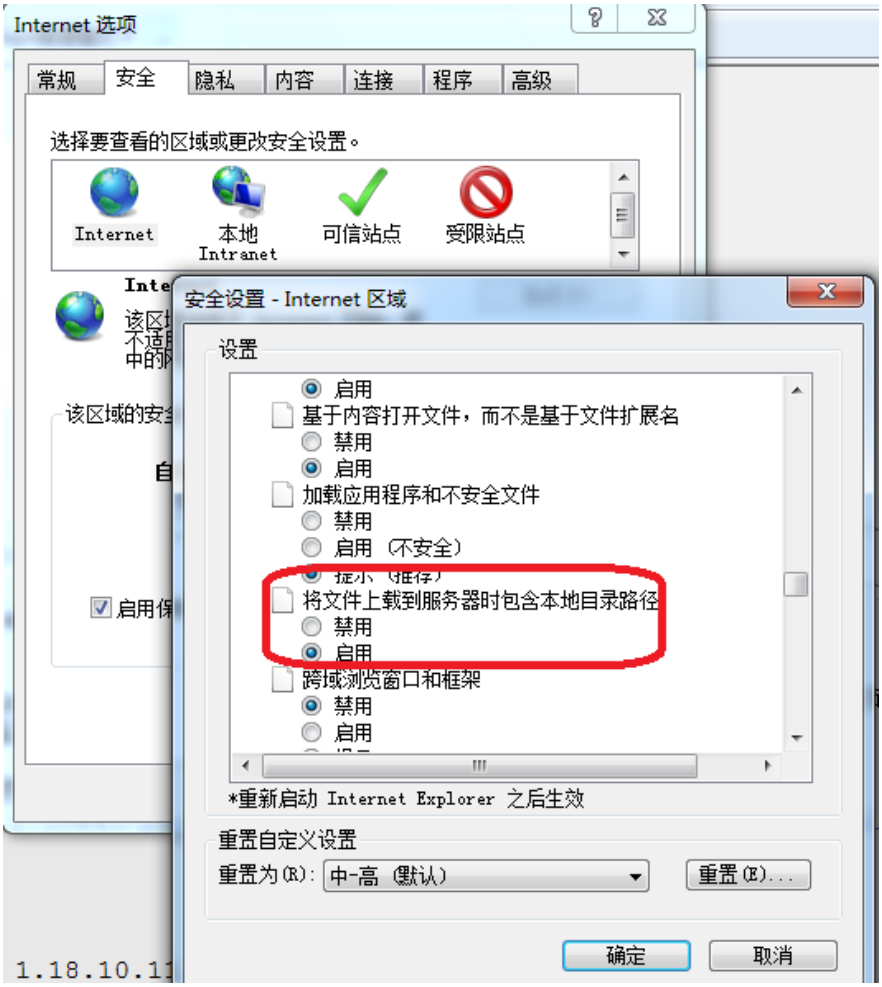
**解决方法：**要右键以管理员身份运行来打开 ie 浏览器，




然后登录到 sslvpn 后连接隧道，就能保持隧道不断，访问资源了。

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

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



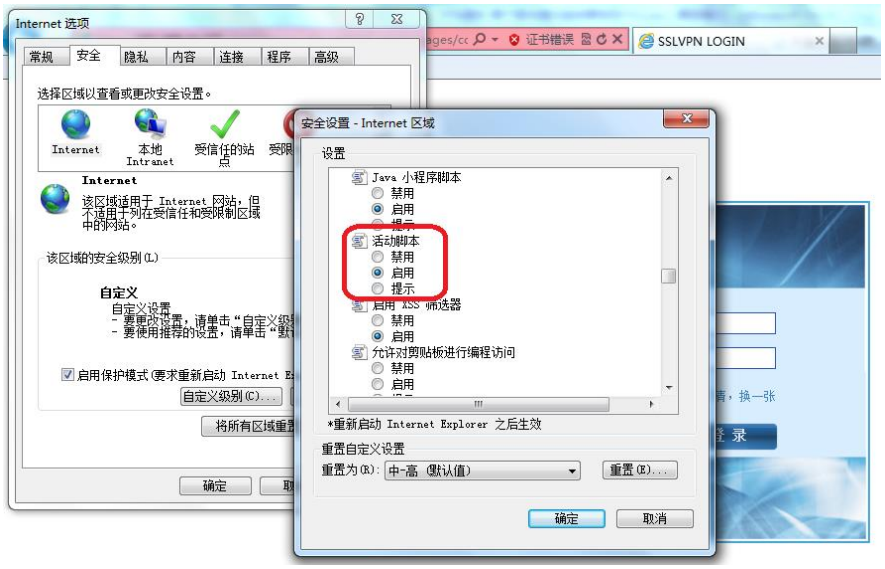

**现象描述 6：通过 web 代理方式无法打开使用启明星辰公司的 erp 报销系统，**页面跳转不正确或跳转后无法登录进去，建立报销单时无法弹出日期选择页面。

**解决方法：**需要启用 html 重写，同时配置特殊改写字段为

/OA_HTML/cabo/jsps/a.jsp。（如果是其他公司特有的网页或系统无法实现页面跳转，请联系启明星辰公司人员帮忙查看对应的特殊改写字段需要怎样配置）

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

**解决方法：**需要将浏览器的安全级别中的自定义项目中的活动脚本设为启用的状态：




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

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

# 56 第56章 协议管理

## 56.1 协议管理

### 56.1.1 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。

### 56.1.2 协议管理配置

**配置步骤：**

1. 进入**网络配置>协议管理>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。


注意

配置协议管理后，对新建的连接才会生效。

## 56.2 TCP状态管理

### 56.2.1 TCP状态管理概述

主要用于设备的连接统计功能，根据设置所有连接或则 ESTABLISED 链接，来判断是否是一个 TCP 的连接。

### 56.2.2 TCP状态管理配置

**配置步骤：**

**1．进入网络配置>协议管理>TCP 状态管理。**


**参数说明：**

**ESTABLISED 链接**：只有 TCP 状态达到 ESTABLISED 状态时，才会被认定为一个 TCP 连接

**所有链接**：指完成 TCP 三次握手的链接被认定为一个 TCP 连接。

# 57 第57章 WEB 调试

## 57.1 WEB调试概述

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

目前可观察的关键流程包含：数据包的流相关处理、NAT 处理、虚拟服务的匹配的调度、七层代理处理。

## 57.2 配置WEB调试

### 57.2.1 配置WEB调试的基本要素

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

**配置步骤：**

1. 进入**网络配置>网络调试>WEB 调试**，如下图：


**参数说明：**

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

**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、虚拟服务、代理。

**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。

**虚拟服务**：数据包匹配虚拟服务，以及相关的调度信息。

**代理**：七层代理相关的处理信息。

**安全策略**：流量匹配安全策略后显示相关流量信息。

2. 配置完毕后，点击**开始**，调试开始。

3. 点击**清除**，可以清空 DEBUG 结果框中显示的信息。

4. 在调试时，点击**停止**，调试停止。

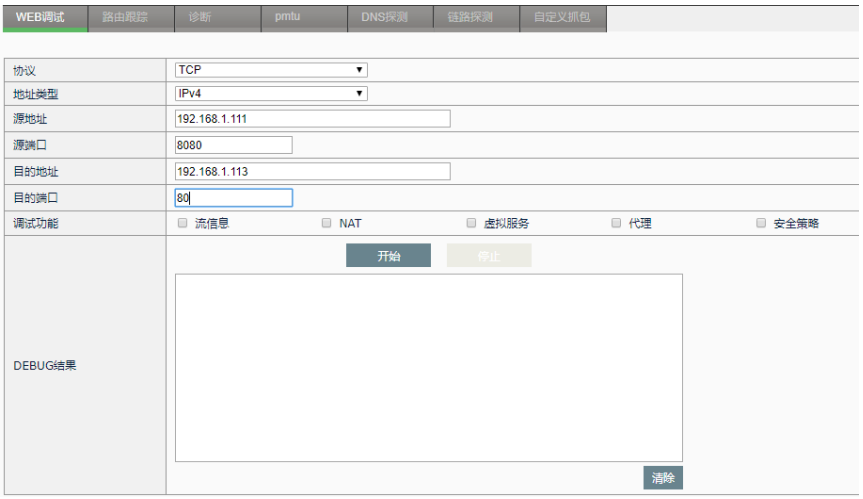

在调试过程中不能更改参数，需停止后方可更改。

## 57.2.2 配置协议为TCP(UDP)的WEB调试

协议为 TCP(UDP)的 WEB 调试需要填写源端口、目的端口参数。

**配置步骤：**

1. 进入**网络配置>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。

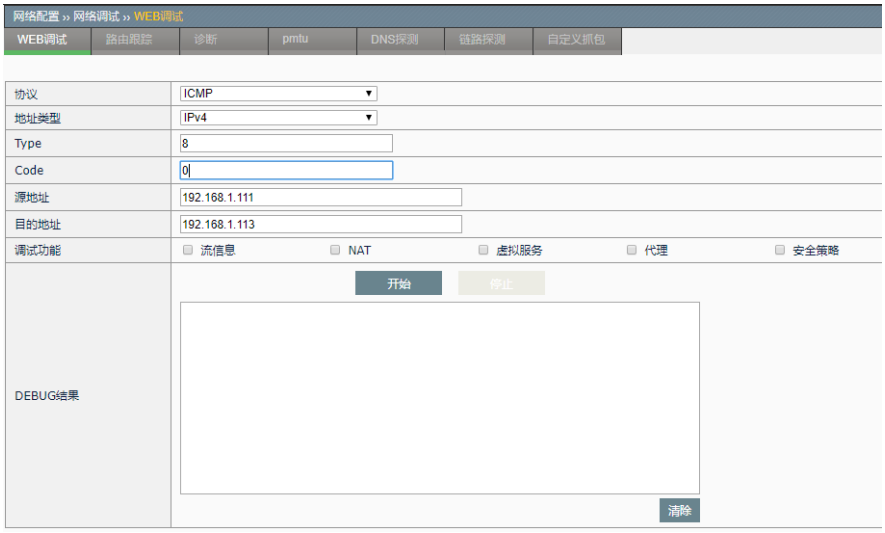
**目的端口**：数据包的目的端口。

### 57.2.3 配置协议为ICMP的WEB调试

协议为 ICMP 的 WEB 调试需要填写 Code、Type 参数。

**配置步骤：**

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




**Type**：ICMP 报文的类型，取值区间 0~255。

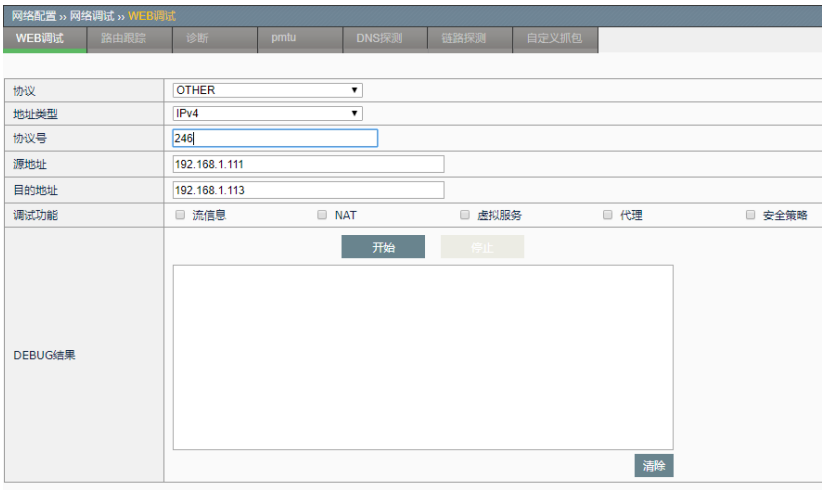
**Code**：ICMP 报文携带的的代码字段，取值区间 0~255。

### 57.2.4 配置协议为OTHER的WEB调试

协议为 OTHER 的 WEB 调试需要填写四层协议号参数。

**配置步骤：**

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



**协议号**：数据包的四层协议号，取值范围为 1~255。

## 57.3 配置案例

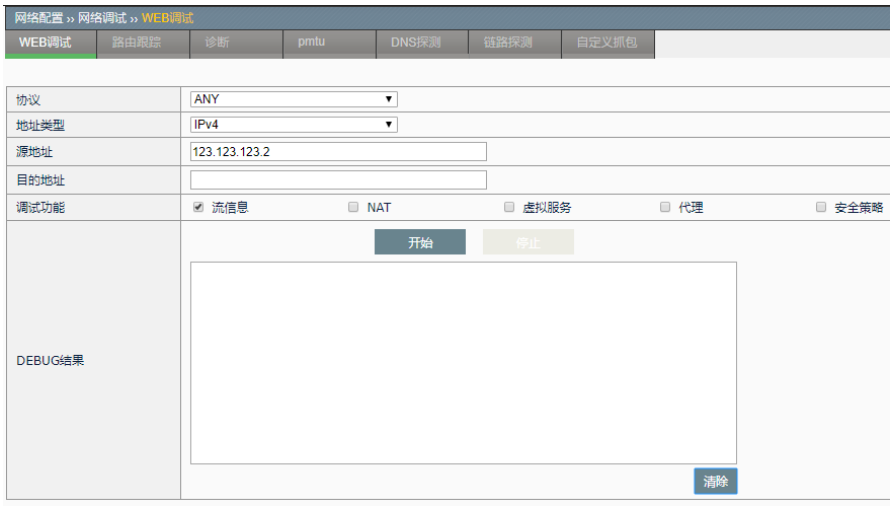
### 57.3.1 案例1：使用IPv4的Web调试功能

**案例描述**

观察主机 200.1.1.200 与任意主机之间交互的数据包的流信息

**配置步骤：**

1. 进入**网络配置>网络调试>WEB 调试**，**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：

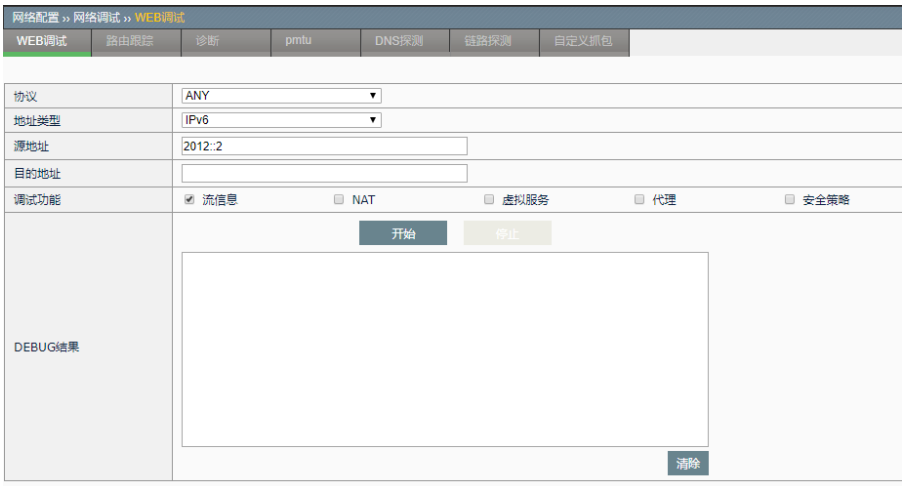

### 57.3.2 案例2：使用IPv6的Web调试功能

**案例描述**

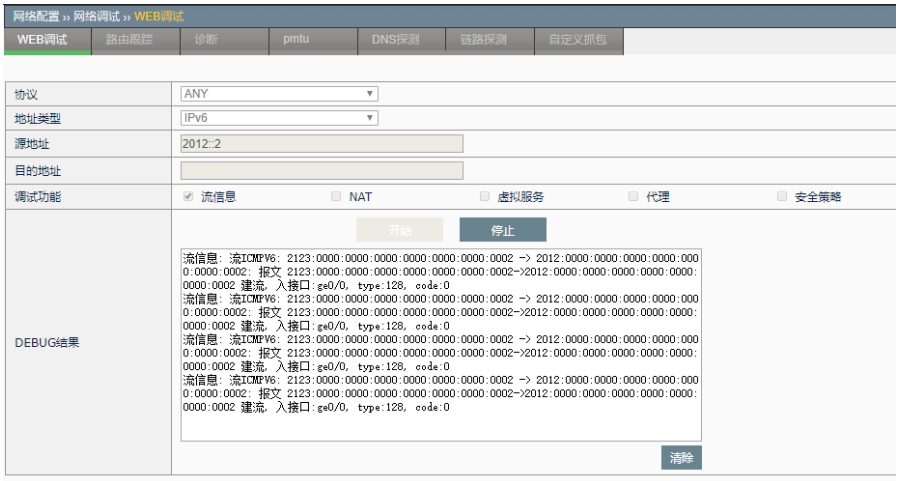
观察主机 2200::200 与主机 2200::11 之间交互的数据包相关的流信息

**配置步骤：**

1．进入**网络配置>网络调试>WEB 调试**，**协议**下拉框中选择 ANY，**IP 类型**下拉框中选择 IPv6，**调试功能**复选框中选择**流信息**，如下图：




点击**开始**，如下图：



# 58 第58章 路由跟踪

## 58.1 路由跟踪

## 58.2 路由跟踪概述

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

路由跟踪的输出结果主要包含：模拟的数据包经过的功能模块及处理结果。

目前支持的功能模块主要包括：虚拟服务的匹配，安全策略的匹配，服务池的调用，真实服务器的调度结果，连接数现在检查结果，NAT 地址转换，路由查询结果。

路由根据只显示数据包经过的功能模块。

## 58.3 配置路由跟踪

### 58.3.1 配置路由跟踪的基本要素

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

用户必须指定所有的基本要素，以模拟一个数据包。

**配置步骤：**

1. 进入网络配置>网络调试>路由跟踪，如下图：


**参数说明：**

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

**入接口：**数据包的流入方向，可以指定某个定义好的 vlan。

**源 IP：**数据包的源地址。

**目的 IP：**数据包的目的地址。

**协议类型：**数据包的四层协议类型，包括 TCP、UDP、ICMP、IP。

**源端口：**数据包的源端口。

**目的端口：**数据包的目的端口。

2. 配置完毕后，点击**开始**。

### 58.3.2 配置TCP(或UDP)协议类型的路由跟踪

协议类型为 TCP(或 UDP)的路由跟踪，需要填写源端口和目的端口参数。

**配置步骤：**

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


**源端口**：数据包的源端口。

**目的端口**：数据包的目的端口。

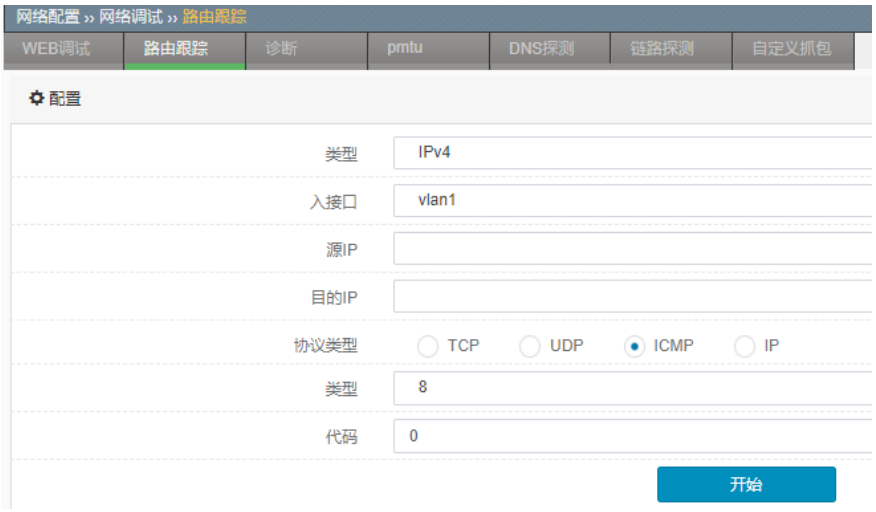
2. 点击**开始**。

### 58.3.3 配置ICMP协议类型的路由跟踪

协议类型为 ICMP 的路由跟踪，需要填写类型、代码、ID 参数。

**配置步骤：**

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




类型：ICMP 报文的类型，下拉框中可以选择 0~18。

代码：ICMP 报文携带的代码字段。

ID：ICMP 报文的 ID 号，值任意。

2. 点击开始。

### 58.3.4 配置IP协议类型的路由跟踪

协议类型为 IP 的路由跟踪，需要填写协议参数。

**配置步骤：**

1. 进入网络配置>网络调试>路由跟踪，在协议类型中选择 IP，如下图：


**协议**：数据流的四层协议号，取值范围为 1~255。

2. 点击**开始**。

## 58.4 配置案例

### 58.4.1 案例1：配置IPv4路由跟踪

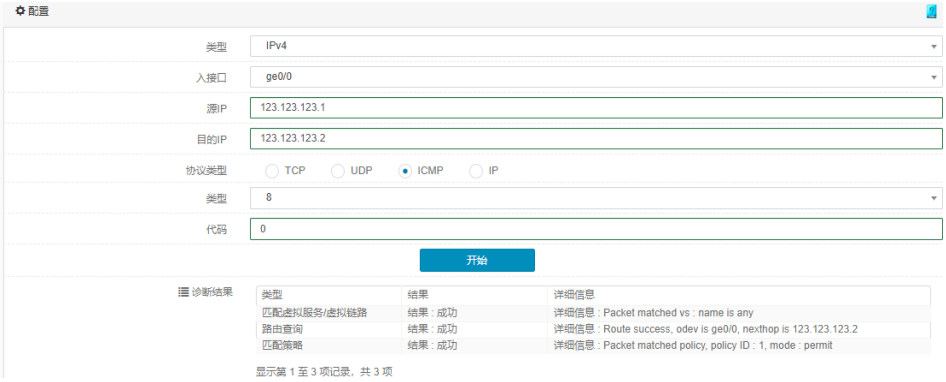
**案例描述**

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

**配置步骤：**

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


2. 点击**开始**，完成配置，如下图：




## 58.4.2 案例2：配置IPv6路由跟踪

**案例描述：**

配置 IPv6 的路由跟踪，模拟 2010::5 访问 4010::40 的 80 端口的数据包。

**配置步骤：**

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


2. 点击开始，完成配置如下图：


配置
类型
IPv6
入接口
ge0/0
源IP
2123::1
目的IP
2123::2
协议类型
TCP
UDP
ICMP
IP
源端口
80
目的端口
80
开始
诊断结果
类型
结果
详细信息
匹配虚拟服务/虚拟链路
结果：成功
详细信息：Packet matched vs : name is anyip6
路由查询
结果：成功
详细信息：Route success, odev is ge0/0, nexthop is 2123:0000:0000:0000:0000:0000:0000:0002
匹配策略
结果：成功
详细信息：Matched default policy
显示第 1 至 3 项记录，共 3 项

# 59 第59章 诊断

## 59.1 概述

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

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

## 59.2 配置

### 59.2.1 配置traceroute诊断

**配置步骤：**

1. 进入**网络配置>网络调试>诊断**，如下图：


**参数说明：**

**诊断配置：**选择诊断类型。

**目标地址：**输入进行诊断的目标 IP 地址。

**启用 UDP 端口探测：**UDP 端口探测开关。

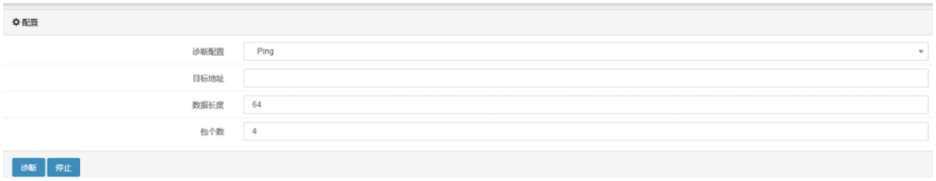
**端口：**配置报文发送的端口号。

2. 配置完毕后，点击诊断。

### 59.2.2 配置ping诊断

**配置步骤：**

1. 进入**网络配置>网络调试>诊断**，如下图：




**参数说明：**

**诊断配置：**选择诊断类型。

**目标地址：**输入进行诊断的目标 IP 地址。

**数据长度：**发送报文的数据长度。

**包个数：**发送的报文个数。

2. 配置完毕后，点击诊断。

### 59.2.3 配置TCP诊断

**配置步骤：**

1. 进入**网络配置>网络调试>诊断**，如下图：


**参数说明：**

**诊断配置：**选择诊断类型。

**目标地址：**输入进行诊断的目标 IP 地址。

**端口：**配置报文发送的端口号。

**包个数：**发送的报文个数。

## 59.3 配置案例

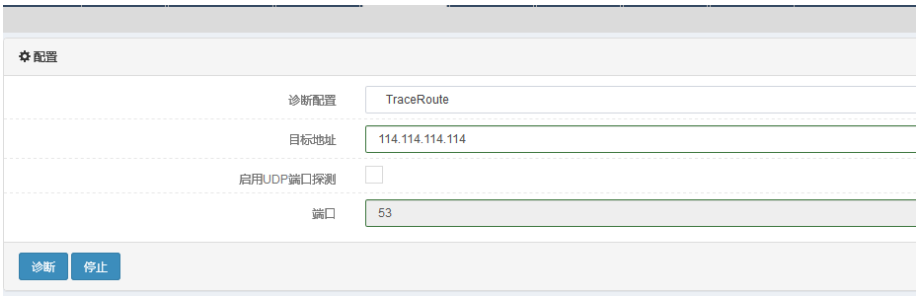
### 59.3.1 配置案例1：配置诊断功能

**案例描述**

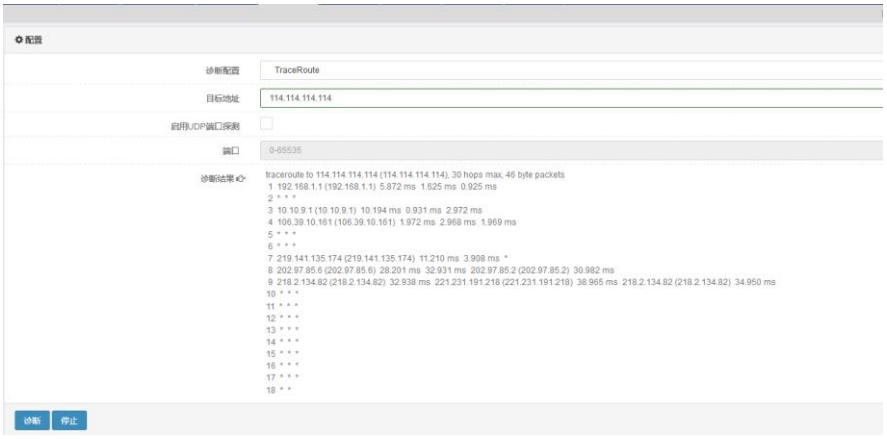
对 114.114.114.114 进行 traceroute 探测。

**配置步骤：**

1. 进入**网络配置>网络调试>诊断**，如下图所示：




2. 点击**诊断**




若不想等待完整结果，可以点击停止。将返回现有的不完整结果。

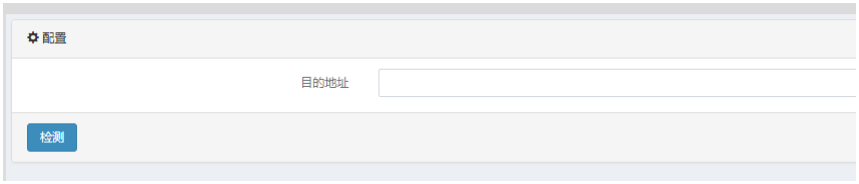
# 60 第60章 PMTU

## 60.1 PMTU概述

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

## 60.2 PMTU配置

进入**网络配置>网络调试>pmtu**，可看到如下界面。




**目的地址：**可根据选择的地址类型，指定探测的目的地址。

**检测：**点击检测后开始探测。

## 60.3 配置案例

**案例描述**

探测到 192.168.1.1 路径上最大传输单元。

**配置步骤：**

1.进入**网络>网络调试>pmtu**，填写目的地址：


2.点击**检测**，进行探测，探测结果：


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

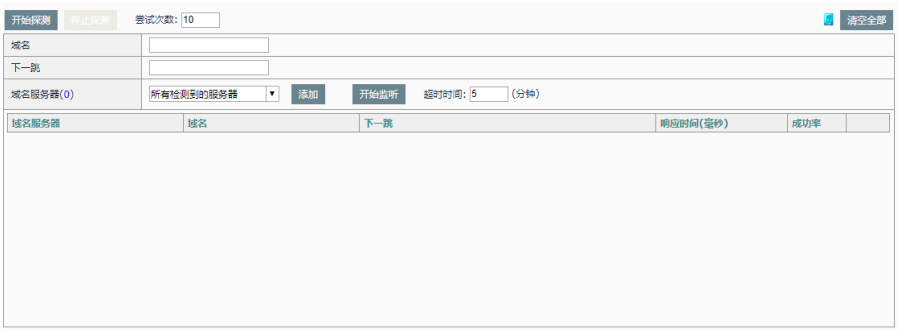
# 61 第61章 DNS 探测

## 61.1 概述

DNS 探测功能，用户可通过此功能，收集用户流量中正在使用的 DNS 服务器，并且可以对服务器进行探测，方便用户掌握 DNS 服务器工作状态，有利于对现有网络进行分析。

## 61.2 DNS探测配置

进入**网络配置>网络调试>DNS 探测**，可看到如下界面。可通过监听，获取 dns 服务器，并对服务器进行探测。




**开始监听：**点击，开始监听目前网络中正在使用的 DNS 服务器，实际为匹配虚拟链路的流量中，找出目的端口为 UDP53 这类报文中的目的 IP 地址。监听到的服务器以下拉表形式存放在域名服务器下拉列表中。

**超时时间：**点击开始监听以后超过时间自动停止监听。（持续监听会影响设备性能）

**域名服务器：**监听完成后得到的域名服务器将出现在下拉列表中供选择

**域名：**探测时使用的域名。

**下一跳：**探测使用的链路，用链路的下一跳来指出。

**添加：**把服务器添加到准备探测。这里指出了：从哪一条链路向哪一个域名服务器探测哪个域名。

**尝试次数：**对每一个添加的探测条目，指定探测次数。

**开始探测：**点击探测，对选定服务器进行探测。

**停止探测：**在探测结束前手动停止探测。

**响应时间：**服务器响应时间，单位毫秒。

**成功率：**探测成功次数与总尝试次数的比例。

注意

3. 超时时间不要配置过长，由于监听 dns 服务器会影响设备性能。
4. 探测次数避免配置过大，探测次数过大，产生大量数据包，导致网络拥塞，还有可能被理解为攻击报文。

## 61.3 配置案例

**案例描述**

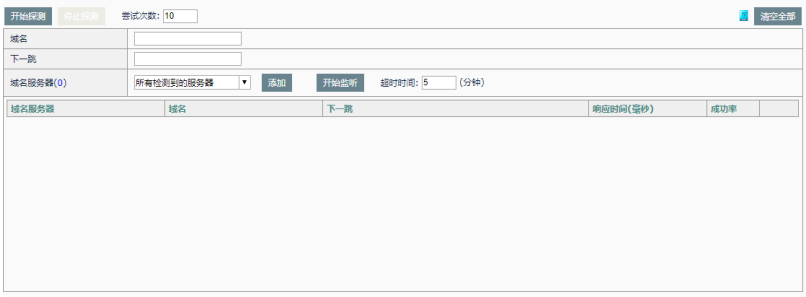
监听 DNS 服务器，并对服务器进行探测。

**配置步骤：**

1. 进入**网络配置>网络调试>DNS 探测**，开始监听：


2. 监听结果

等待超时结束自动返回结果，或者点击停止监听得到当前结果。




3. 添加服务器到准备监听

指定探测使用的域名和使用的链路下一跳，从域名服务器下拉列表中选择一个域名服务器，最后点击添加按钮。


4. 点击开始探测，查看结果


此结果展示中，向域名服务器 202.106.0.20 请求解析 www.baidu.com，响应时间很快，仅 12 毫秒，但是 10 次请求服务器只响应了 3 次。

# 62 第62章 链路探测

## 62.1 链路探测概述

链路探测用于探测从本机通过某条链路的上网速度。通过指定要探测的链路、该链路上的 DNS 服务器地址、要探测的域名信息，来探测通过该链路上网的速度与探测成功率。

## 62.2 链路探测配置管理

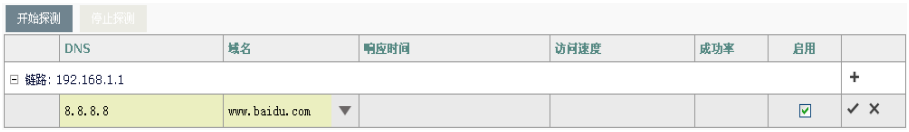
链路探测配置管理用于对要进行探测的链路，添加、删除要探测的 DNS 服务器地址、域名。

1. 进入**网络配置>网络调试>链路探测**，如下图：


**链路**：已经配置的链路节点，可以在 **虚拟链路>链路节点>链路节点** 页面查看并修改。


只有配置了链路节点，才可以进行链路探测

2. 点击 ✚，添加要探测 DNS 服务器地址、域名，如下图：




**DNS**：DNS 服务器地址

**域名**：探测的域名 URL

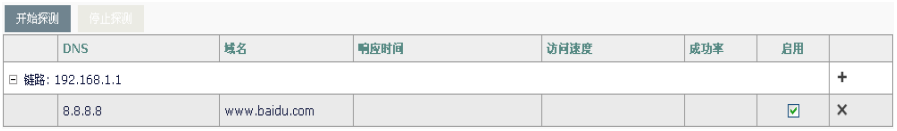
**响应时间**：链路探测的时间结果

**访问速度**：链路探测的访问速度，分为较快、一般、很慢三种

**成功率**：链路探测成功率

**启用**：启用/不启用本条探测配置

3. 点击  添加链路探测配置，点击  删除链路探测配置

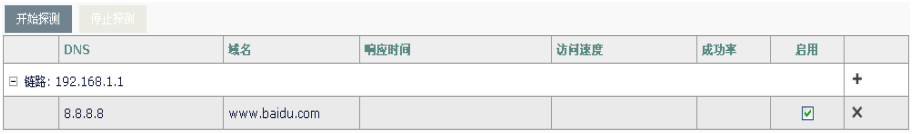



## 62.3 链路探测

配置好要探测的链路节点、DNS 服务器地址、域名，并启用该条配置后，可以对链路进行探测。探测过程需要等待，在探测期间可以停止探测。

### 62.3.1 链路探测

1. 进入**网络配置>网络调试>链路探测**，添加一条链路探测配置 DNS 服务器 8.8.8.8，域名 www.baidu.com 如下图：




2. 点击**开始探测**，进行链路探测，如下图：


3. 点击**停止探测**，停止本次探测

### 62.3.2 探测结果查看

链路探测完成后，显示探测结果，如下图：


**DNS**：DNS 服务器地址

**域名**：探测的域名 URL

**响应时间**：链路探测的平均时间结果，单位为毫秒，本次探测为 2107 毫秒

**访问速度**：链路探测的访问速度，本次探测速度为一般

**成功率**：链路探测成功率，本次探测成功率为 10 次全部成功

# 63 第63章 自定义抓包

## 63.1 概述

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

## 63.2 自定义抓包配置

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


**协议：**指定抓包的传输层协议。默认为 ANY。

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；例如对于虚拟服务来说，就是从客户端到虚拟服务器，以及虚拟服务器到客户端的所有报文。

**接收端：**抓取接收端发出和接收的报文；例如对于虚拟服务来说，就是从设备出接口到服务成员，以及从服务成员返回设备接口的所有报文。

**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）

**负载类型：**可选择抓取某个特定的虚拟服务或者虚拟链路的报文，默认为

全部。

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

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

**开始：**点击开始后开始抓取报文。

**停止：**点击停止后停止抓包（当报文抓满 10 个后会自动停止抓取）。

注意

1. 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。
2. 最多保存 10 个抓包文件，抓满 10 个文件后会自动停止抓取。
3. 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。
4. 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。
5. 源地址和目的地址始终为连接的初始源地址和目的地址。例如对于虚拟服务来说，不管是抓取发送端还是接收端报文，源地址始终为真实客户端地址。

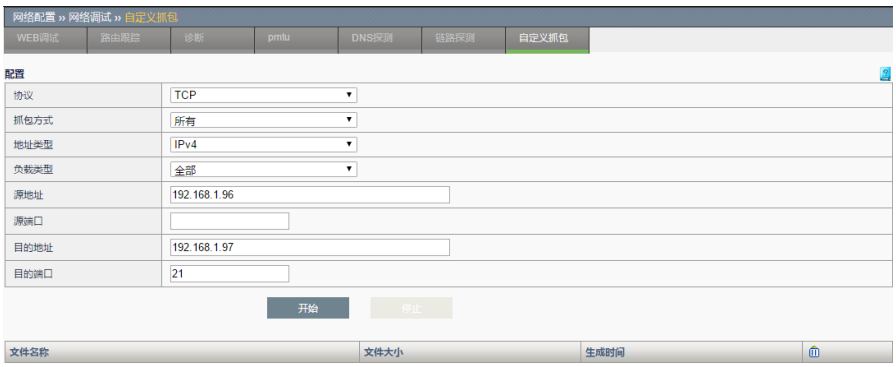
## 63.3 配置案例

**案例描述**

虚拟服务的虚拟地址为 192.168.1.97，提供 FTP 服务，客户端地址为 192.168.1.96，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**网络配置>网络调试>自定义抓包**，进行过滤条件的设置：




注：地址和端口输入框，如果不设置任何值的话，就相当于指定了所有该

类型的地址和端口。

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

| 文件名称 | 文件大小 | 生成时间 | |
|---|---|---|---|
| capture_file_0.cap | 15.49 KB | Thu Nov 20 10:14:41 2014 | |
| capture_file_1.cap | 5.24 KB | Thu Nov 20 10:15:19 2014 | |

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。

# 64 第64章 安全策略

## 64.1 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，应用交付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。

## 64.2 配置安全策略

### 64.2.1 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**安全功能>防火墙>安全策略**，点击新建。


**参数说明：**

**地址类型：**安全策略分为 IPv4 和 IPv6 两种类型，数据包匹配相应协议类型的安全策略。

**入接口：**数据流的流入方向，可以指定某个特定接口，any 表示所有接口。

**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。

**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。

**安全防护表：**引用安全防护表，对匹配的流量进行控制，防止 FLOOD 攻

击

**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。

**流量控制**：默认关闭。包含总上下行带宽和主机上下行带宽限制，用来对匹配的流量做带宽限制。

**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。

**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**。


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。

### 64.2.2 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**安全功能>防火墙>安全策略**，点击**新建**，在**动作**下拉框中选择**DENY**。

**日志**：选中此复选框启用日志功能，匹配该策略的数据流被阻断的信息会被发往 syslog 服务器，日志的优先级为信息级别。

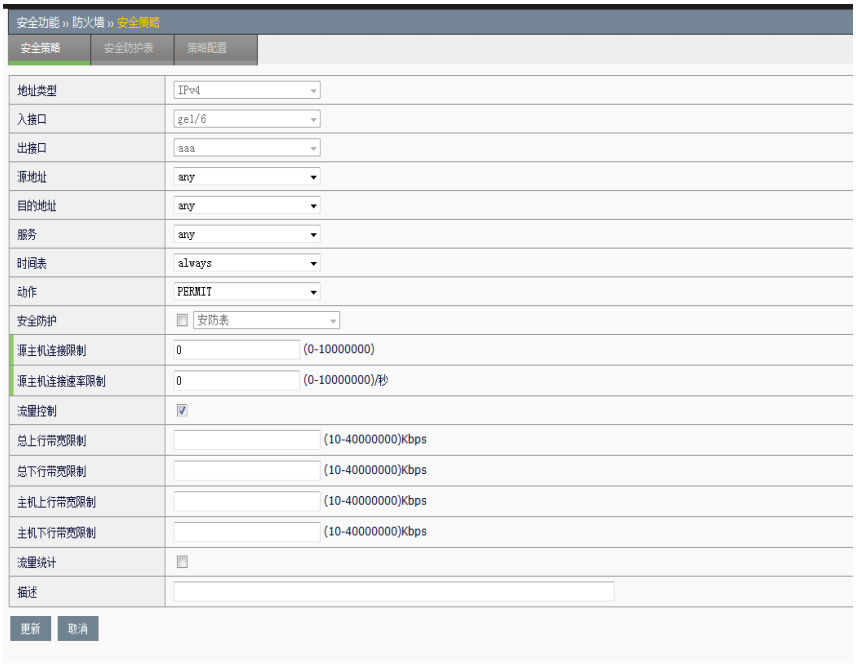
2. 点击**提交**。

### 64.2.3 配置PERMIT策略

动作为 PERMIT 的安全策略中，可以引用安全防护表。

**配置步骤：**

1. 进入**安全功能>防火墙>安全策略**，点击**新建**，在**动作**下拉框中选择**PERMIT**。




**安全防护**：选中此复选框可以在防火墙策略中启用安全防护功能，在下拉框中选择一个已经定义好的安全防护表模板，匹配该策略的数据流都要经过相应的安全防护表的检查。

**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。

**流量控制**：对到该安全策略的流量进行限制，选中后，会出现下列选项。

**总上行带宽限制**：限制匹配安全策略的上行流量，范围为 10-40000000Kb/s

**总下行带宽限制**：限制匹配安全策略的下行流量，范围为 10-40000000Kb/s

**主机上行带宽限制：**限制匹配该安全策略的每个主机的上行流量（以 IP 作为不同主机的区分），范围为 10-40000000Kb/s

**主机下行带宽限制：**限制匹配该安全策略的每个主机的下行流量（以 IP 作为不同主机的区分），范围为 10-40000000Kb/s

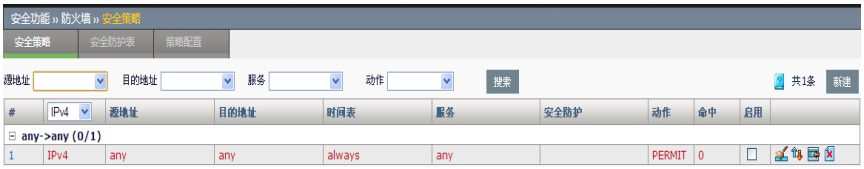
**流量统计：**统计匹配该策略的流量，可在 系统信息->会话监控->流量统计->基于策略 中进行查看。

### 64.2.4 启用安全策略

配置好的安全策略必须启用才能使其生效。

**配置步骤：**

1. 进入**安全功能>防火墙>安全策略**，如下图：



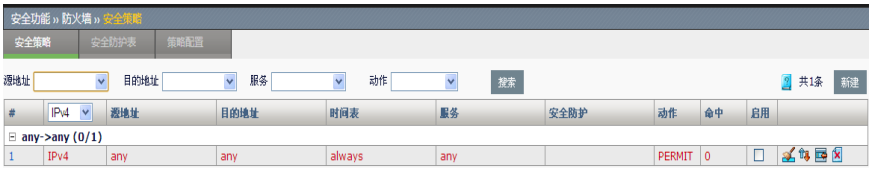

2. 勾选**启用**可以启用一条策略。

注意 策略缺省为不启用，配置后必须手工启用才能使其生效。

### 64.2.5 编辑安全策略

**配置步骤：**

1. 进入**安全功能>防火墙>安全策略**，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**。


注意

编辑策略时，地址类型和入接口及出接口都不能改变。

### 64.2.6 删除安全策略

**配置步骤：**

1. 进入**安全功能>防火墙>安全策略**，如下图：


2. 点击 删除策略。

### 64.2.7 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**安全功能>防火墙>安全策略**，如下图：


2. 点击 移动策略。


**策略 ID**：需要被移动的策略的 ID 号。

**移动到（策略 ID）**：参考策略的 ID 号。

**之前**：移动策略到参考策略之前。

**之后**：移动策略到参考策略之后。

3. 点击**提交**。

注意

只有定义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。

### 64.2.8 插入一条安全策略

**配置步骤：**

1. 进入**安全功能>防火墙>安全策略**，如下图：

2. 点击 插入一条新的策略到参考策略之前。


3. 点击**更新**。

注意

插入策略中的入接口、出接口、地址类型都必须与参考策略中的相同。

### 64.2.9 查询安全策略

**查询步骤：**

1. 进入**安全功能>防火墙>安全策略**，如下图：

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。


### 64.2.10 设置策略配置模块

在策略配置模块可以开启或者关闭整个策略匹配模块，也可以设置策略匹配不到时候的默认动作。

**配置步骤：**

1. 进入**安全功能>防火墙>策略配置.**


2. **勾选或者取消**策略匹配的复选框，实现整个策略匹配模块的开启和关闭。


若勾选则开启策略匹配模块，经过系统的数据包都要经过安全策略的匹配；否则为关闭策略匹配模块，经过系统的数据包都不进行安全策略的匹配。

3. 在下拉框里**选择策略默认动作**，可选择 permit 或者 deny，此动作为匹配不到安全策略时的默认动作。


## 64.3 配置案例

### 64.3.1 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**模板和对象>对象管理>地址对象>地址节点**，配置地址对象“内网”和“外网”，如下图：


2. 进入**模板和对象>对象管理>时间对象>周期时间**，配置时间对象“非工作时间”，如下图：


3. 进入**安全功能>防火墙>安全策略**，点击**新建**，输入参数，如下图：


4. 点击**提交**。

5. 进入**安全功能>防火墙>安全策略**，如下图：

6. 勾选**启用**完成设置。

### 64.3.2 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**模板和对象>对象管理>地址对象>地址节点**，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 | 1 | | |
| 测试部 | 4010::2013:0/112 | 0 | | |
| 研发部 | 4010::2014:0/112 | 0 | | |

2. 进入**模板和对象>对象管理>时间对象>周期时间**，配置时间对象“上班时间”，如下图：

| 名称 | 每周 | 开始时间 | 结束时间 | 开始日期 | 结束日期 | 引用 | 描述 | |
|---|---|---|---|---|---|---|---|---|
| 上班时间 | | | | 2000-01-01 09:00 | 2099-01-01 18:00 | 0 | | |

3. 进入**安全功能>防火墙>安全策略**，点击**新建**，输入参数，如下图：

4. 点击**提交**。

5. 进入**安全功能>防火墙>安全策略**，如下图：

勾选**启用**完成设置。

## 64.4 安全策略监控与维护

### 64.4.1 查看安全策略

进入**安全功能>防火墙>安全策略**，可以根据协议类型查看已经配置的安全策略



## 64.5 常见故障分析

### 64.5.1 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：<br>➢ 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<br>➢ 该策略没有启用，请检查策略状态是否为启用。<br>➢ 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 |

# 65 第65章 安全防护表

## 65.1 安全防护表概述

安全防护表是防 FLOOD 攻击安全功能的配置模版，并且可对相应的日志进行配置。安全防护表需要在安全策略中引用才能起作用。

## 65.2 配置安全防护表

### 65.2.1 创建安全防护表

**配置步骤：**

进入**安全功能>防火墙>安全防护表**，点击**新建。**


**名称：**安全防护表名称，支持中文名称。

**描述：**安全防护表的简单描述信息。

**Anti-Flood Attack：**配置是否启用防 Flood 攻击。

**TCP Flood：**选择启用 TCP 协议的防 Flood 攻击功能。

**UDP Flood：**选择启用 UDP 协议的防 Flood 攻击功能。

**ICMP Flood**：选择启用 ICMP 协议的防 Flood 攻击功能。

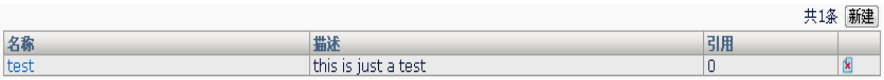
> 注意
>
> 请谨慎配置限制数量，当内部网络是通过 NAT 的方式上网时，由于源 IP 都相同，如果配置值过小，会导致防 Flood 攻击生效。

**日志**：配置安全防护表中各模块的日志过滤，支持日志信息在本地内存、syslog 服务器(日志控制中心)及 Email 这三种方式进行记录，每种方式都可以配置过滤的等级，当产生的日志高于或等于配置的过滤等级时，才会输出日志信息。

> 注意
>
> 个别模块的日志量较大，请谨慎开启并选择合适的过滤级别；
>
> 本地日志是记录在系统缓存中的，由于系统缓存有限，当缓存满时，新的日志信息会覆盖老的信息。

输入防护表**名称**和**描述**，配置好各项功能：

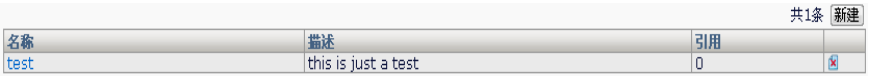

点击**提交**，完成对安全防护表的配置，显示如下页面：



### 65.2.2 编辑安全防护表

已经创建的安全防护表可以编辑修改。

**1.** 进入**安全功能>防火墙>安全防护表**



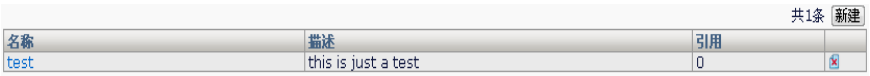

2. 单击需要修改的安全防护表**名称**，进行修改编辑。


可以对该安全防护表进行配置修改，其中名称不能改变。

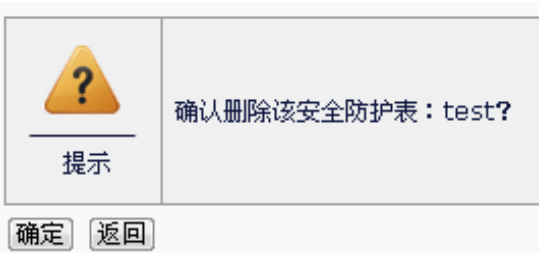
3. 点击**更新**完成修改的配置。

### 65.2.3 删除安全防护表

进入**安全功能>防火墙>安全防护表。**




选择需要删除的安全防护表，点击 进行删除。




点击**确定**，完成安全防护表的删除。

注意　正在被安全策略引用的安全防护表，其删除按钮为灰色 ，不能被删除。

### 65.2.4 在安全策略中引用安全防护表

安全防护表只有在安全策略中被引用才能生效，符合安全策略的报文才能受该安全防护表的保护。

详细配置请参见**安全策略**章节。

# 66 第66章 防攻击

## 66.1 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 fragment、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

应用交付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。

## 66.2 配置防攻击

**配置步骤：**

1．进入**安全功能>防攻击>配置**。


**防 DOS 攻击**

**Jolt2**：Jolt2 攻击通过向目的主机发送报文偏移加上报文长度超过 65535 的报文，使目的主机处理异常而崩溃。

配置了防 Jolt2 攻击功能后，应用交付设备可以检测出 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，应用交付设备可以检测出 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，应用交付设备可以检测出 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，应用交付设备可以检测出 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，应用交付设备可以检测出 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，因此应用交付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，应用交付设备可以检测出 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。

**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。应用交付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。

应用交付设备的防 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。

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**。

## 66.3 配置案例

### 66.3.1 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**安全功能>防攻击>配置**，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。

### 66.3.2 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**安全功能>防攻击>配置**，如下图：

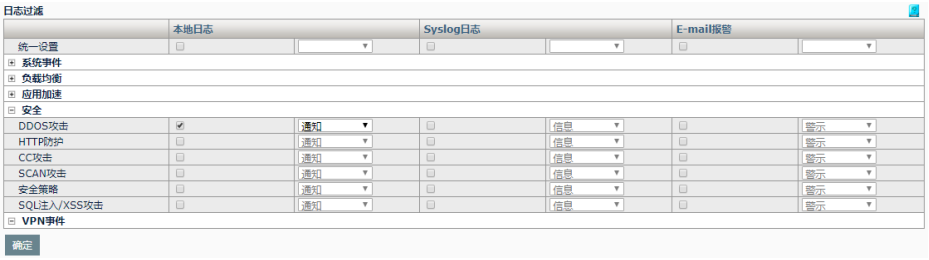

2.启用防扫描功能，输入参数。

3.点击**确定**完成设置。

## 66.4 防攻击监控与维护

### 66.4.1 查看防攻击日志

1. 进入**系统管理>日志管理>选项>日志过滤**，勾选出安全模块的相关日志，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。


## 66.5 常见故障分析

### 66.5.1 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VENUSTECH应用交付设备。 |
| 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。<br>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。<br>3．查看攻击门限设置是否过高，如过高，可降低攻击门限。 |

### 66.5.2 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：<br>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。<br>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。 |

# 67 第67章 HTTP 防护表

## 67.1 HTTP防护表概述

HTTP 防护表模块，提供了基于应用层数据的安全防护，主要针对 HTTP 协议。与传统的 4 层安全防护相比，摆脱了五元组的限制，可以深入到报文内容进行分析，更能接近用户的实际需求，也使得配置方式更为灵活、更为友好。

这部分的功能主要包括四部分：

**CC 攻击防护**：CC 攻击，主要是通过代理服务器向服务器发送大量消耗 cpu 资源的请求，导致服务器无法响应其他正常请求的一种攻击方式。CC 攻击防护的功能是将攻击报文从正常流量中识别、并进行隔离，保护服务器的正常业务。

**SQL 攻击防护**：SQL 注入，是指用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些他想得知的数据。SQL 注入攻击防护可以检测 SQL 注入，并根据配置对攻击流量进行阻断。

**XSS 攻击防护**：XSS 攻击指恶意 web 用户将代码植入到提供给其它用户使用的页面中。XSS 攻击防护能检测到 XSS 攻击，并根据配置对攻击流量进行阻断。

**HTTP 防护规则**：针对进入设备的 HTTP 流量，可按指定的规则进行报文内容检查，从而可以对不合法的流量进行阻断、重写等安全性操作。

**HTTP 浪涌保护**：如果有过多的请求到达时，将它们进行排队，当服务器有空闲连接的时候，才会发送这些请求到服务器。

**HTTP 连接确认**：对服务器无法立即回应的某些请求，设备可以回应一个提示页面，使用户等待或者自动刷新，这样可以很好的改善用户体验。

## 67.2 HTTP防护表配置

CC 攻击防护、SQL 攻击防护、XSS 攻击防护，可以直接在 **HTTP 防护表**中配置；HTTP 防护规则、HTTP 浪涌保护、HTTP 连接确认，需要单独配置完后，再由 **HTTP 防护表**来引用。

如要使 **HTTP 防护表**生效，则需在代理模式的**虚拟服务**的“**HTTP 防护**”下拉列表中选择。

### 67.2.1 配置HTTP防护表

**配置步骤：**

1. 进入**安全功能>HTTP 防护>HTTP 防护表**，如下图：


**新建：**添加一个 HTTP 防护表。

：删除掉该模板。

点击名称，可修改原有的配置。

2. 点击**新建。**


**名称：**HTTP 防护表的名称

**CC 防护：**是否启用 CC 防护。默认关闭。

**CC 防护上限：**启用 CC 防护后，当每秒 HTTP 请求数高于该值后，CC 防护才会生效。

**CC 防护下限：**启用 CC 防护后，当每秒 HTTP 请求数低于该值后，CC 防护则不生效。

提示

CC 防护的下限必须小于 CC 防护的上限

如果 CC 防护的上限值、下限值设置太低，会频繁启动、运行 CC 防护，对 HTTP 的转发性能有一定影响，请根据服务器实际情况合理配置。

注意

CC 防护是基于重定向的原理，所以如果受保护服务器提供的某些服务对应的客户端不支持重定向，那么会影响这些服务的正常功能，请谨慎配置。

**SQL 注入：**是否启用 SQL 注入防护。默认关闭。

**动作：**启用 SQL 注入防护后，可以选择。配置检测出攻击以后对流量的动

作，分阻断和无两种。阻断表示断开检测到攻击的链接，无表示不阻断该连接。

**XSS 攻击：**是否启用 XSS 攻击防护。默认关闭。

**动作：**启用 XSS 攻击防护后，可以选择。配置检测出攻击以后对流量的动作，分阻断和无两种。阻断表示断开检测到攻击的链接，无表示不阻断该连接。

**HTTP 防护规则：**可选的 HTTP 防护规则在左侧列出，后侧表示已经选中的规则。HTTP 防护规则的配置，在下一节详述。


提示

一个 HTTP 防护表，可以配置多条 HTTP 防护规则。

多条 HTTP 防护规则，是按从上到下的顺序进行匹配的，只要有一条匹配成功了，就中止匹配。

**HTTP 浪涌保护：**列表选择、匹配顺序与“HTTP 防护规则”一致

**启用：**表示启用该功能。


提示

如果只启用，而不选择浪涌规则，则表示该功能对应的是“中优先级”。优先级，可以参考“HTTP 浪涌保护”一章

**HTTP 连接确认：**列表选择、匹配顺序与“HTTP 防护规则”一致

3.点击**提交：**使当前配置生效。

## 67.3 配置案例

### 67.3.1 配置案例1：对服务器进行CC防护等

**案例描述：**

启用 CC 攻击防护、SQL 攻击防护、XSS 攻击防护。

**配置步骤：**

1. 进入**安全功能>HTTP 防护>HTTP 防护规则**，新建 111，并勾选相关的防护。如下图：


2. 所使用的虚拟服务中引用：


## 67.4 常见故障分析

### 67.4.1 故障现象1：配置应用安全规则，无法触发动作

| | |
|---|---|
| 现象 | 配置了对应的规则，但是防护无法生效 |
| 分析 | 有可能是以下几种情况导致的：<br>1. 对应的虚拟服务中是否引用了该HTTP防护表，以及是否引用了HTTP模板<br>2. 攻击是否为XSS、SQL注入 |
| 解决 | 应在虚拟服务中引用HTTP防护，并且需同时引用了某个HTTP模板才能生效。<br>检查攻击报文。 |

# 68 第68章 HTTP 防护规则

## 68.1 HTTP防护规则概述

HTTP 防护规则，针对进入设备的 HTTP 流量，可按指定的规则进行报文内容检查，从而可以对不合法的流量进行阻断、重写等安全性操作。

该功能，属于 HTTP 防护的一部分，使用时，需要在 HTTP 防护表中引用。

## 68.2 HTTP防护规则配置

**配置步骤：**

1. 进入**安全功能>HTTP 防护>HTTP 防护规则**，如下图：


**新建：**添加一个 HTTP 防护规则。

：删除掉该规则。

点击对应的名称，即可对原有的配置进行编辑。

2. 点击**新建**,如下图：


**名称：**HTTP 防护规则的名称

**源 IP：**源 IP 地址。

**IP：**输入的可以是单个 IP，例如：10.1.1.1，也可以是子网，例如 10.1.1.0/24, 2010::/64。支持 IPv4 和 IPv6。

**地址对象：**下拉选择已经配置的地址对象。关于地址对象的配置，可以参照“地址对象”相关章节。

**Host：**请求中的 Host，下拉包括任意匹配、条件匹配

**任意匹配：**该项匹配成功，即不做处理

**条件匹配：**规则类型下拉，包括完整字符串、正则。添加后在 **Host 列表**中显示，列表中带有(regex)前缀表示为正则

**URI 路径、Cookie、头域名称：**配置方式与 Host 相同

**速率：**每秒请求数。对符合当前规则的请求，计算速率，如果超过该设定值，则执行下面配置的动作。

**动作：**对满足上面配置的请求，所对应的处理动作。

**阻断：**断开连接

**响应：**对客户端进行响应，需在下方配置需响应的内容

**重写 URI：**对请求的 URI 进行改写，使之无法访问原来的 URI。需在下方配置要改写的 URI 路径

**重定向**：对客户端的请求进行重定向，使之访问新的目标。需在下方配置重定向目标网址

**放行**：对该请求做放行处理


配置>Cookie，指的是 cookie 名称，例如访问百度首页 cookie： BAIDUID=0F745D2BF00126E4C872D4A63E0CC46C:FG=1; 应该填写 BAIDUID

配置>URI 路径是大小写敏感的，而 Cookie、头域名称则是大小写不敏感的

配置>URI 路径需包含'/'，例如 http://www.baidu.com/duty/，其 URI 路径为 '/duty/'

配置>速率，0 表示每个请求都会触发设定的动作

动作>重写 URI 的配置，一般是以"/"开始的

动作>重定向的配置，应注意带上协议类型，http 或者 https。完整的重定向配置格式形如："http://www.baidu.com"

## 68.3 配置案例

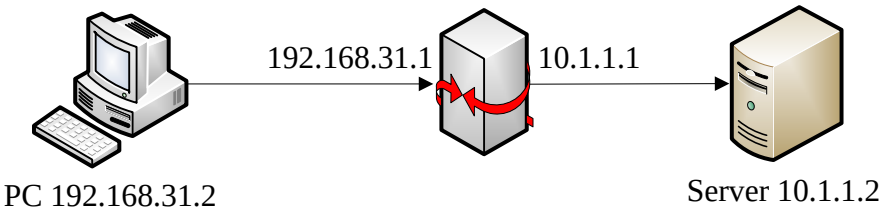
### 68.3.1 配置案例1：对某些IP屏蔽某页面的访问

**案例描述：**

使 192.168.31.0/24 网段的用户无法访问/login.html，即无法访问登录页面。

方案：将请求中含有/login.html 的 URI，改写到首页，即/index.html。

拓扑如下：




**配置方法：**

1. 配置 HTTP 防护规则，名称为 1。

   源 IP 配置为：192.168.31.30/24

   URI 路径配置为：/login.html

   速率配置为：0，即每个请求都处理

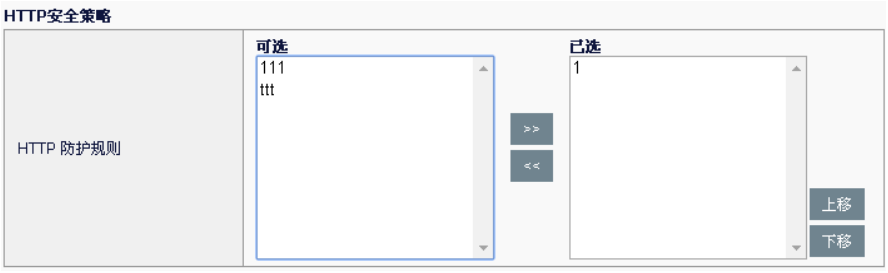
动作选择重写 URI，重写 URI 填写/index.html

2. 配置 HTTP 防护表 111，在 HTTP 防护规则列表中选中 1。
3. 在使用的虚拟服务中引用 HTTP 防护 111。

**配置步骤：**

1. 进入**安全功能>HTTP 防护>HTTP 防护规则**，新建 1，如下图：


2. 进入**安全功能>HTTP 防护>HTTP 防护表**，新建 111，如下图：




3. 所使用的虚拟服务中引用：


4. 192.168.31.0/24 网段的用户，通过浏览器访问/login.html，会发现回应的都是主页/index.html 的内容。

## 68.4 常见故障分析

### 68.4.1 故障现象1：配置应用安全规则，无法触发动作

| | |
|---|---|
| 现象 | 配置了对应的规则，但是无法触发对应的动作 |
| 分析 | 有可能是以下几种情况导致的：<br>1. 对应的虚拟服务中是否引用了该HTTP防护表，以及是否引用了HTTP模板<br>2. 所配置的规则，完整字符串、正则的配置是否合适<br>3. HTTP请求中是否与匹配的规则一致<br>4. 源IP，是否符合<br>5. 速率非0时，计算的是符合规则的请求，而不是所有的请求 |
| 解决 | 应在虚拟服务中引用HTTP防护，并且需同时引用了某个HTTP模板才能生效。<br>检查配置的规则是否正确。 |

# 69 第69章 HTTP 浪涌保护

## 69.1 HTTP浪涌保护概述

在实际的应用中，服务器经常会达到自己的连接上限，这样就会出现响应慢、无法响应、返回出错等等问题，用户体验比较差。

这样就提出了 HTTP 浪涌保护，可以把发送给服务器的请求连接数控制在合理范围，同时不会对后续的请求做丢弃处理，能够提供一个最佳的响应时间。

该功能将超过服务器限制的请求暂存，等到服务器有空闲的连接时，再将这些请求送到服务器。

该模块是在 HTTP 防护表中引用的。

## 69.2 HTTP浪涌保护配置

由两部分组成 HTTP 浪涌保护、服务池的服务成员。

### 69.2.1 配置HTTP浪涌保护

**配置步骤：**

1. 进入**安全功能>HTTP 防护>HTTP 浪涌保护**，如下图：


**新建：**添加一个 HTTP 浪涌保护。

：删除掉该规则。

点击对应的名称，即可对原有的配置进行编辑。

2. 点击**新建**,如下图：


**名称：**HTTP 浪涌保护的名称

**源 IP：**源 IP 地址。

**IP：**输入的可以是单个 IP，例如 10.1.1.1，也可以是子网，例如 10.1.1.0/24, 2010::/64。支持 IPv4 和 IPv6。

**地址对象：**下拉选择已经配置的地址对象。关于地址对象的配置，可以参照“地址对象”相关章节。

**Host：**请求中的 Host，下拉包括任意匹配、条件匹配

**任意匹配：**该项匹配成功，即不做处理

**条件匹配：**规则类型下拉，包括完整字符串、正则。添加后在 **Host 列表**中显示，列表中带有(regex)前缀表示为正则

**URI 路径、Cookie、头域名称：**配置方式与 Host 相同

**优先级：**对满足上面配置的请求，按照哪个优先级进行处理。

**高优先级：**该级别的请求会最先发送

**低优先级：**该级别的请求会最后发送

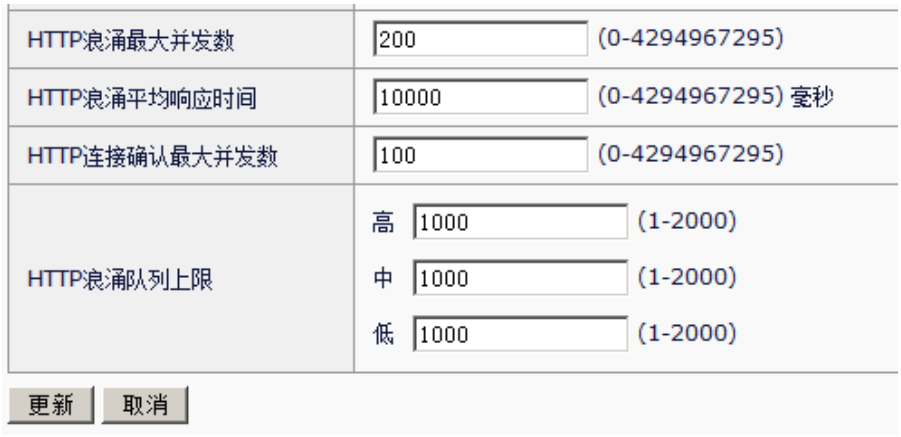

提示

中优先级，在 HTTP 防护表中有介绍

### 69.2.2 配置服务成员参数

要使 HTTP 浪涌生效，还需配置**服务器负载>服务池>服务池>服务成员**中的参数。

**配置**中选择**高级**，相关参数如下：




**HTTP 浪涌最大并发数：**到服务器的并发数，超过该值，则启用浪涌保护。

**HTTP 浪涌平均响应时间：**服务器响应请求的平均时间，超过该值，则启用浪涌保护。

提示

服务器实际响应请求的平均时间，超过设定的 HTTP 浪涌平均响应时间后，设备系统会自动降低并发阈值，直到服务器响应请求的平均时间降低到设定值以下，并发阈值才会慢慢上升到设定并发阈值。

**HTTP 浪涌队列上限：**三个优先级队列可容纳的最大请求数。

提示

当服务器端的并发连接达到 HTTP 浪涌最大并发数阈值时，设备只对后续新建连接中的 HTTP 请求进行优先级入队，已建长连接中的多个请求，直接通过已建连接转发，并不会进入队列。

## 69.3 配置案例

### 69.3.1 配置案例1：通过浪涌减轻服务器压力

**案例描述：**

当服务器连接数超过设定的并发阈值时，对客户端发往服务器的新建请求进行浪涌保护，将访问/login.html 的请求放入高优先级队列，其他请求放入中优先级队列，以减轻服务器压力。

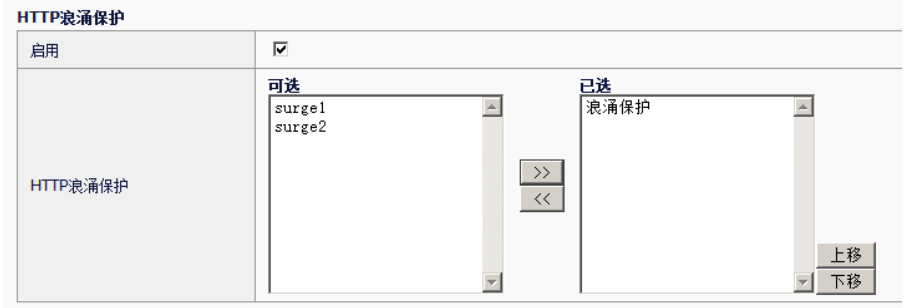
**配置步骤：**

1. 进入**安全功能>HTTP 防护>HTTP 防护规则**，新建 111

URI 路径配置为：/login.html

优先级为：高优先级


2. 进入**安全功能>HTTP 防护>HTTP 防护表**，浪涌保护启用并选择 111，如下图：




3. 所使用的虚拟服务中引用：

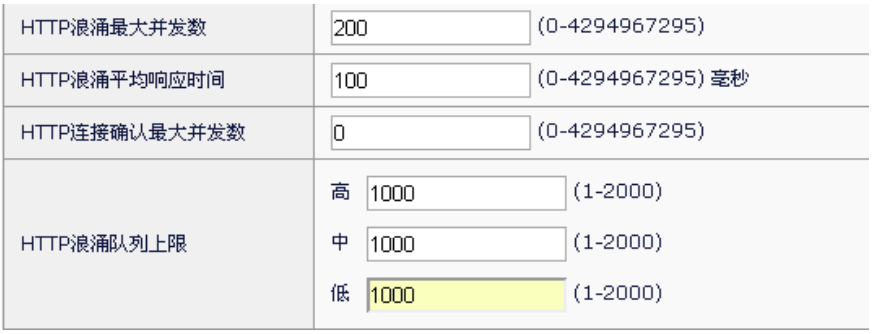

4. 设置服务成员参数

并发数设为 200，超过该值的请求就进入浪涌队列

响应时间设为 100 毫秒，响应超过该值后，后续请求进入浪涌队列。

队列上限都设为 1000。

具体如下图：




5. 大并发访问服务器，查看到服务器的连接数。

## 69.4 常见故障分析

### 69.4.1 故障现象1：配置浪涌保护，无法生效

| | |
|---|---|
| 现象 | 配置了对应的规则，但是无法触发对应的动作 |
| 分析 | 有可能是以下几种情况导致的：<br>1. 对应的虚拟服务中是否引用了该HTTP防护表，以及是否引用了HTTP模板<br>2. 所配置的规则，完整字符串、正则的配置是否合适<br>3. HTTP请求中是否与匹配的规则一致<br>4. 源IP，是否符合<br>5. 服务成员的参数是否符合 |
| 解决 | 应在虚拟服务中引用HTTP防护，并且需同时引用了某个HTTP模板才能生效。<br>检查配置的参数是否正确。 |

# 70 第70章 HTTP 连接确认

## 70.1 HTTP连接确认概述

在 web 服务器的实际应用中，某些情况下用户的请求页面并不能及时得到响应，比如后台服务器处理请求时间较长、或者服务器目前繁忙无法立即响应等，导致用户长时间处于空白页面的等待状态、或者连接失败的状态。

针对这些情况，为了提供更好的用户体验，就可以使用 HTTP 连接确认，该模块主要功能是：

- 当服务器连接数较高时，设备给用户返回“服务器繁忙，请等待 N 秒后再次重试”的提示页面，直到服务器恢复正常。
- 当服务器返回应答时间较长时，设备给用户返回“正在处理中、请耐心等待”的中间提示页面，直到后台服务器完成服务。

连接确认主要的目的是改善用户体验、减少用户因等待时间过长造成的流失，本身有一定的适用性。

## 70.2 HTTP连接确认配置

由以下几部分组成。

### 70.2.1 配置HTTP连接确认配置

**配置步骤：**

1. 进入**安全功能>HTTP 防护>HTTP 连接确认>配置**，如下图：


**新建：**添加一个 HTTP 连接确认配置。

：删除掉该规则。

点击对应的名称，即可对原有的配置进行编辑。

2. 点击**新建,**如下图：


**名称：**HTTP 连接确认的名称

**源 IP：**源 IP 地址。

**IP：**输入的可以是单个 IP，例如 10.1.1.1，也可以是子网例如 10.1.1.0/24, 2010::/64。支持 IPv4 和 IPv6。

**地址对象：**下拉选择已经配置的地址对象。关于地址对象的配置，可以参照“地址对象”相关章节。

**Host：**请求中的 Host，下拉包括任意匹配、条件匹配

**任意匹配：**该项匹配成功，即不做处理

**条件匹配：**规则类型下拉，包括完整字符串、正则。添加后在 **Host 列表**中显示，列表中带有(regex)前缀表示为正则

**URI 路径、Cookie、头域名称：**配置方式与 Host 相同

**确认类型：**指的是按哪种方式就行回应，下拉选择两种方式：

**并发数：**通过设置并发数的方式，来返回页面


**回应页面：**下拉选择该模式下的模板，具体模板配置随后一节介绍

**失效时间：**连接确认返回页面中提示可重试的等待时间

**超时：**通过超时的方式，来返回页面


**回应页面**：下拉选择该模式下的模板，具体模板配置随后一节介绍。

**超时时间**：等待服务器响应页面的超时时间。

**重试次数**：服务器响应超时后，再次请求 uri 的重试次数。

**重试间隔**：请求 uri 重试之间的间隔时间。


必须配置一条 URI 路径

## 70.2.2 配置HTTP连接确认模板

**配置步骤：**

1. 进入**安全功能>HTTP 防护>HTTP 连接确认>配置**，如下图：


**新建**：添加一个 HTTP 连接确认模板。

：删除掉该模板。

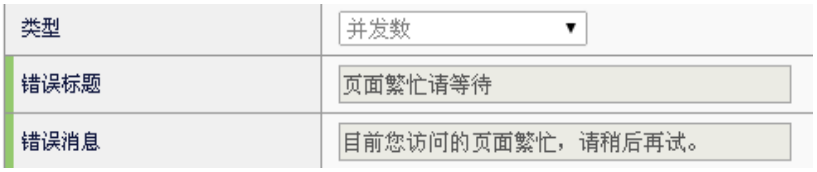
点击对应的名称，即可对原有的配置进行编辑。

2. 点击**新建,**如下图：


**名称：**HTTP 连接确认模板的名称

**类型：**回应页面的类型，下拉选择，包括两个：

**并发数：**并发数方式的回应页面




**错误标题：**返回页面的错误标题

**错误消息：**返回页面的错误消息

**并发数：**并发数方式的回应页面


**超时标题：**返回页面的超时标题

**超时消息：**返回页面的超时消息

**错误标题：**返回页面的错误标题

**错误消息：**返回页面的错误消息


提示

两种方式各有一个参照的模板

### 70.2.3 配置服务成员参数

要使 HTTP 浪涌生效，还需配置**服务器负载>服务池>服务池>服务成员**中的参数。

**配置**中选择**高级**，相关参数为：

**HTTP 连接确认最大并发数：**启用连接确认的服务器并发数阈值，超过该值则启用。

## 70.3 配置案例

### 70.3.1 配置案例1：通过并发数的方式回应页面

**案例描述：**

通过并发数方式，对访问/login.html 的请求进行控制，超过并发数则给客户端浏览器回应一个页面。

**配置步骤：**

1. 进入**安全功能>HTTP 防护>HTTP 连接确认**，新建 111

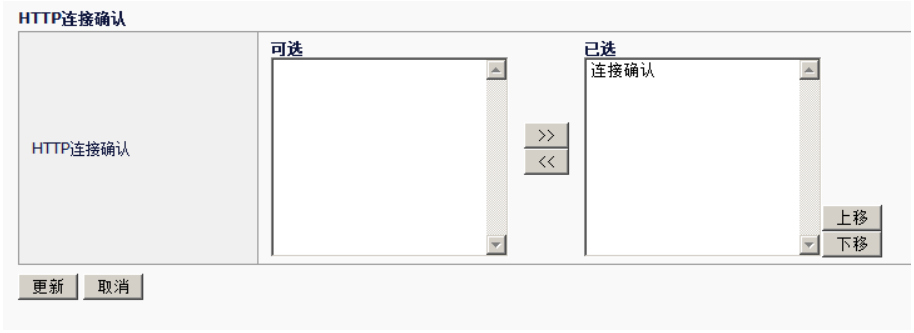
   URI 路径配置为：/login.html

   确认类型：并发数

   回应页面：使用默认的模板 maxlimit

   失效时间：10 秒


2. 进入**安全功能>HTTP 防护>HTTP 防护表**，连接确认中选择 111，如下图：




3. 所使用的虚拟服务中引用：


4. 设置服务成员参数

HTTP 连接确认最大并发数设为 100，超过该值的请求就会触发回应页

面

5. 大并发访问服务器，查看到服务器的连接数，并查看浏览器的页面。

## 70.4 常见故障分析

### 70.4.1 故障现象1：配置连接确认，无法生效

| | |
|---|---|
| 现象 | 配置了对应的规则，但是无法触发对应的动作 |
| 分析 | 有可能是以下几种情况导致的：<br>1. 对应的虚拟服务中是否引用了该HTTP防护表，以及是否引用了HTTP模板<br>2. 所配置的规则，完整字符串、正则的配置是否合适<br>3. HTTP请求中是否与匹配的规则一致<br>4. 服务成员的参数是否符合 |
| 解决 | 应在虚拟服务中引用HTTP防护，并且需同时引用了某个HTTP模板才能生效。<br>检查配置的参数是否正确。 |

# 71 第71章 系统配置

## 71.1 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：

1. 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。
2. 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。
3. 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。
4. 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。
5. 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。
6. 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。
7. 问题反馈。填写问题反馈的收件人及反馈内容。
8. 设备重启。可以重启设备或者恢复出厂配置并重启设备。
9. 设备运行状态记录。包括设备运行记录配置、设备运行记录日志导出、系统运行记录导出三项。主要用于对设备运行的健康状态进行记录。

## 71.2 配置说明

### 71.2.1 配置设备

**配置步骤：**

进入**系统管理>配置>设备**


**IPv4 地址/掩码：**设备的管理地址，即 mgt 接口地址。

**IPv6 地址/前缀：**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。

**本地 HTTPS 服务证书：**该选项的默认值为默认证书，可以通过下拉菜单的方式选择本地证书作为本地 HTTPS 证书。在使用 HTTPS 方式访问设备时，设备将把该证书提供给客户端用于客户端验证设备身份。

**HTTPS 客户端认证:**若使用该功能，需要在 web 页面的小方框中打勾表示启用该功能。同时可以在下拉框里选择相应的 CA 证书。该功能需要与本地 HTTPS 服务证书结合使用，完成客户端和设备之间的双向认证。

**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，一个管理员同时只能在一台 pc 上登录。

**页面超时时间：**在 web 无操作的情况下，超过该设置的时间，登录用户会自动退出。缺省为 10 分钟。

**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：**

1. 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。
2. 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。**
3. 配置**主机名称**，默认为 host。
4. 如果需要实时保存配置，勾选**实时保存配置**。
5. 如果要限制同一管理员同时在不同 pc 上登陆设备,勾选**管理员唯一性检查**。
6. 输入**页面超时时间**，默认为 10 分钟。
7. 输入**在线管理员**个数。
8. 输入**管理员最大登录重试次数**。
9. 输入**管理员失败登录阻断间隔**。
10. 点击**确定**。

### 71.2.2 系统监控

进入**系统管理>配置>系统监控**


此界面可以设置 CPU 占用率、内存占用率、流量、连接数及报文大小的阈值，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 告警阀值，指业务核平均使用率。
2. 输入内存告警阀值，指共享内存使用率。
3. 输入流量告警阈值。
4. 输入连接数告警阈值。
5. 输入报文大小告警日志。

6. 选择日志类型。本地日志、日志、E-mail 报警。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。

7. 点击**确定**。

### 71.2.3 时间配置

进入**系统管理>配置>时间配置**


**系统时间:** 显示当前的系统时间。

**时区选择:** 配置所在的时区。

**配置方式:** 可以手动配置系统时间，也可以选择 NTP 服务器来同步系统时间。

**配置步骤:**

1. 选择**配置方式**。**手动配置或**与 **NTP 服务器同步**。

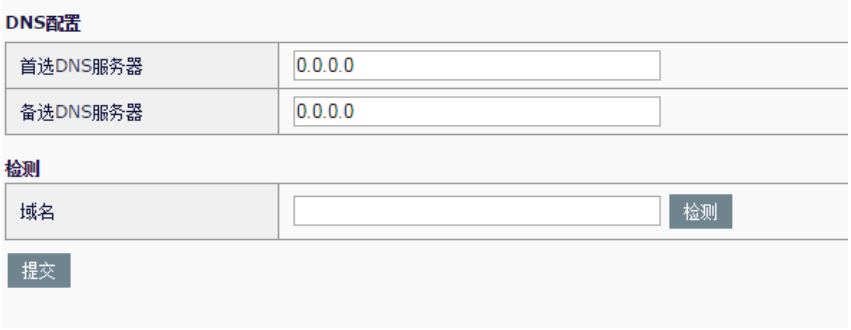
2. 手动配置时，用户自己设定具体的时间。

3. 与 NTP 服务器同步时，需要指定 ntp **服务器**域名及**同步间隔**。有 2 个前提步骤：(1)配置默认路由。(2)配置下节描述的 DNS 配置。

4. 点击**确定**。

### 71.2.4 DNS配置

进入**系统管理>配置>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。**

### 71.2.5 备份恢复

进入**系统管理>配置>备份恢复**


**系统配置导入:** 选择配置文件导入到设备中。

**恢复备份配置到主配置文件:** 设备内的备份配置覆盖主配置。

**系统配置导出:** 将设备中的配置文件导出。

**拷贝主配置文件到备份配置文件:** 对设备内的主配置进行备份。

### 71.2.6 告警邮件配置

进入**系统管理>配置>告警邮件配置**


**SMTP 服务器**：邮件服务器地址。

**SMTP 服务器端口**：邮件服务器的端口。

**安全连接**：是否启用安全连接。

**发件人 E-Mail**：发件人邮箱。

**认证**：是否启用邮件认证。

**SMTP 用户**：发件人邮箱登陆用户名。

**密码**：发件人邮箱登陆密码。

**测试邮件地址**：发送测试邮件到该地址，检测地址是否可达。

**最短发送间隔**：E-mail 日志消息最短发送的间隔时间，配置范围 1-60 分钟。

**收件人 E-Mail**：收件人邮箱地址。多个邮箱地址用分号隔开。

**配置步骤**：

1. 输入 **SMTP 服务器**。
2. 输入 **SMTP 服务器端口**号，缺省为 25。
3. 如果 SMTP 服务器需要安全连接，勾选上启用**安全连接**。

4. 输入**发件人 E-Mail** 地址。
5. 如果您的 SMTP 服务器需要认证，勾选上启用**认证**。
6. 输入 **SMTP 用户**。
7. 输入邮箱登录**密码**。
8. 填写日志信息**最短发送间隔**。
9. 填写日志信息**收件人 E-Mail**。
10. 点击**确定**。

### 71.2.7 问题反馈

**配置步骤：**

进入**系统管理>配置>问题反馈**


**收件人:**收件人邮箱地址。

**抄送:**邮件抄送地址。

**标题:** 邮件标题。

**问题描述:**本次反馈的问题描述。

**联系人:**联系人姓名。

**联系地址:**联系人地址。

**联系电话:**联系人电话。

设备信息提取：是否将设备配置及运行信息打包反馈给抄送和收件人

**配置步骤：**

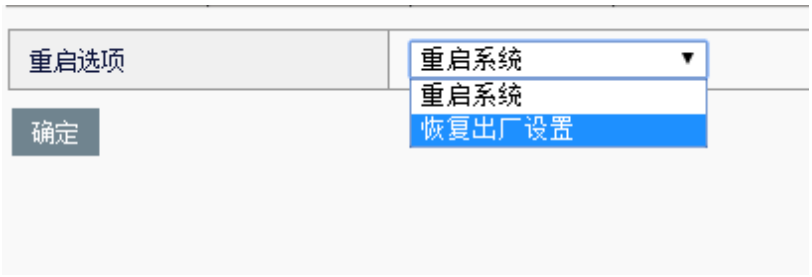
配置前提，必须配置上节描述的**告警邮件配置**，且告警邮箱可成功发送测试邮件。

1. 输入**收件人**邮箱地址。
2. 选择输入**抄送**地址。

3. 填写**联系人姓名，地址和联系方式**。
4. 输入**标题**。
5. 输入**问题描述**。
6. 根据需要是否勾选设备信息提取单选框
7. 点击**确定**。

### 71.2.8 设备重启

进入**系统管理>配置>设备重启**




该界面可以重启设备或者恢复出厂设置并重启设备。

### 71.2.9 设备运行状态记录

**1.** 进入**系统管理>配置>设备运行状态记录>配置**


**参数说明：**

**记录设备运行状态：**该功能是否使能。

**生成间隔：**多长时间记录一次信息，包括流量信息、接口信息、版本信息等。每天形成一个以日期为名称的新日志文件

**保存时间：**记录几天。若配置的是 3，代表记录连续 3 天的文件，即在磁盘中保存 3 个日志文件。新形成的文件会覆盖形成时间最早的文件。

**配置步骤：**

1. 选中记录设备运行状态。
2. 设置生成间隔，默认 3600 秒。

3. 设置保存时间，默认 7 天。
4. 点击**提交**。


该功能只能在有磁盘的设备上使用。

### 71.2.10 导出设备运行记录

**配置步骤：**

1. 进入**系统>配置>设备运行记录>导出**，如下图：


**参数说明：**

**日志文件导出：**导出某一天及某几天的日志文件。

**系统运行日志导出：**导出系统运行日志。

## 71.3 管理员

### 71.3.1 管理员概述

ADC 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，支持使用 ACS 服务器进行用户认证及授权。

（1）可以把用户名添加到 ADC 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。

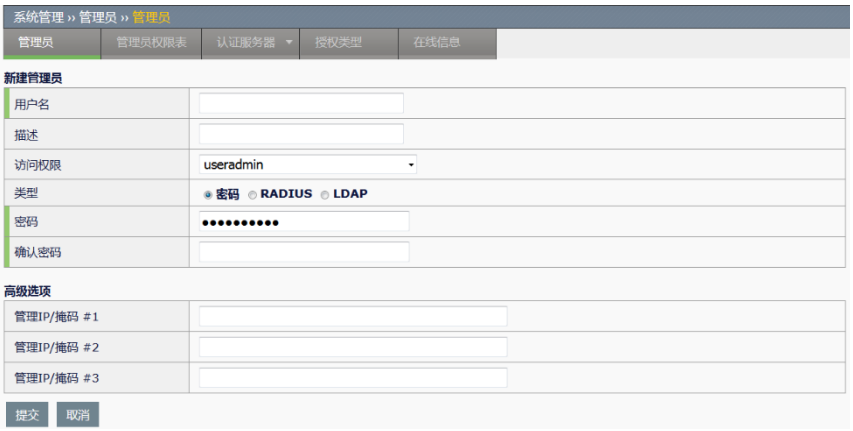
（4）可以配置远程服务器认证授权，用户输入的用户名和密码发送给远程服务器认证，认证通过后服务器下发授权获取相应权限。

## 71.3.2 配置管理员

**配置管理员**

配置用于认证的管理员用户。

进入**系统管理>管理员>管理员**




**用户名：**管理员的名称。

**描述：**对管理员的描述。

**访问权限：**管理员使用的访问权限列表，默认的权限表有 admin、useradmin、readadmin 三项，已配置的自定义权限表也可以在此处被选择。

**类型：**管理员认证的类型，包括密码、RADIUS、LDAP。

注意

**密码：**选择该域表示对于创建的用户，其用户名和密码都保存在本地，然后在**密码**和**确认密码**中输入你设置的本地用户的密码。

**RADIUS：**选择该域表示对于创建的用户，本地只保存用户名，不保存密码，用户需要到指定的 RADIUS 服务器上去认证，该用户需要在 radius 服务器上存在。下拉列表中列出了当前已经配置了的 RADIUS 服务器。

**LDAP：**选择该域表示对于创建的用户，本地只保存用户名，不保存密码，用户需要到指定的 LDAP 服务器上去认证，该用户需要在 ldap 服务器上存在。下拉列表中列出了当前已经配置了的 LDAP 服务器。

**管理 IP/掩码 #1：**允许哪些网段的用户登录。

**管理 IP/掩码 #2：**允许哪些网段的用户登录。

**管理 IP/掩码 #3：**允许哪些网段的用户登录。

### 71.3.3 配置RADIUS服务器

如果您配置了 RADIUS，当某个用户被配置为要求使用 RADIUS 服务器认证的时候，ADC 将连接 RADIUS 服务器以获得认证。

**配置 RADIUS 服务器**

进入**系统管理>管理员>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

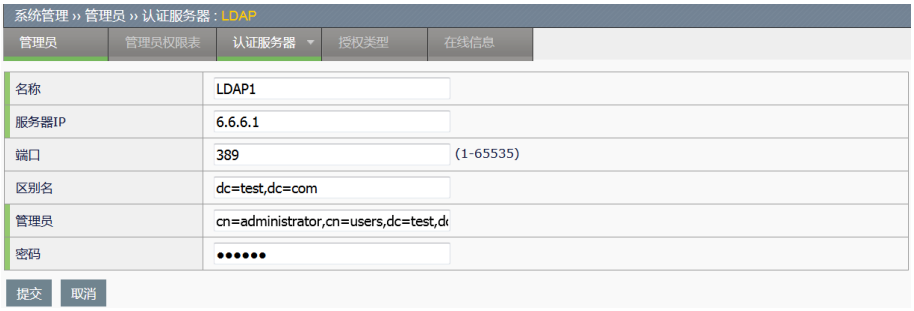
点击**认证服务器**下的 **RADIUS 配置**标签页，显示当前系统中配置的所有 RADIUS 服务器。

### 71.3.4 配置LDAP服务器

如果您配置了 LDAP，当某个用户被配置为要求使用 LDAP 服务器认证的时候，ADC 将连接 LDAP 服务器以获得认证。

**配置 LDAP 服务器**

进入**系统管理>管理员>认证服务器>LDAP**，点击**新建**




**名称**：LDAP 服务器名称，标识 LDAP 服务器。

**服务器 IP**：LDAP 服务器的 IP 地址。

**端口**：LDAP 服务器用于认证的端口。缺省为 389

**区别名：**用来指明在 LDAP 服务器上查找数据的起始位置。如，ldap 服务器上，在路径 test.com 中，容器 users 下有用户 user2。则区别名中配置为”dc=test，dc=com”。

**管理员：**LDAP 服务器的管理员用户。如，登陆 ldap 服务器的系统用户名为 administrator，密码为 111111，且该系统用户也存在于 ldap 服务器下，处于 test.com 中容器 users 下。则此管理员配置为”cn=administrator,cn=users,dc=test,dc=com”密码为”111111”。

**密码：**LDAP 服务器的管理员密码。


点击**认证用户**下的 **LDAP** 标签页，显示当前系统中配置的所有 LDAP 服务器。

### 71.3.5 配置管理员授权类型

可以对管理员的授权类型进行选择，若选择本地认证授权，则由设备进行认证并为该管理员下发授权，若选择远程授权，则由配置的某个 RADIUS 对管理员进行认证并授权，通常和第三方认证授权服务器如 cisco 的 ACS 服务器配合使用。

**配置本地授权**

进入**系统管理>管理员>授权类型**，默认为本地授权，不需要进行配置。


**配置远程授权**

进入**系统管理>管理员>授权类型**，选择服务器授权。


**RADIUS 认证类型：**选择本地授权还是服务器授权。

**ACS 主服务器：**对管理员登陆进行认证和授权的服务器。

**ACS 备用服务器：**可以选择不填，也可以在下拉框里选择一个除主服务器

外的其他服务器作为备用服务器。当主服务器认证失败的时候，会将管理员信息发往备用服务器进行认证授权。

**重播次数：**指当主 ACS 服务器没有回应时，最大尝试次数。

**应答超时时间：**单位是秒，将信息发往主 ACS 服务器后，设备等待的时间，超过这个时间没有回应，设备才进行重传。

**重置：**将现有配置还原为默认值。

配置完成之后点击确定。


配置授权类型为服务器授权后，若用户再本地管理员中能查到则匹配本地认证，若查询不到，才会匹配服务器授权转发到授权服务器去认证。

## 71.3.6 认证用户监控与维护

### 查看管理员信息

进入**系统管理>管理员>管理员**，查看管理员信息。


可以查看用户的用户名，管理地址，访问权限，描述。

### 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。


可以查看 RADIUS 服务器名称，服务器 IP，端口。

### 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。

可以查看 LDAP 服务器名称，服务器 IP，端口，区别名。

**查看在线管理员信息**

**进入系统管理>管理员>在线信息，**查看在线管理员信息。


**可以**查看在线的管理员信息，阻断的管理员用户。

### 71.3.7 配置案例1

**案例描述：**

当前设备的管理员密码信息存在在 radius 服务器上，管理员用户需要到 radius 服务器上进行认证。

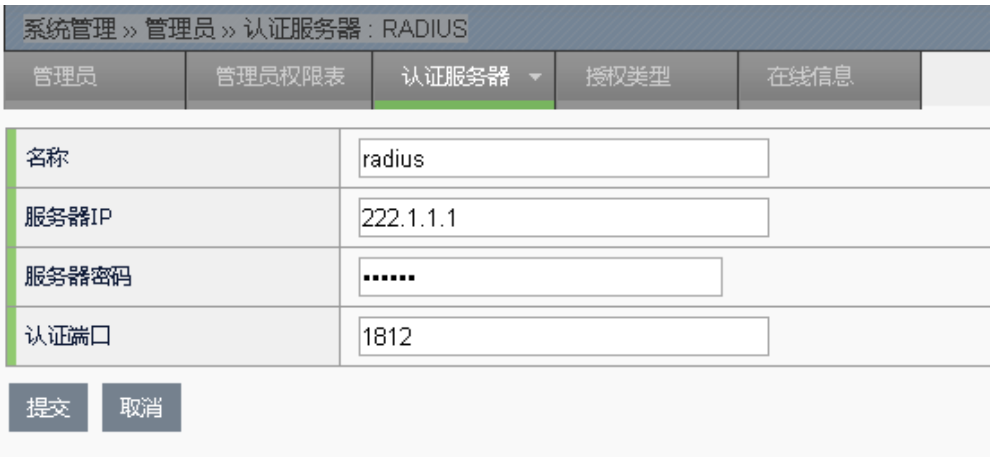
**配置步骤：**

radius 服务器配置方法：

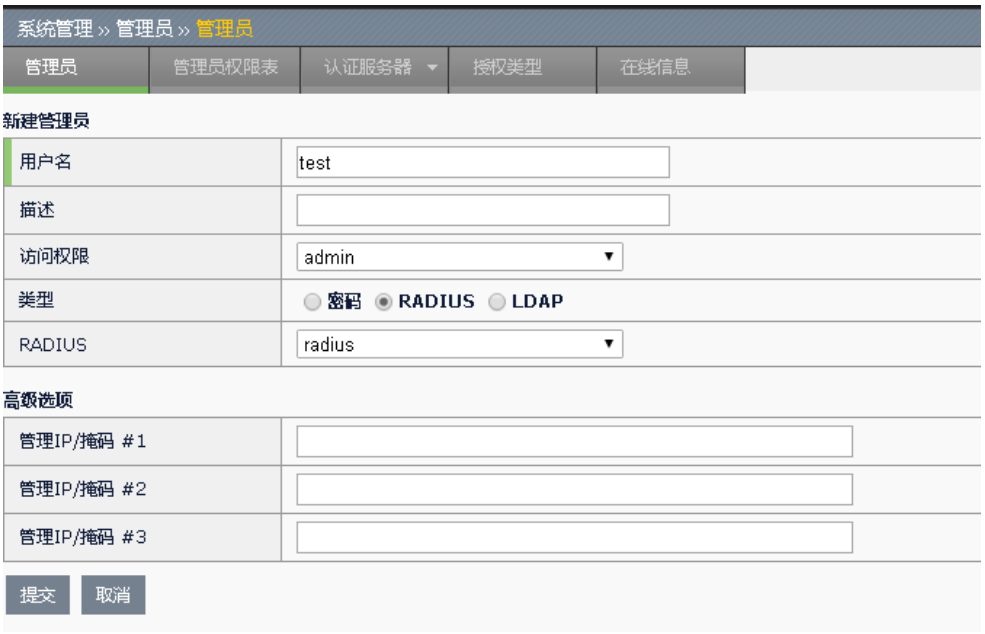
1、 Radius 服务器上添加用户 test，并设置 radius 密钥。

ADC 设备配置方法：

1、 进入**系统管理 ›› 管理员 ›› 认证服务器 ：RADIUS** 页面，添加 radius 服务器，服务器 IP 地址填写 ACS 服务器地址，服务器密码保持和 radius 服务器的密钥一致。




2、 进入**系统管理 ›› 管理员 ›› 管理员**页面，添加管理员用户 test，类型为 radius，选择 radius 服务器为 radius。




3、 进入**系统管理 ›› 管理员 ›› 授权类型**页面，授权类型配置为本地授权。


## 71.3.8 配置案例2

**案例描述：**

当前网络中所有设备的管理员认证及授权需要通过 ACS 服务器集中下发，便于对网络中的管理员用户的统一管理。管理员用户为：testadmin，需要授予超级管理员权限。

**配置步骤：**

ACS 服务器配置方法：

1、 在 ACS 服务器上配置 radius 扩展字段，属性字典中加入私有属性：添加厂商 venus，vendor ID 配置为 25510

2、 在 ACS 服务器上配置添加 ADC 设备并设置 radius 密码

3、 添加 testadmin 用户，该用户授权 ID 通过私有属性下发，下发值设置为 20

ADC 设备配置方法：

1、配置认证服务器

**进入系统管理 ›› 管理员 ›› 认证服务器：RADIUS** 页面，添加主和备认证服务器，服务器 IP 填写 ACS 服务器地址，服务器密码保持和 ACS 服务器配置添加设备时配置的密码一致：


**2**、开启服务器授权功能

**进入系统管理 ›› 管理员 ›› 授权类型**页面，选择认证类型为服务器授权，并配置选择进行认证的主、备认证服务器。


## 71.3.9 常见故障分析

**故障现象：系统用户使用 radius 认证失败**

| | |
|---|---|
| 现象 | 使用radius用户登陆ADC系统失败。 |
| 分析 | 1. 密码错误<br>2. RADIUS服务器配置错误（比如：共享密钥，IP等）<br>3. RADIUS服务器连接不上（比如：PING不通）<br>4. RADIUS服务器上没有这个用户 |
| 解决 | 1. 检查用户密码，输入正确的用户名和密码<br>2. 修改该RADIUS服务器的配置<br>3. 首先确保ADC和RADIUS服务器能通讯，能PING通<br>4. 为该RADIUS服务器添加该用户 |

**故障现象：用户远程认证失败**

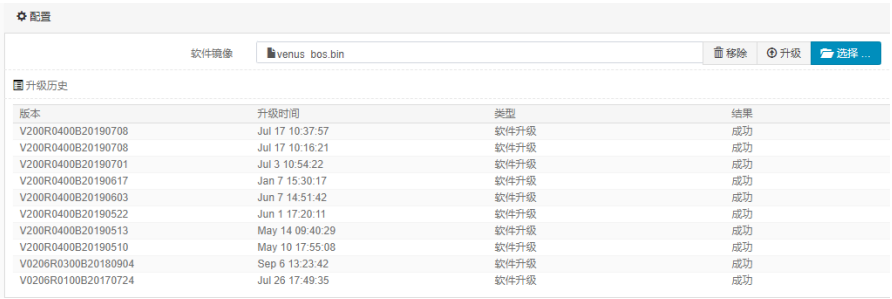
| | |
|---|---|
| 现象 | 使用远程服务器上存在的用户认证失败。 |
| 分析 | 1. 确认是否开启了服务器授权 |

| | | |
|---|---|---|
| | 2. | 确认认证用户名在设备本地是否存在 |
| | 3. | 确认输入的用户名密码是否和服务器配置一致 |
| | 4. | 确认该用户名在服务器上配置下发的授权ID在ADC设备上存在 |
| | 5. | 确认ADC设备和ACS服务器网络通信是否正常 |
| | 6. | 确认添加的radius服务器密码和ACS服务器添加设备时的密码是否一致 |
| 解决 | 1. | 授权类型选择服务器授权 |
| | 2. | 若用户名在本地存在会使用本地认证方式，使用本地不存在的用户名进行认证 |
| | 3. | 检查用户密码，输入正确的用户名和密码 |
| | 4. | 确保服务器下发的授权ID在设备的管理员权限表下存在 |
| | 5. | 确保ADC设备和ACS服务器之间能正常通信 |
| | 6. | 确保radius服务器密码和ACS服务器添加设备时的密码一致 |

# 71.4 版本管理

## 71.4.1 版本管理

1. 进入**系统管理>版本管理：**




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：**

1. 通过**选择**需要的升级包。
2. 点击**升级**。
3. 根据弹出的提示框，选择**确定**升级或**取消**升级。

## 71.4.2 特征库升级

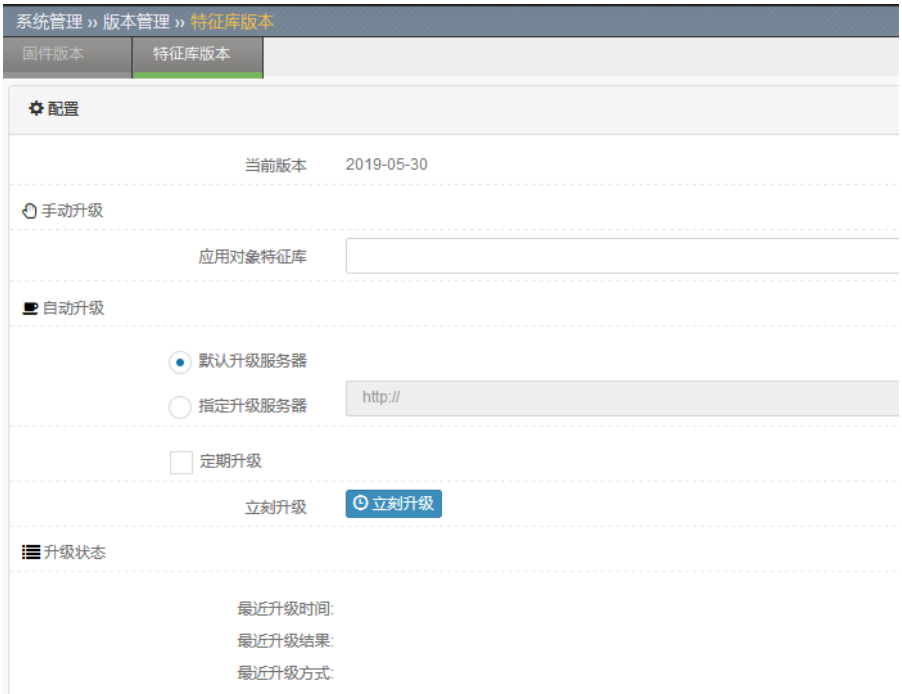
ADC 设备可以手动、自动升级应用特征库版本。

该特征库是“应用引流”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 出厂时，已经默认加载了最新版本的特征库。

选择**系统管理**->**版本管理**->**特征库版本**，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

提示 采用手动升级功能时，需要保证升级文件为合法的特征库文件。

**自动升级：**

**默认升级服务器:** 升级服务器设为默认升级服务器。

**指定升级服务器:** 设置升级服务器地址。

**定期升级:** 启用定期自动升级。

**每周:** 设置每周星期几。

**每月:** 设置哪些月份。

**时间:** 每次自动升级的当天时间。

配置好后，点击**提交**。

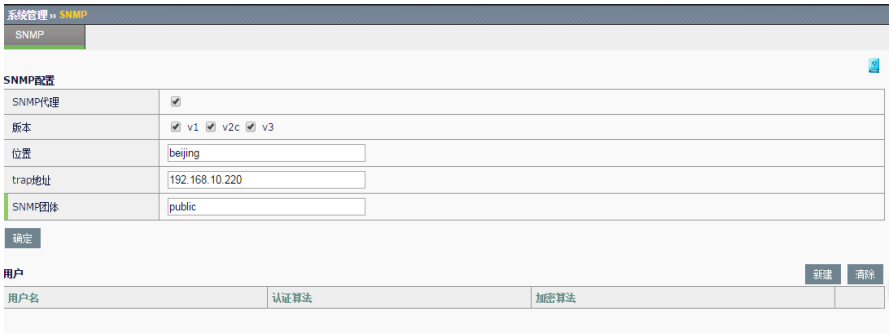
**立即升级：**启用立即自动升级。

## 71.5 SNMP

### 71.5.1 配置SNMP

**配置步骤：**

1. 进入**系统管理>SNMP：**




**SNMP 代理：**选中为启动 SNMP 代理。

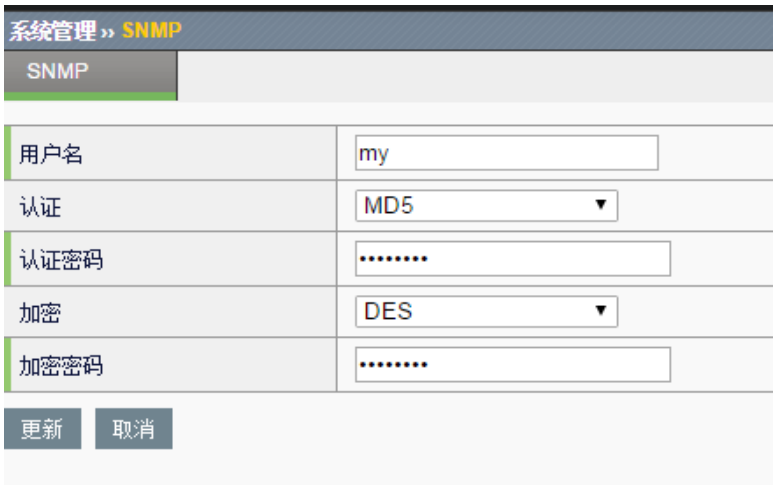
**版本：**选择是否启用 v1、v2c、v3 版本的 SNMP。

**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。

**配置步骤：**

1. 勾选启用 **SNMP 代理。**
2. 选择是否启用 **v1、v2c、v3** 版本的 SNMP
3. 输入**位置**。
4. 输入 **trap 地址**。
5. 输入 **SNMP 团体**。
6. 点击**确定**。
7. 如果是 V3 版本需要用户认证，点击**新建**。
8. 在弹出框中配置**用户名**、**认证**方式、**认证密码**、**加密方式**、**加密密码**。
9. 点击**更新**。

### 71.5.2 配置案例

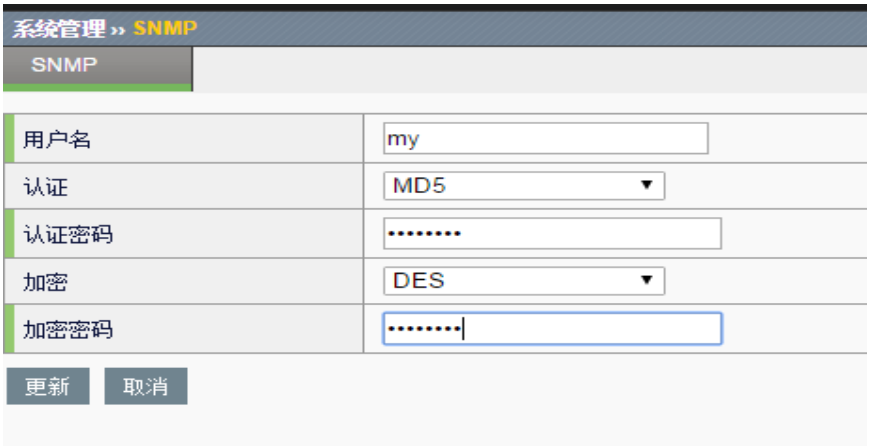
配置案例：配置 SNMP

**案例描述:**

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

**配置步骤：**

1. 进入**系统管理>SNMP**，配置 v3 认证用户：




2. 输入其他参数，启用 snmp 代理，启用 v3 版本，如下图：


通过如上配置，可以使用 mib browser 等 snmp 客户端工具访问设备的 snmp 功能，在该工具上要配置相应的 snmp v3 用户信息，可获取设备相应信息。

默认 snmp 客户端工具中自带 RFC1213 mib 库，若要读取 VENUSTECH 设备私有信息，需要导入公司私有 mib 库文件。

# 72 第72章 许可管理

## 72.1 许可管理概述

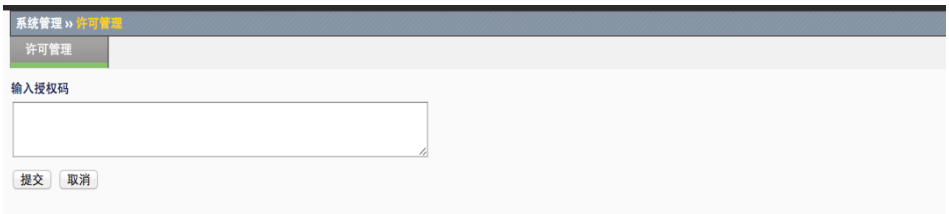
ADC 设备的一些附加模块受许可(license)管理控制，如果没有导入许可，这些模块将无法配置及生效。目前受许可管理的模块包含：**HTTP 内容交换，应用加速，智能 DNS，防火墙，HTTP 防护，整机吞吐流量**。


为了保证 ADC 基础业务的正常，在没有导入任何许可的时候，整机吞吐流量缺省按照 1Gbps 授予。

## 72.2 许可导入

选择**系统管理->许可管理**，如下图：


点击“**更新授权**”，将通过通过正常商务渠道获得的授权码粘贴到输入框中：




点击“**提交**”。

提示

如果输入的授权码无效，系统会提示失败。如果输入的授权码生效，返回页面会显示相关模块的许可信息。

## 72.3 许可试用

在“许可管理”中可点击“试用”，可以激活试用授权。试用授权的注意事项请参考点击后弹出的页面。

# 73 第73章 高可靠性

## 73.1 HA概述

高可靠性即 HA（High-Availability），是保证网络高可靠的一种技术方案，应用交付平台支持两台 ADC 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 ADC 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 ADC 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 ADC 上的相关配置，如浮动 IP、虚拟服务等。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 ADC 设备通过用户设置 IP 地址发送心跳报文来检测对端 ADC 的工作状态，同时 ADC 产品支持另外三个附加因素可选项：“网关监控”，“接口监控”和“链路聚合监控”作为切换条件。正在工作中的 ADC 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 ADC 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。

## 73.2 HA基本配置

ADC 设备 HA 的基本配置包括工作模式，心跳地址、单元 ID 等。

**配置步骤：**

进入**系统管理>高可靠性>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，默认设置 ID 为 1。

**抢占模式：**HA 主备模式下的抢占状态。启用后，选择抢占主或抢占备，在监控对象的状态完全正常的情况下，由该选项决定设备的主备状态。默认禁用。

**心跳发送间隔：**两台设备的心跳发送间隔。取值范围 1-3 秒，默认配置为 3 秒。

**浮动 MAC：**当设备发生状态切换时，浮动 MAC 地址也随之切换，始终在主状态设备上生效，从而保证上下游设备看到的浮动 IP 和 MAC 地址总是一一对应的，减少状态切换对上下游设备的影响。默认不启用。

点击**确定**。

注意

1. 两台设备的通信地址必须成对配置，并且不能指定为接口的浮动 IP。
2. 主主模式下，两台设备的单元 ID 必须指定为不同。
3. 主备模式下，两台设备的抢占模式必须成对配置。
4. 两台设备的心跳发送间隔必须配置为相同。

## 73.3 配置配置同步

ADC 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，也支持配置的自动同步。

**配置步骤：**

进入**系统管理>高可靠性>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。

**自动同步：**开启自动同步之后，设备配置就能进行自动同步。

**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。

点击**确定。**

提示

1. 本地和对端地址可以和 HA 通信地址相同，不能指定为接口的浮动 IP。
2. 指定本地和对端地址后，可以在 HA 监控页面进行手动同步配置。
3. 启用实时监测同步状态后，可以在 HA 监控页面查看检测结果。
4. 两台设备中，只要有一台启用实时监测即可。
5. 配置同步功能，不会同步 HA 本身的配置，以及网络配置→接口、网络配置→设备 IP 相关的配置、VRRP、CA 证书相关配置和动态路由配置。

## 73.4 配置连接同步

连接同步包括四层流同步，四层会话保持，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。这里只配置连接同步的地址，连接同步的开启和关闭，分别在虚拟服务和会话保持模块中实现。

**配置步骤：**

进入**系统管理>高可靠性>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

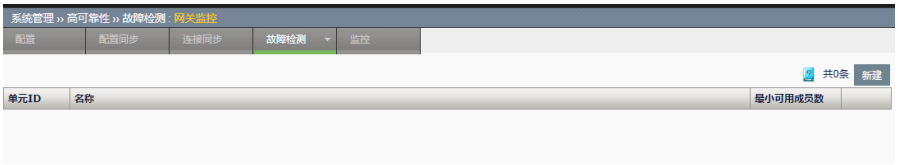
该地址为可选项，当首选地址发送失败时，使用备选通信地址，提高了连接同步的可靠性。如果设备开启了连接同步，当需要同步的连接数量非常大时，会严重影响设备的性能。

## 73.5 配置HA监控

HA 监控分网关监控、接口监控和链路聚合监控，实时监控设备上的运行状况，当出现监控故障时，会引起设备的状态切换，保证业务不中断。

**配置步骤：**

进入**系统管理>高可靠性>故障检测**，进入**网关监控**界面。




点击  **删除**监控。

点击**新建**。


**网关监控：**要监控的网关服务池，该服务池中存放的是设备默认网关的 IP 地址，当服务池配置健康检查后，按照服务池中配置的健康检查算法来检查网关的状态。

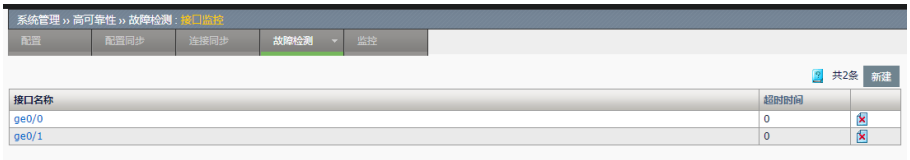
**单元 ID：**单元 ID 在主主模式下使用，标识网关监控所属的设备 ID，当该 ID 与设备的 ID 相同时，监控生效；当该 ID 与设备 ID 不相同时，只在主 A 状态下生效。

**最小可用成员数：**当监控的网关服务池中的正常成员数少于最小可用成员数时，则该监控故障。

1. 选择要监控的服务池
2. 选择监控所属的设备 ID
3. 配置服务池中最小可用成员数
4. 点击**提交**

**配置步骤：**

进入**系统管理>高可靠性>故障检测**，进入**接口监控**界面。




点击 **删除**监控。

点击**新建。**

**接口：**需要监控的物理接口或 vlan 名称，可以监控用户认为重要的所有 vlan 和除了管理口之外的物理接口，监控基于物理接口或 VLAN 的 UP/DOWN。建议监控设备上下游直连的接口，这些接口的故障会造成业务的中断，必须进行故障切换。

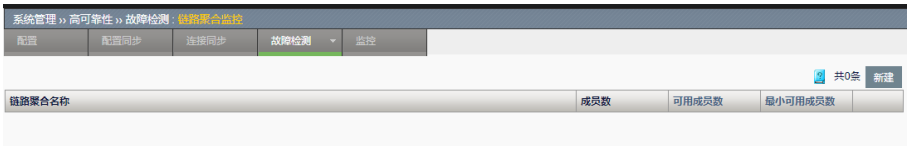
**超时时间：**监控故障后，等待的超时时间，避免接口短时间内多次 up/down，引起 HA 状态频繁切换，造成设备不稳定。

1. 选择需要监控的接口
2. 配置超时等待时间

点击**提交。**

**配置步骤：**

进入**系统管理>高可靠性>故障检测**，进入**链路聚合监控**界面。




点击  **删除**监控。

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。

1. 选择需要监控的链路聚合接口
2. 配置最小可用成员数
3. 点击**提交**

## 73.6 HA状态控制

### 73.6.1 查看HA监视器

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。

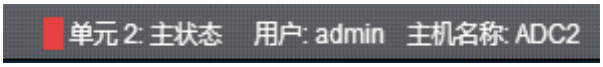
**检测配置：**可以点击该按钮，探测两端配置是否同步。

注意

1. 点击同步配置到对端，一段时间后页面会返回同步结果，此过程中请不要离开页面。
2. 同步配置到对端后，需要不保存配置直接重启对端设备，配置才能生效。
3. 主主模式下不支持主备切换。
4. 主备模式下配置了抢占模式，不支持主备切换。

### 73.6.2 查看HA实时信息

进入 ADC 用户 web 管理控制界面，如果开启了 HA 功能，在界面右下角会显示当前 HA 的状态，单元 ID，配置同步信息。




**说明：**

■ ：显示两端配置是否同步，蓝色：未知，红色：不同步，绿色：同步；

**单元 2：**本设备的单元 ID 号为 2。

**主状态：**显示本设备当前 HA 状态为主。

**用户：**登录本设备的用户名称。

**主机名称：**本设备的主机名称。

## 73.7 配置案例

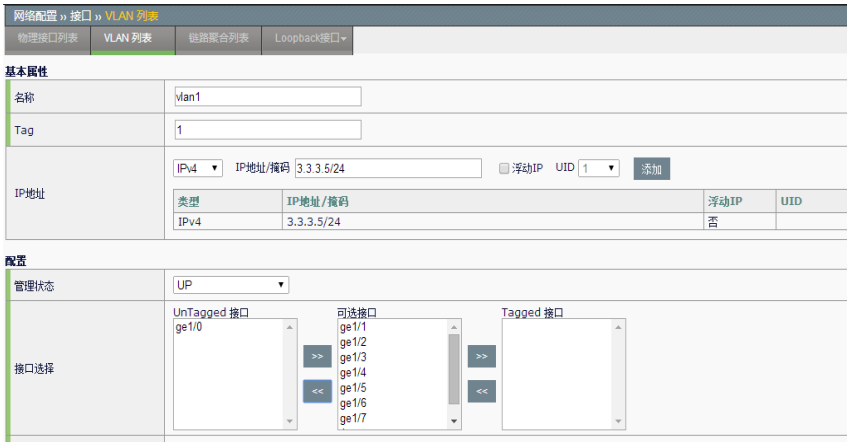
### 73.7.1 案例1：配置主备模式基本配置

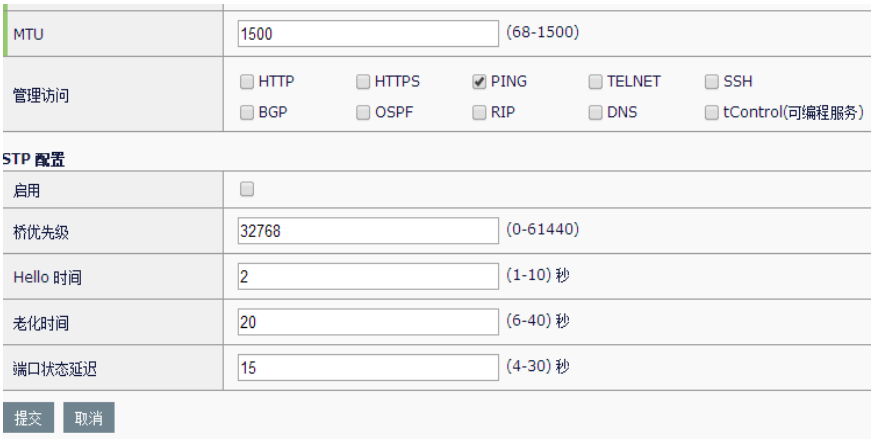
**案例描述：**

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

**配置步骤：**

1. 配置 ADC_A 进入**网络配置>接口**，进入 **VLAN 列表**界面，点击**新建**，配置 HA 所需的接口 IP。



**IP 地址：**配置 IP 地址 3.3.3.5

**掩码：**24 位网络掩码 **Tag**,配置相应 VLAN 号，此处配置为 1 **浮动 IP：**不勾选

**接口选择：**选择相应物理接口以 tag/untag 方式加入 VLAN

其他相关参数请见具体章节

2. 点击**提交**，完成新建设备 **IP3.3.3.5** 重复以上操作创建接口 IP9.9.9.7。创建设备 IP**3.3.3.5** 绑定在 VLAN1 上，设备 IP**9.9.9.7** 绑定在 VLAN2 上，分别用于主备心跳地址。

3. 配置 ADC_A,进入**系统管理>高可靠性>配置**，进入**配置**界面。


**工作模式：**主备模式

**首选通信地址：步骤 1** 和 **2** 中创建的 3.3.3.5 地址，作为本地通信地址，对端设备需要创建 IP 地址 3.3.3.3。

**备选通信地址：**步骤 1 和 2 中创建的 9.9.9.7 地址，作为本地通信地址，对端设备

需要创建 IP 地址 9.9.9.7。

**单元 ID：**配置设备 ID 号为 1。

**抢占模式：**抢占主，本设备优先成为主设备。

**心跳发送间隔：**3 秒，每隔 3 秒发送一次心跳。

4. 配置 ADC_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：3.3.3.3。

**配置同步：**配置自动同步按钮，默认不开启。

**实时监测同步状态：**勾选，实时探测两边的配置是否存在差异。

5. 配置 ADC_A,进入**系统管理>高可靠性**，进入**连接同步**界面。


**首选通信地址：**复用心跳备选通信地址 9.9.9.7 为本地地址，对端设备需要配置设备 IP9.9.9.9。

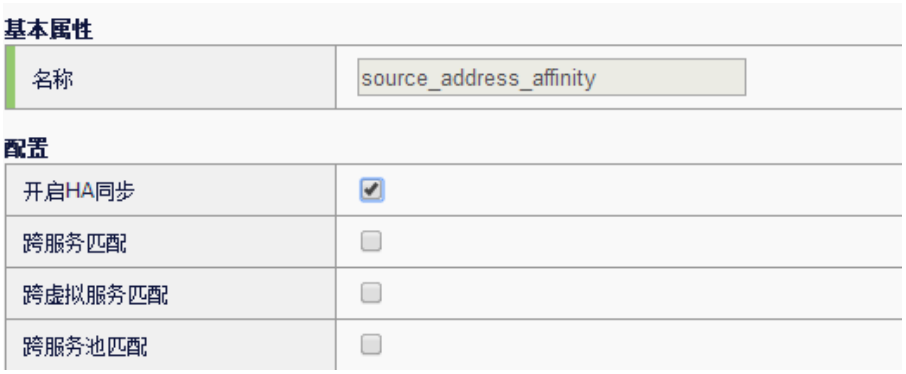
**备选通信地址：**可选配，本实例中没有配置。

6. 配置 ADC_B，配置步骤请参照设备 ADC_A，这里不再重复介绍，以下是设备 ADC_B 配置完成后的配置页面。


到此 HA 主备工作模式配置完成。

7. 如果设备上配置有虚拟服务，需要开启虚拟服务连接同步，才会进行连接同步，进入**链路负载>虚拟链路>虚拟链路**页面，选择需要同步连接的虚拟服务，进入配置页面，勾选 HA 状态同步。


8. 如果设备开启了会话保持，需要开启会话保持同步，才会进行会话保持同步，进入**模板和对象>会话保持**，选择需要开启同步的会话保持，进入配置页面，勾选开启 HA 同步。




9. 查看 HA 监控，进入**系统管理>高可靠性>监控**页面。
10. 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。

以上是 HA 主备模式的配置过程，需要让设备实现业务转发功能，还需要配置虚拟服务，虚拟链路等功能，具体配置步骤请参照对应模块的介绍。

## 73.7.2 案例2：配置主主模式基本配置

**案例描述：**

两台设备，ADC_A,ADC_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，也可以进入配置同步。

**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。
2. 配置 ADC_A，进入**系统管理>高可靠性>配置**，进入**配置**界面。


**工作模式：**选择主主模式；

**首先通信地址：**步骤 1 中配置的地址。

**备选通信地址：**步骤 1 中配置的地址。

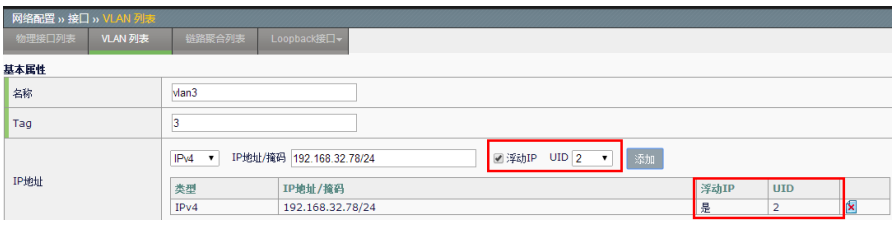
**单元 ID：**设置设备单元 ID 号为 2，两台设备必须不一样。虚拟服务，浮动 IP 也会有自己的 ID 号，只有与设备单元 ID 号相同的虚拟服务，浮动 IP 才会在本设备上生效，否则不会生效。

**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 ADC_A，进入**系统管理>高可靠性**，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 ADC_A，进入**系统管理>高可靠性**，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 ADC_A，如果设备配置了虚拟服务，通过设置虚拟服务 ID 与设备单元 ID 相同，让虚拟服务在本设备生效。进入**服务器负载>虚拟服务>虚拟服务地址列表**，选择需要配置的虚拟服务，进入配置页面，选择 unit ID 为 2。


6. 配置 ADC_A，如果设备配置了浮动 IP，通过设置浮动 IP 的 ID 与设备单元 ID 相同，让浮动 IP 在本设备生效。进入**网络配置>接口>VLAN 列表**，选择需要配置的浮动 IP。




7. 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：**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。

8. 配置 ADC_B，配置步骤请参照设备 ADC_A，这里不再重复介绍，以下是设备 ADC_B 配置完成后的配置页面。


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，还需要配置虚拟服务，虚拟链路等功能，具体配置步骤请参照对应模块的介绍。

注意

主主模式下，设备通过单元 ID，区分两台设备上的业务和配置，如果配置不正确，会造成业务无法正常工作。在修改设备单元 ID 时，对应的浮动 IP，虚拟服务的 ID 也需要修改。

### 73.7.3 案例3：配置虚拟服务会话保持同步

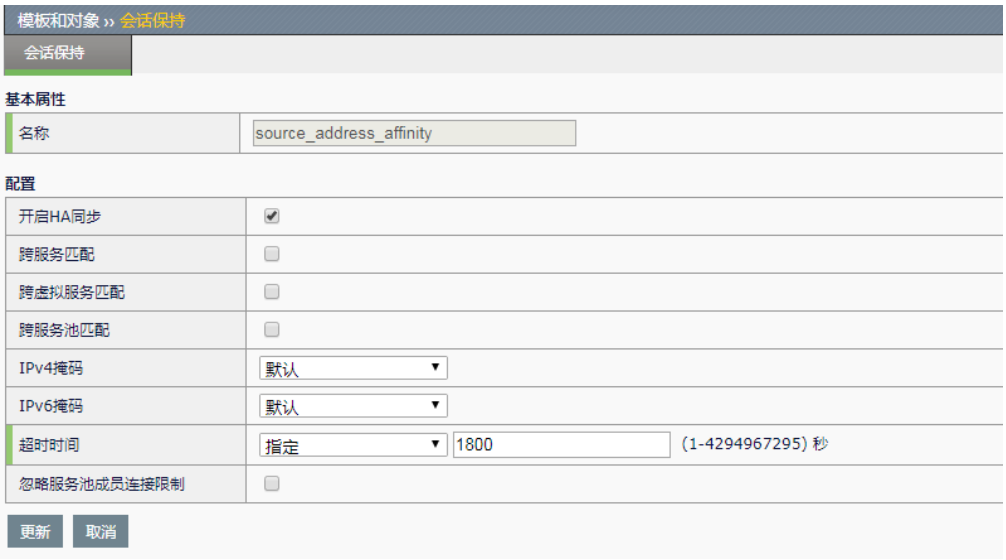
**案例描述：**

两台设备，ADC_A,ADC_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，配置虚拟服务 vs1，开启会话保持按钮，会话保持表项从主设备同步到备设备，client 访问 server 过程中进行主备切换之后，会话保持功能生效。

**配置步骤：**

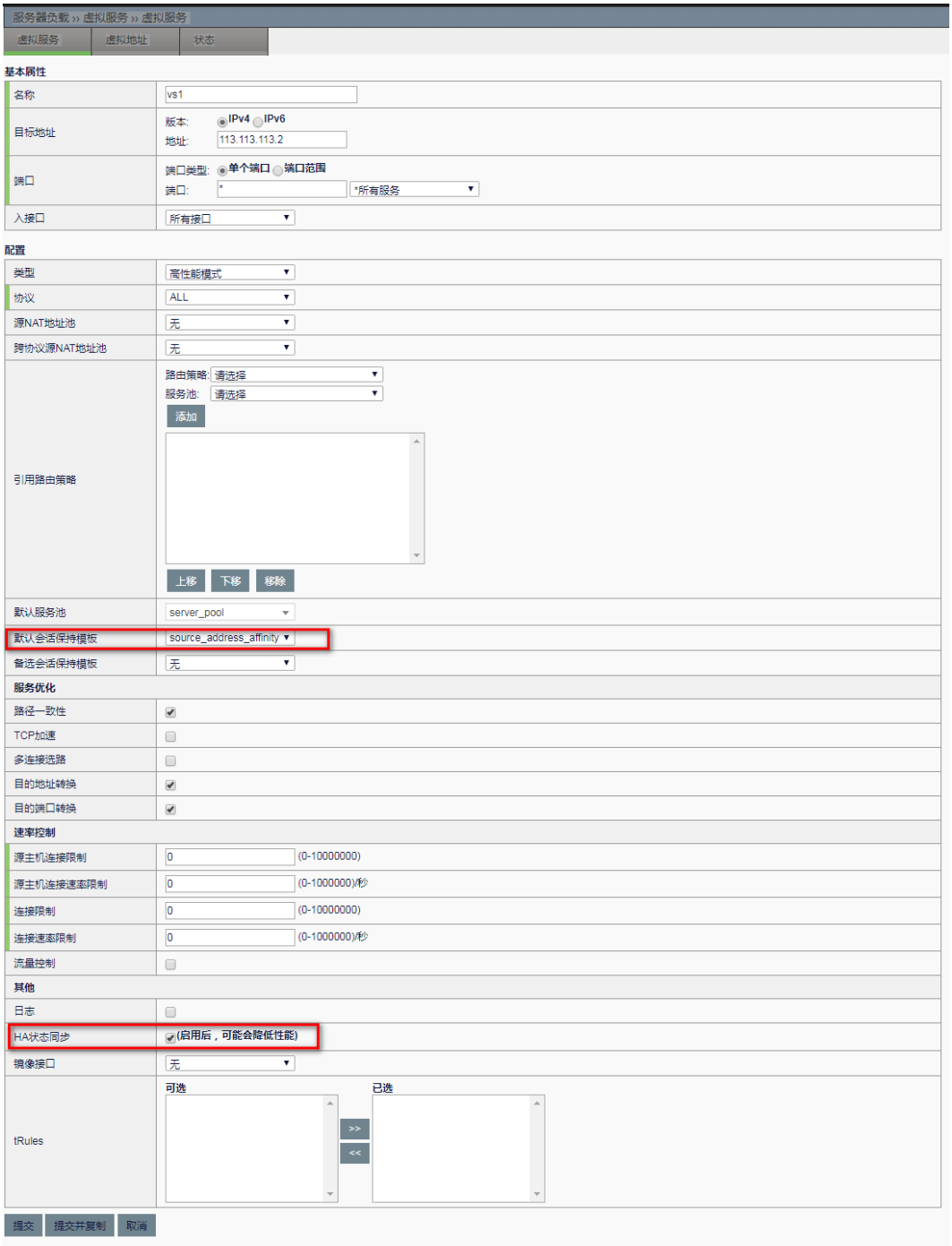
1、参照主备配置案例进行配置，使两台设备协商出主备状态，开启连接同步功能。

2、ADC_A 会话表项模板开启 HA 同步，进入**模板和对象>会话保持>source_address_affinity**，进入配置界面

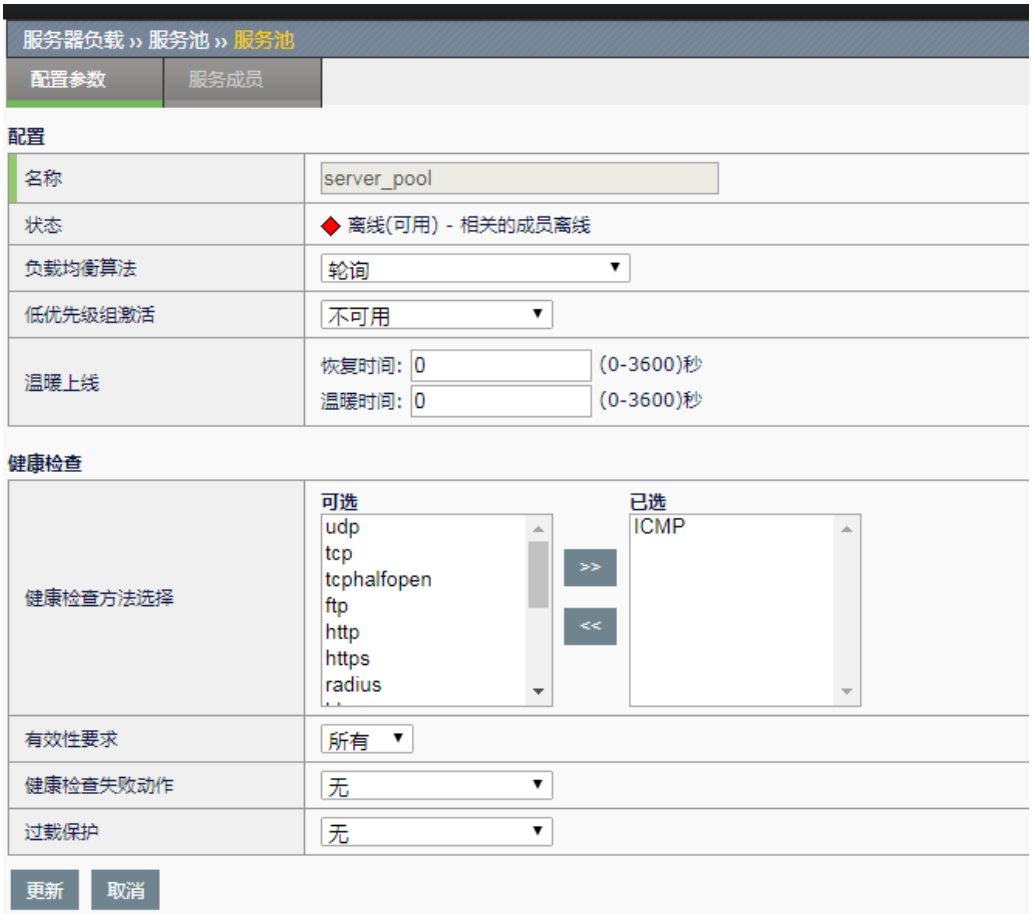



开启 HA 同步：勾选此项后，开启了 HA 会话保持同步功能，点击**更新**按钮，配置成功

3、ADC_A 配置虚拟服务 vs1，配置会话保持模板，开启 HA 状态同步。




4、虚拟服务 vs1 引用的地址池成员为多个。





5、ADC_B 对照 ADC_A 设备进行相应配置

6、client 通过 vs1 访问 server，主设备的会话保持表项同步到备设备

```
host#
host# show src-addr template all
source address vs vs1 template: key 115.115.115.100 ->member 212.1.1.100 port 0 pool server_pool left time 1800
host#
```

主设备

```
mayan238# show src-addr template all
source address vs vs1 template: key 115.115.115.100 ->member 212.1.1.100 port 0 pool server_pool left time 1748
mayan238#
```

备设备

7、两台设备进行主备切换，通过监控页面的主备切换按钮进行切换后，新主的流量还是分配到 212.1.1.100 服务成员上面，会话保持同步功能生效。




### 73.7.4 案例4：配置的手动同步和自动同步功能

**案例描述：**

两台设备，ADC_A,ADC_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，关闭配置自动同步功能，主设备配置时间对象 time1 后进行手动配置同步；开启配置自动同步功能之后，主设备配置时间对象 time2，配置自动同步功能生效。

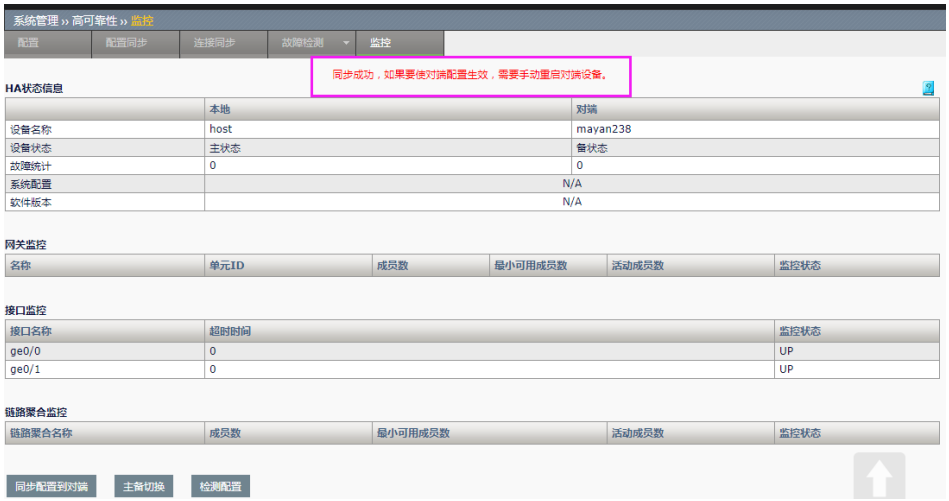
**配置步骤：**

**1、**参照主备配置案例进行配置，使两台设备协商出主备状态，关闭配置自动同步功能。



2、配置时间对象 time1


3、进入 HA 监控页面，点击配置同步到对端按钮，系统给出提示信息




4、不保存配置，直接重启备设备，备设备起来之后查看时间对象模板 time1 手动同步成


5、开启主设备和备设备的配置自动同步功能



6、查看后台配置自动同步连接是否正常

```
/ # netstat -an |grep 13421
tcp        0      0 9.9.9.11:13421          0.0.0.0:*               LISTEN
tcp        0      0 9.9.9.11:45565          9.9.9.12:13421          ESTABLISHED
tcp        0      0 9.9.9.11:13421          9.9.9.12:50626          ESTABLISHED
/ #
```

主设备

```
/ # netstat -an |grep 13421
tcp        0      0 9.9.9.12:13421          0.0.0.0:*               LISTEN
tcp        0      0 9.9.9.12:13421          9.9.9.11:45565          ESTABLISHED
tcp        0      0 9.9.9.12:50626          9.9.9.11:13421          ESTABLISHED
/ #
```

备设备

7、主设备配置时间对象 time2


8、查看备设备时间对象 time2 自动同步成功


注：配置自动同步的连接会定时查询，发现连接断开后，系统会自动重新连接，当需要进行配置同步的时候，系统也会去查询自动同步按钮是否存在，如果不存在的话，系统会去重新建立连接

### 73.7.5 案例5：HA主备切换过程详解

**案例描述：**

两台设备，ADC_A,ADC_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，三种主备切换方式。

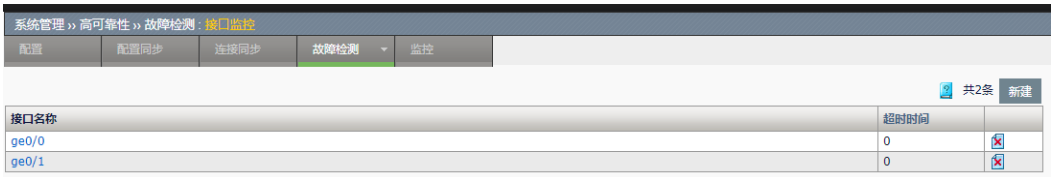
**配置步骤：**

1、通过 HA 监控页面的**主备切换**按钮进行主备切换，只有主设备才能使用这个按钮且抢占模式为禁用

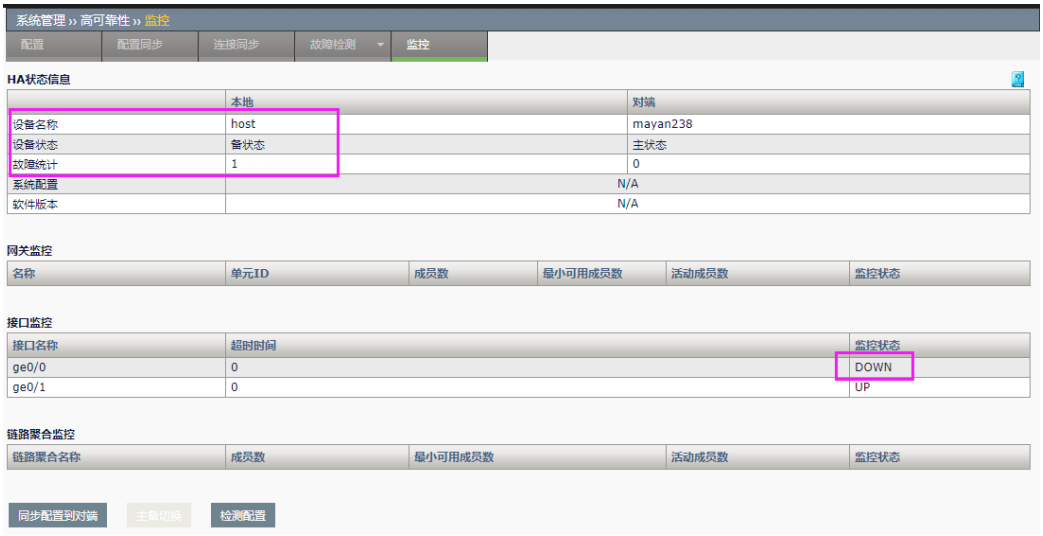

2、点击主备切换按钮之后，主设备变成了备设备，且主备切换按钮为置灰状态


3、主备切换之后，新主设备的虚拟地址、浮动 IP、SNAT 的 NAT 池地址、目的 NAT 的目的地址、静态转换的外部地址均会发送免费 arp，来刷新上下游交换机或者路由器的 arp 表项，使业务引导到新的主设备上面，旧主设备也会把所有的连接一起同步到新主设备，保证已建连接流量转发正常

4、通过监控的接口、链路聚合口或者网关监控故障进行主备切换，此处以监控物理接口为例，新建业务的入接口和出接口的监控

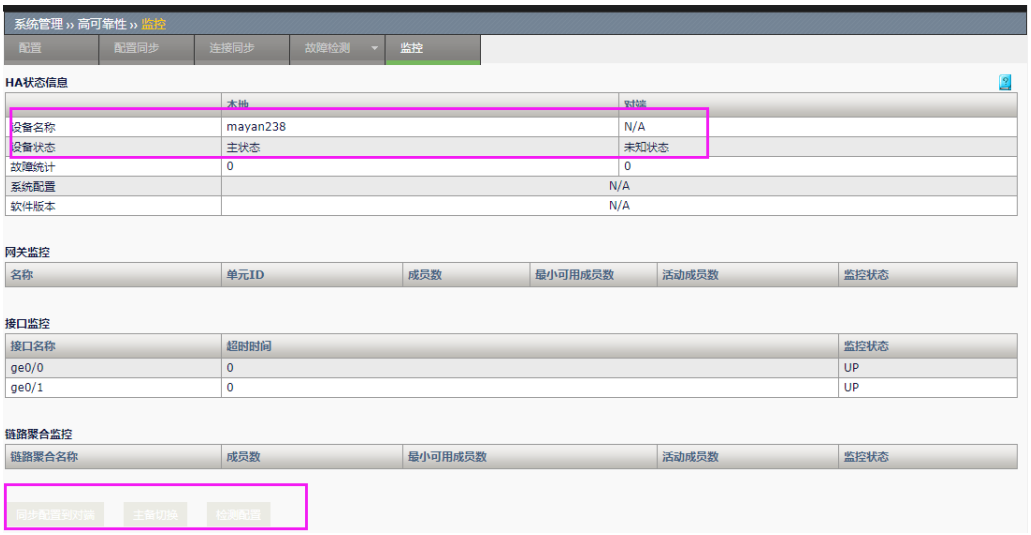



5、拔掉接口 ge0/0 的网线，查看 HA 监控页面，故障统计为 1，主设备变成了备设备，主备切换成功，新主设备会接管旧主设备的业务




6、第三种主备切换的方式是重启主设备，重启主设备之后，旧的备设备会变成主设备，但是对端显示为未知状态，此时业务也会引导到旧的备设备上面来，其中配置同步到对端按钮、主备切换按钮和配置检查按

钮均为不可用的状态，按钮置灰




### 73.7.6 案例6：HA偶尔丢失邻居的市场问题分析

**市场问题描述：**

两台设备，ADC_A,ADC_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，设备偶尔会出现丢失邻居的现象。

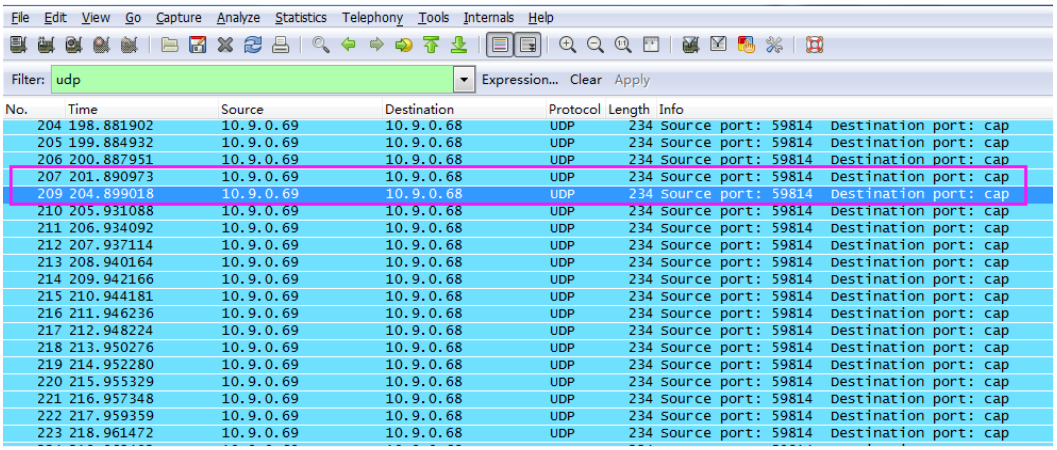
**问题分析：**

1、心跳通信地址不能是连接同步的通信地址，如果是的话，可以先关闭来连接同步功能。查看丢失邻居的日志，在线设备查看或者日志导出来之后查看，这里就是市场导出来的系统日志

```
时间  类型  级别  消息
2019-06-12 20:35:50警示  HA事件Action="Master to Backup" Content="I have
backup grob config"

2019-06-12 20:35:50警示  HA事件Content="HA (Master) get neighbour!fd1 rcv
pkt id=7 sec=1071759 usec=473323, fd2 rcv pkt id=0 sec=0 usec=0, cpu=0"

2019-06-12 20:35:50警示  HA事件Action="Backup to Master" Content="HA no
neigbour"

2019-06-12 20:35:50警示  接口信息    Content=" Duplicate INTERFACE ge0/0
IP address 10.9.0.41 from MAC address: FA:16:4E:6D:89:50
"
2019-06-12 20:35:50警示  接口信息    Content="Duplicate INTERFACE ge0/1
IP address 10.9.3.167 from MAC address: FA:16:4E:8D:43:4A   devmac:
FA:16:4E:79:DF:67"
2019-06-12 20:35:50警示  接口信息    Content="Duplicate INTERFACE ge0/1
IP address 10.9.3.167 from MAC address: FA:16:4E:8D:43:4A   devmac:
FA:16:4E:79:DF:67"
2019-06-12 20:35:50警示  接口信息    Content="Duplicate INTERFACE ge0/0
IP address 10.9.0.41 from MAC address: FA:16:4E:6D:89:50   devmac:
FA:16:4E:6D:C6:B7"
2019-06-12 20:35:50警示  接口信息    Content="Duplicate INTERFACE ge0/0
IP address 10.9.0.41 from MAC address: FA:16:4E:6D:89:50   devmac:
FA:16:4E:6D:C6:B7"
2019-06-12 20:35:50警示  HA事件Content="HA (Backup) lost neighbour!fd1
rcv last pkt id=4 sec=1071756 usec=466323, fd2 rcv last pkt id=0 sec=0
usec=0, cpu=0"
```

分析：备设备丢失邻居之前最后的首选通信地址得到的心跳报文编码为 4，重新收到心跳报文的编码为 7，证明丢失邻居是因为心跳报文丢失了两个报文

2、将心跳报文间隔调整为 1 秒，在备机上面抓包，查看丢失邻居时没有收到心跳报文，正好没有收到两个报文




| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 204 | 198.881902 | 10.9.0.69 | 10.9.0.68 | UDP | 234 | Source port: 59814 Destination port: cap |
| 205 | 199.884932 | 10.9.0.69 | 10.9.0.68 | UDP | 234 | Source port: 59814 Destination port: cap |
| 206 | 200.887951 | 10.9.0.69 | 10.9.0.68 | UDP | 234 | Source port: 59814 Destination port: cap |
| 207 | 201.890973 | 10.9.0.69 | 10.9.0.68 | UDP | 234 | Source port: 59814 Destination port: cap |
| 209 | 204.899018 | 10.9.0.69 | 10.9.0.68 | UDP | 234 | Source port: 59814 Destination port: cap |
| 210 | 205.931088 | 10.9.0.69 | 10.9.0.68 | UDP | 234 | Source port: 59814 Destination port: cap |
| 211 | 206.934092 | 10.9.0.69 | 10.9.0.68 | UDP | 234 | Source port: 59814 Destination port: cap |
| 212 | 207.937114 | 10.9.0.69 | 10.9.0.68 | UDP | 234 | Source port: 59814 Destination port: cap |
| 213 | 208.940164 | 10.9.0.69 | 10.9.0.68 | UDP | 234 | Source port: 59814 Destination port: cap |
| 214 | 209.942166 | 10.9.0.69 | 10.9.0.68 | UDP | 234 | Source port: 59814 Destination port: cap |
| 215 | 210.944181 | 10.9.0.69 | 10.9.0.68 | UDP | 234 | Source port: 59814 Destination port: cap |
| 216 | 211.946236 | 10.9.0.69 | 10.9.0.68 | UDP | 234 | Source port: 59814 Destination port: cap |
| 217 | 212.948224 | 10.9.0.69 | 10.9.0.68 | UDP | 234 | Source port: 59814 Destination port: cap |
| 218 | 213.950276 | 10.9.0.69 | 10.9.0.68 | UDP | 234 | Source port: 59814 Destination port: cap |
| 219 | 214.952280 | 10.9.0.69 | 10.9.0.68 | UDP | 234 | Source port: 59814 Destination port: cap |
| 220 | 215.955329 | 10.9.0.69 | 10.9.0.68 | UDP | 234 | Source port: 59814 Destination port: cap |
| 221 | 216.957348 | 10.9.0.69 | 10.9.0.68 | UDP | 234 | Source port: 59814 Destination port: cap |
| 222 | 217.959359 | 10.9.0.69 | 10.9.0.68 | UDP | 234 | Source port: 59814 Destination port: cap |
| 223 | 218.961472 | 10.9.0.69 | 10.9.0.68 | UDP | 234 | Source port: 59814 Destination port: cap |

3、备设备没有收到心跳报文，现在查一下，主设备在此段时间内是否发送了心跳报文，在主设备上面的心跳通信地址的接口做镜像，将报文都镜像到其他接口引导连接的 PC 上面，PC 抓包查看主设备是否有发送出心跳报文，如果丢失邻居期间心跳报文已经发送出去，证明我司设备没有问题，是心跳通信线的问题，请换跟心跳线再观察，如果是虚拟环境的话，请排查虚拟环境中报文转发是否异常；如果抓到的主设备的心跳报文也是丢失两个报文，那就要查下主设备丢失邻居的过程中的 CPU 是否突然变高，是否是有攻击报文。

4、丢失邻居的现象偶尔出现，为了降低出现的概率也可以暂时将心跳间隔时间调整为 3 秒，保证对用户业务的影响降到最低。

# 74 第74章 VRRP

## 74.1 VRRP概述

### VRRP 简介

通常，同一网段内的所有主机都设置一条相同的以网关为下一跳的缺省路由。主机发往其他网段的报文将通过缺省路由发往网关，再由网关进行转发，从而实现主机与外部网络的通信。当网关发生故障时，本网段内所有以网关为缺省路由的主机将无法与外部网络通信。

缺省路由为用户的配置操作提供了方便，但是对缺省网关设备提出了很高的稳定性要求。增加出口网关是提高系统可靠性的常见方法，此时如何在多个出口之间进行选路就成为需要解决的问题。

VRRP（Virtual Router Redundancy Protocol，虚拟路由器冗余协议）将可以承担网关功能的路由器加入到备份组中，形成一台虚拟路由器，由 VRRP 的选举机制决定哪台路由器承担转发任务，局域网内的主机只需将虚拟路由器配置为缺省网关。

VRRP 是一种容错协议，在提高可靠性的同时，简化了主机的配置。在具有多播或广播能力的局域网（如以太网）中，借助 VRRP 能在某台设备出现故障时仍然提供高可靠的缺省链路，有效避免单一链路发生故障后网络中断的问题，而无需修改动态路由协议、路由发现协议等配置信息。

### VRRP 备份组

VRRP 将局域网内的一组路由器划分在一起，称为一个备份组。备份组由一个 Master 路由器和多个 Backup 路由器组成，功能上相当于一台虚拟路由器。

### 虚拟 IP

虚拟路由器具有 IP 地址。局域网内的主机仅需要知道这个虚拟路由器的 IP 地址，并将其设置为缺省路由的下一跳地址，网络内的主机通过这个虚拟路由器与外部网络进行通信。

### 备份组中路由器的优先级

VRRP 根据优先级来确定备份组中每台路由器的角色（Master 路由器或 Backup 路由器）。优先级越高，则越有可能成为 Master 路由器。

### 备份组中路由器的工作方式

备份组中的路由器具有以下两种工作方式：

非抢占方式：如果备份组中的路由器工作在非抢占方式下，则只要 Master 路由器没有出现故障，Backup 路由器即使随后被配置了更高的优先级也不会成为 Master 路由器。

抢占方式：如果备份组中的路由器工作在抢占方式下，它一旦发现自己的优先级比当前的 Master 路由器的优先级高，就会对外发送 VRRP 通告报文。导致备份组内路由器重新选举 Master 路由器，并最终取代原有的 Master 路由器。相应地，原来的 Master 路由器将会变成 Backup 路由器。

**备份组中路由器的认证方式**

VRRP 提供了两种认证方式：

Text：简单字符认证。在一个有可能受到安全威胁的网络中，可以将认证方式设置为 Text。发送 VRRP 报文的路由器将认证字填入到 VRRP 报文中，而收到 VRRP 报文的路由器会将收到的 VRRP 报文中的认证字和本地配置的认证字进行比较。如果认证字相同，则认为接收到的报文是真实、合法的 VRRP 报文；否则认为接收到的报文是一个非法报文。

MD5：MD5 认证。在一个非常不安全的网络中，可以将认证方式设置为 MD5。发送 VRRP 报文的路由器利用认证字和 MD5 算法对 VRRP 报文进行加密，加密后的报文保存在 Authentication Header（认证头）中。收到 VRRP 报文的路由器会利用认证字解密报文，检查该报文的合法性。

在一个安全的网络中，用户也可以不设置认证方式。


注意

在 VRRPv3 版本模式下，不支持认证。

**VRRP 定时器**

1. VRRP 通告报文时间间隔定时器

用户可以通过设置 VRRP 定时器来调整 Master 路由器发送 VRRP 通告报文的时间间隔。如果 Backup 路由器在等待了 3 个间隔时间后，依然没有收到 VRRP 通告报文，则认为自己是 Master 路由器，并对外发送 VRRP 通告报文，重新进行 Master 路由器的选举。

2. VRRP 抢占延迟时间定时器

在性能不够稳定的网络中，Backup 路由器可能因为网络堵塞而无法正常收到 Master 路由器的报文，导致备份组内的成员频繁的进行主备状态转换。用户可以通过设置 VRRP 抢占延迟时间的方法来解决这个问题。

设置了 VRRP 抢占延迟时间后，Backup 路由器会在等待了 3 倍的通告报

文时间间隔后，再等待 VRRP 抢占延迟时间。如在此期间还是没有收到 VRRP 通告报文，则此 Backup 路由器将认为自己是 Master 路由器，对外发送 VRRP 通告报文，触发备份组内路由器进行 Master 路由器的选举。

**VRRP 报文格式**

支持 VRRPv2 和 VRRPv3 两种格式的报文。

## 74.2 配置VRRP

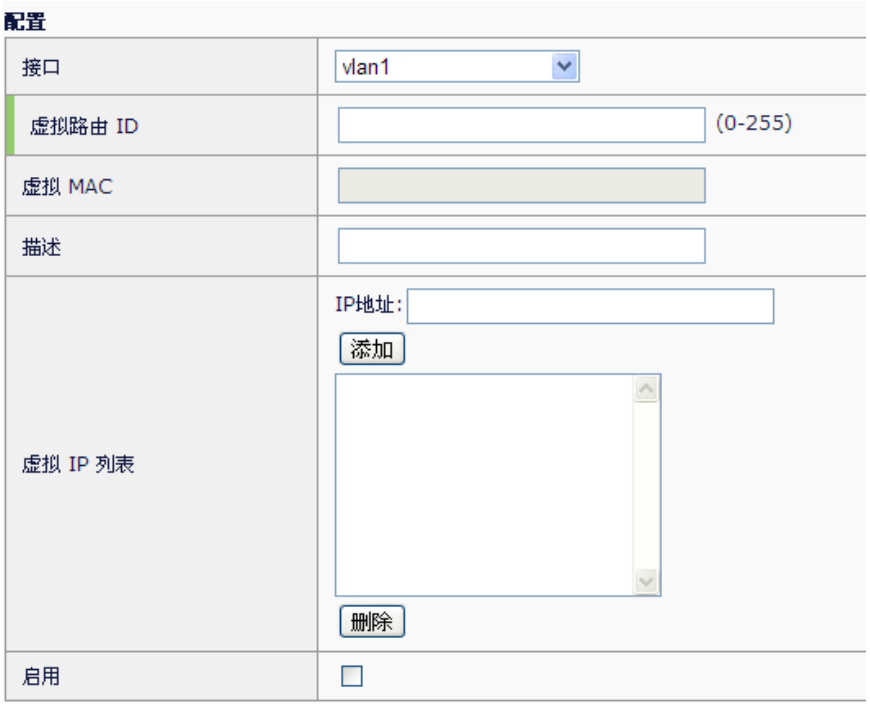
### 74.2.1 配置VRRP

**配置准备**

在**网络配置>接口>VLAN 列表**中，为一个 VLAN 接口配置好 IP 地址。

1. 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 vlan 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

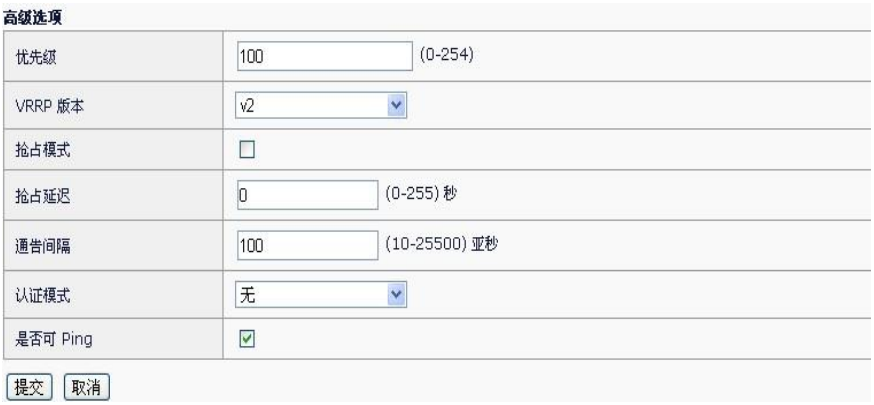
**描述**：用于管理目的的说明性信息。

**虚拟 IP 列表：**设置备份组的虚拟 IP 地址。

- 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。

2. 点击“提交”按钮，新建完成。

注意

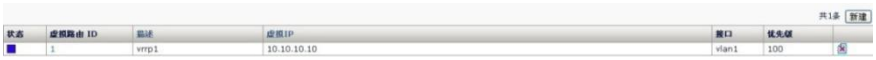
有时候备份组即使被启用了，但仍然无法工作，因为备份组进入工作状态的前提条件是：

1. 接口处于 UP 状态
2. 接口网线上能检测到载波信号
3. 接口上至少配置了一个真实 IP 地址
4. 备份组至少配置了一个虚拟 IP 地址
5. 备份组被启用

以上条件如果任何一个没有被满足，该备份组都无法进入工作状态。

### 74.2.2 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。

### 74.2.3 删除VRRP备份组

在已经建立好的备份组的操作选项中，点击“  ”按钮，经确认后删除。

注意

如果备份组所属的接口被“注销”，如 vlan 下的物理接口被热拔除或者 vlan 接口被删除，那么该接口下所有的备份组都将自动被删除。

### 74.2.4 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。

## 74.3 配置案例

### 74.3.1 配置案例1（单备份组）

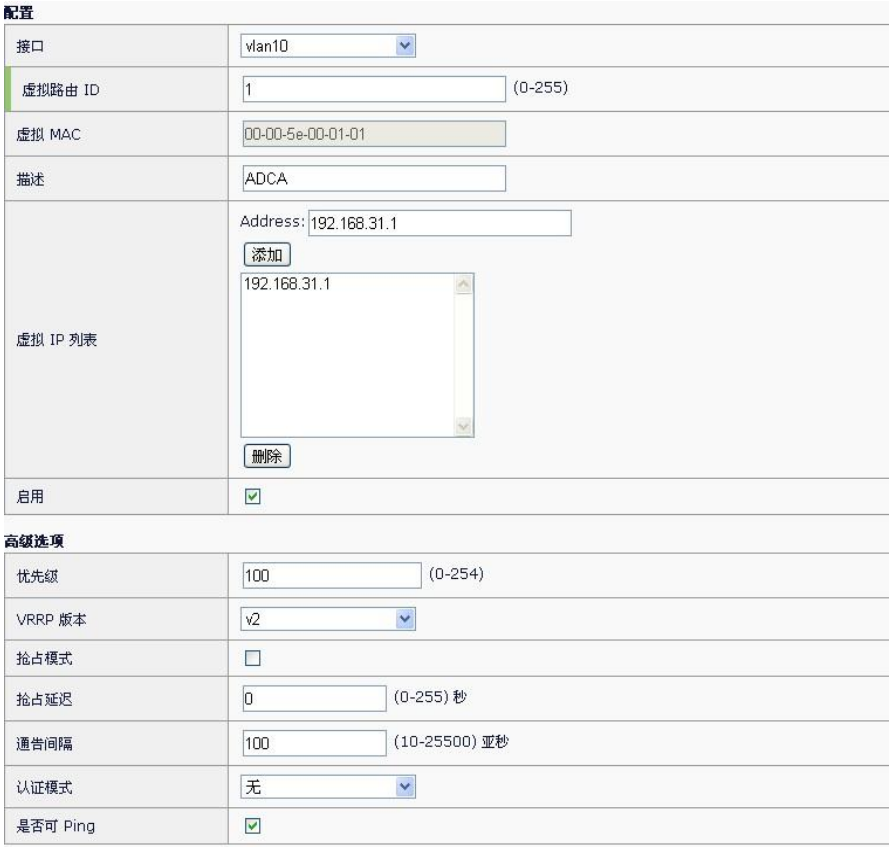
**案例描述：**

单备份组方式表示业务仅由 Master 路由器承担。当 Master 路由器出现故障时，才会从其他 Backup 路由器选举出一个接替工作。主备备份方式仅需要一个备份组，不同路由器在该备份组中拥有不同优先级，优先级最高的路由器将成为 Master 路由器。

在 LAN 中，主机使用 192.168.31.1 这个 IP 地址作为它们的默认网关。把 ADC_A 和 ADC_B 两台路由器组成一个备份组 1。

**配置步骤：**

在 ADC_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 192.168.31.1，提交后启用此备份组。

在 ADC_B 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 50，虚拟 IP 为 192.168.31.1，提交后启用此备份组。

### 74.3.2 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 ADC_A 和 ADC_B 两台路由器创建两个备份组：

备份组 1：ADC_A 作为 Master 路由器，ADC_B 作为 Backup 路由器，虚拟 IP 为 192.168.31.1。

备份组 2：ADC_A 作为 Backup 路由器，ADC_B 作为 Master 路由器，虚拟 IP 为 192.168.31.2。

为了实现业务流量在 ADC_ A、和 ADC_B 之间进行负载分担，需要将局域

网内的主机的默认网关分别设置 192.168.31.1 和 192.168.31.2。在配置优先级时，需要确保两个备份组中各路由器的 VRRP 优先级形成交叉对应。

**配置步骤：**

在 ADC_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 192.168.31.1，提交后启用此备份组。

在 ADC_A 上继续配置备份组 2，如下图配置：


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

在 ADC_B 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 50，虚拟 IP 为 192.168.31.1，提交后启用此备份组。

在 ADC_B 上继续配置备份组 2，如下图配置：


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

## 74.4 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：<br>1．接口处于 UP 状态<br>2．接口网线上能检测到载波信号<br>3．　　接口上至少配置了一个真实 IP 地址 |

# 75 第75章 虚拟化系统

## 75.1 虚拟化系统概述

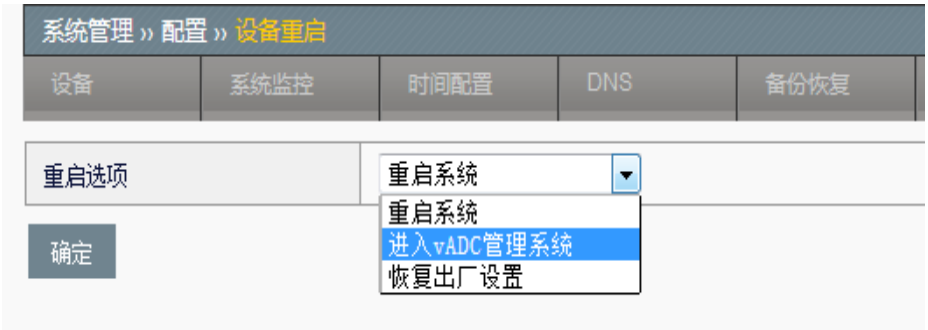
在虚拟化系统中可以创建多个虚拟机，并在每个虚拟机中运行一个应用交付系统。每个系统的软件版本、系统配置等都是独立的，这样可以实现一台应用交付硬件，同时运行多个应用交付系统，同时服务于多个租户（tenant）。

## 75.2 配置虚拟化系统

虚拟化系统的相关配置，包含如下几个方面：

### 75.2.1 进入虚拟化系统

缺省情况下，硬件系统启动后直接进入应用交付系统运行。可以通过在“重启选项”中，选择“进入 vADC 管理系统”，并经过重启，进入虚拟化管理系统，如下图所示：

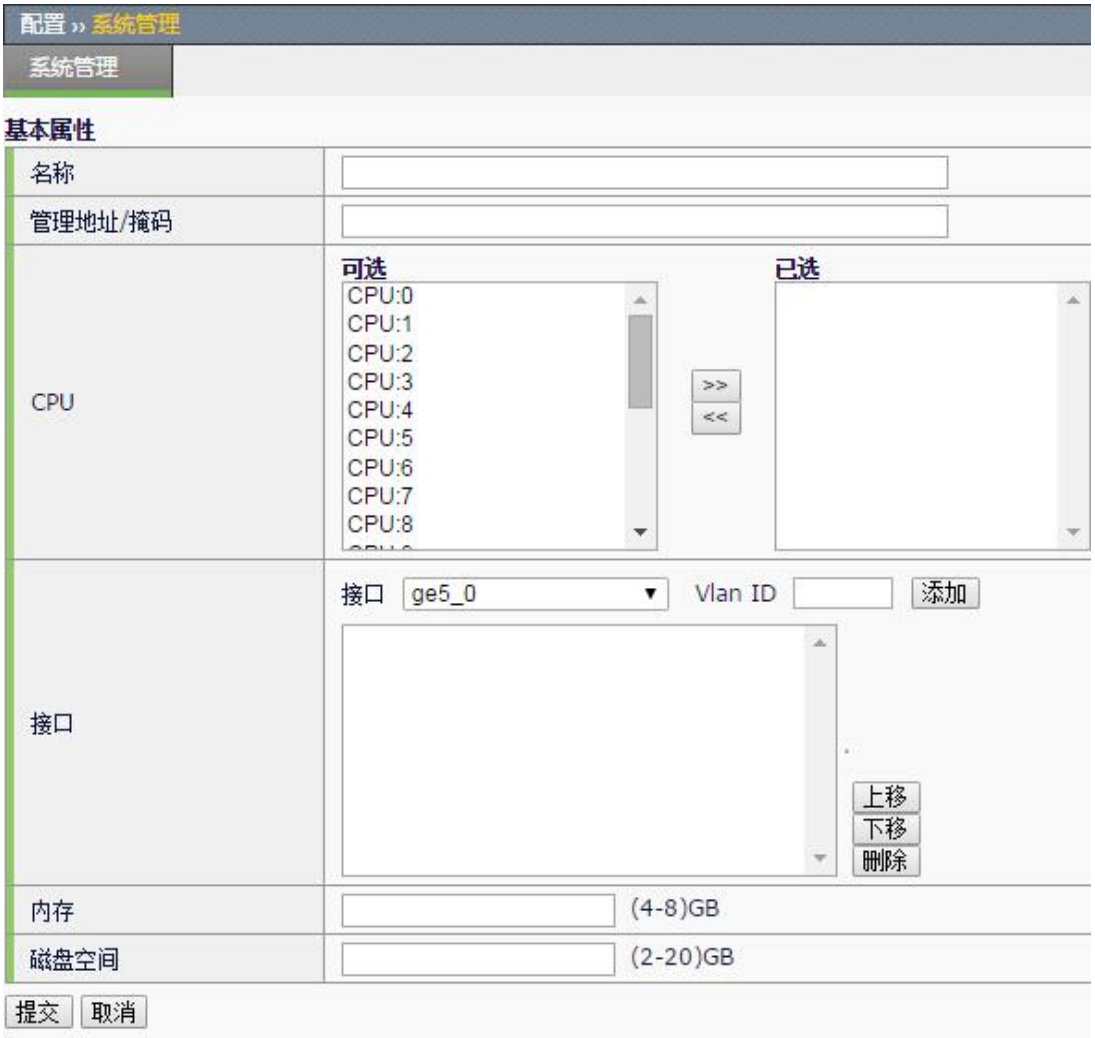



注意

6. 虚拟化系统依赖 Intel VT 和 Intel VT-d 技术，要进入虚拟化管理系统前，需要确保 BIOS 中的相关选项已经打开。
7. 要确保系统软件是支持虚拟化管理系统的版本。

### 75.2.2 创建虚拟机

进入**配置->系统管理**页面，点击**“新建”**，就可以开始创建虚拟机，如下图：




**参数说明：**

**名称：**指定要创建的虚拟机的名称，最多 32 个字符。在系统中，每个虚拟机的名称应该唯一。

**管理地址/掩码：**指定虚拟机管理口的 IP 地址和掩码。在创建虚拟机时，会注入虚拟机的配置文件中。

**CPU：**指定虚拟机所使用的 CPU

**接口：**指定虚拟机所使用的接口。由于一个物理接口可能被多个虚拟机同时使用，可以通过接口的 VLAN ID 属性，将报文传给不同的虚拟机。

**内存：**指定虚拟机使用的内存大小。

**磁盘空间：**指定虚拟机能使用的磁盘空间。

### 75.2.3 管理员账户

要新建管理员账户，可以进入**配置->管理员**页面，点击“新建”，如下

图：


**参数说明：**

**用户名：**管理员名称

**密码：**设置的密码

**确认密码：**确认设置的密码

### 75.2.4 版本管理

要升级虚拟化管理系统的软件版本，可以进入**配置->版本管理**页面，如下图：


点击“**浏览**”，选择升级包，然后点击“**升级**”，并根据弹出的提示框，选择“**确定**”，系统就会进行升级。

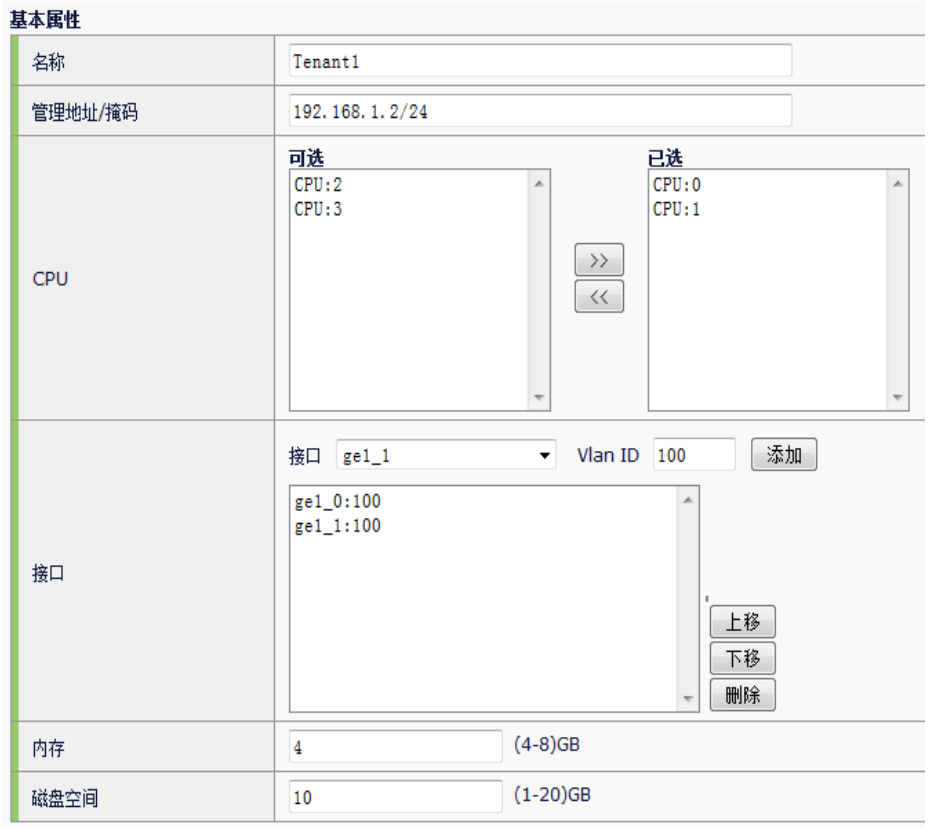
## 75.3 配置案例

**案例描述**

创建一个虚拟机名为 Tenanvenustech 的虚拟机，并为其指定 CPU、内存和接口等计算资源，并启动该虚拟机。

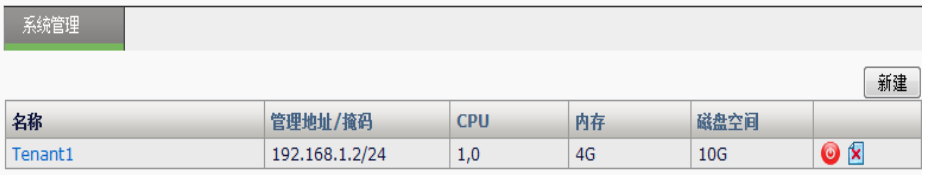
1. **配置步骤：**创建虚拟机

进入**配置->系统管理**页面，点击“新建”：



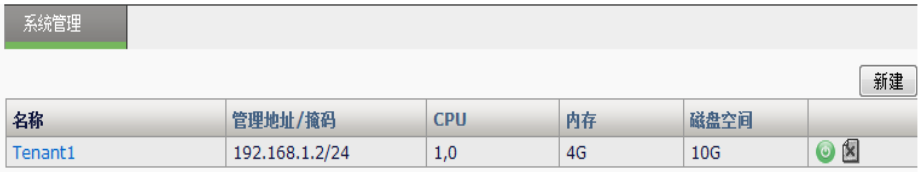

在属性框中设置虚拟机的各种属性。如上图中，指定虚拟机的名称为“Tenanvenustech”；指定虚拟机的管理口 IP 地址为“192.168.1.2/24”；指定虚拟机使用的 CPU 为 0 和 1，虚拟机最多可以指定 4 个 CPU；指定虚拟机使用的接口为 ge1_0 和 ge1_1 两个接口，并且 VLAN ID 为 100，即这两个物理接口上，收到 VLAN ID 为 100 的报文，都交给本虚拟机处理；指定虚拟机的内存大小为 4GB；指定虚拟机可使用的硬盘空间为 10GB。

设置好虚拟机的属性后，点击“**提交**”，就会按指定的属性创建虚拟机，结果如下图：




2. 启动虚拟机

点击虚拟机描述栏中的开关按钮（红色），即可启动该虚拟机。启动成功后，该按钮变为绿色，如下图：



3. 停止虚拟机

点击虚拟机描述栏中的开关按钮，即可停止该虚拟机运行。

# 76 第76章 日志管理

## 76.1 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，包括本地日志，以及 E-mail 日志，提供给用户掌握系统运行状况的方法。

## 76.2 配置说明

### 76.2.1 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 |

### 76.2.2 配置SYSLOG服务器

1. 进入**系统管理>日志管理>选项：日志服务器**，如下图：


**参数说明：**

**启用**：选中表示启用，不选表示关闭。

**IP 地址**：Syslog 服务器地址。

**IPV6 地址**：IPV6 Syslog 服务器地址。

**端口**：Syslog 服务器端口。

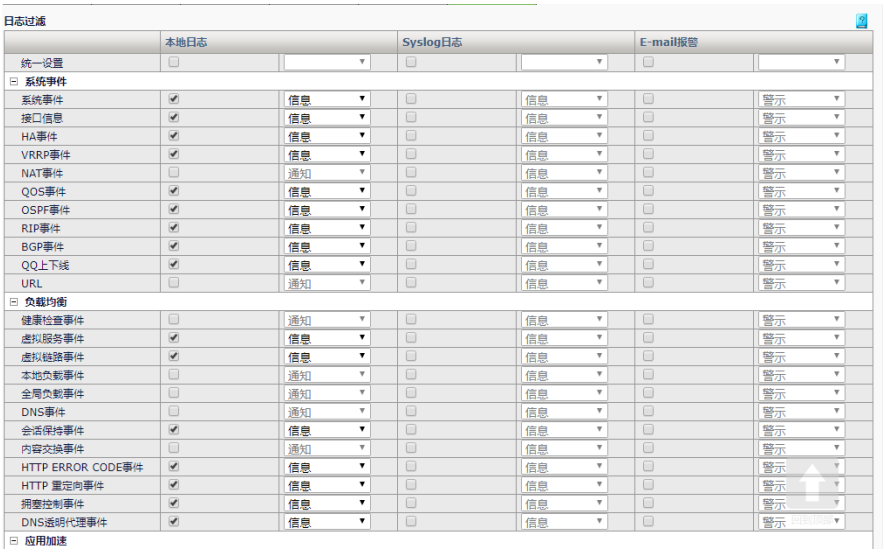
**服务器 1、服务器 2、服务器 3** 表示可以同时将日志发送到数个不同的 Syslog 服务器，之间互不影响。

**配置步骤：**

1. 填写 SYSLOG 服务器地址。
2. 填写服务器端口。
3. 选择**启用**服务器。
4. 点击**提交。**

## 76.2.3 配置日志过滤

进入**系统管理>日志管理>选项：日志过滤**，如下图：




**参数说明：**

**模块名称**：各模块对应的名称。

**本地日志**：是否启用本地日志及其级别。

**Syslog 日志**：是否启用 Syslog 日志及其级别。

**E-mail 报警**：是否启用 E-mail 日志及其级别。

**配置步骤：**

1. 选择对应模块，启用本地日志及其级别。

2. 选择对应模块，启用 Syslog 日志及其级别。

3. 选择对应模块，启用 E-mail 日志及其级别。

4. 点击**提交**。


提示

1.**日志过滤**中只对大于或等于该级别的日志有效。

2.**日志过滤**中涉及到的日志模块只是发送日志模块的的一部分。

## 76.3 监控与维护

### 76.3.1 日志查看

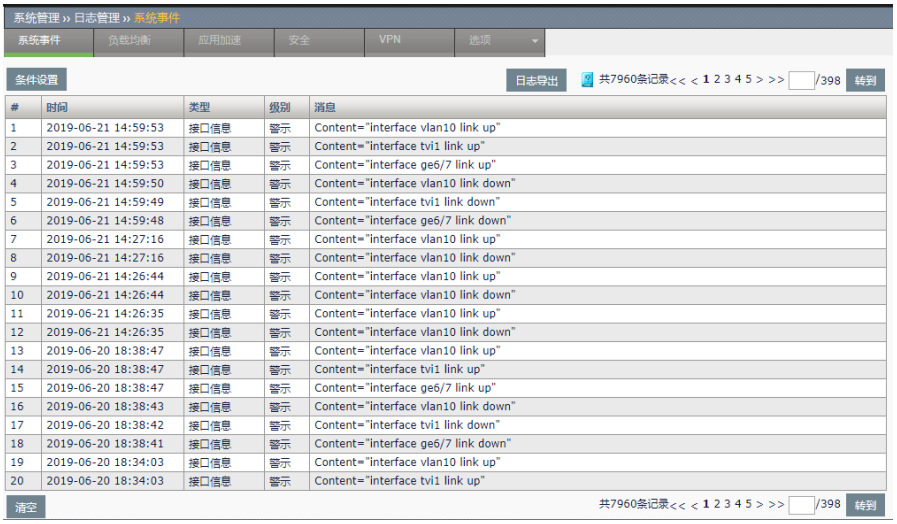
ADC 设备上的日志展示一共分为六大类，包括**系统事件**、**负载均衡**、**应用加速**、**安全**、**VPN** 和**配置审计**，该分类同**系统管理>日志管理>选项：日志过滤**中所包含功能模块一致。

要查看对应分类的日志内容，需要在**系统管理>日志管理**下选择对应分类，进入对应分类页签后，还可以根据“**条件设置**”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。

**配置审计**的日志内容和日志配置只能在 audit 审计用户下查看和操作

**系统事件**、**负载均衡**、**应用加速**、**安全**、**VPN** 和**配置审计**六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**系统管理>日志管理>系统事件**，如下图：




**参数说明：**

**#：**该系统事件日志消息的序号。

**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。

**清空**：清空当前系统事件类别中所有日志消息。

**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 20 条日志。

点击 条件设置：设置过滤条件，详细配置参考“条件设置”。

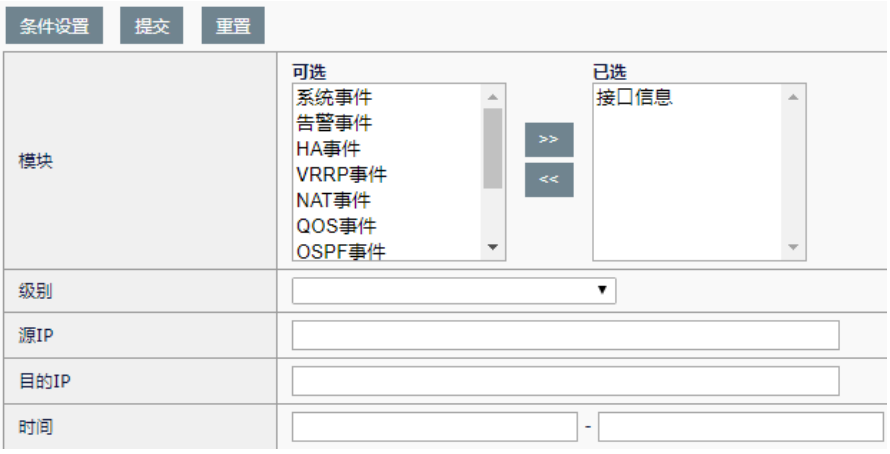

1. 对日志进行分类，分为六大类：系统事件、负载均衡、应用加速、安全、VPN、配置审计。负载均衡、应用加速、安全、VPN、配置审计类别下的日志配置参考系统事件类别日志操作。

2. **配置审计日志**只有 audit 用户可以配置查看。

## 76.3.2 日志查询条件设置

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

进入**系统管理>日志管理>系统事件**点击**条件设置**，如下图：




**模块**：选择需要查看的日志模块。

**级别**：选择需要显示的日志级别。默认为空，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**：触发日志的源 IP。可输入具体 ip 地址，也可输入带掩码的网段地址。

**目的 IP**：触发日志的目的 IP。可输入具体 ip 地址，也可输入带掩码的网段地址。

**时间**：日志产生的时间段。

**配置步骤：**

1. 选择对应**模块**。
2. 选择**级别**。
3. 选择**源 IP**。
4. 选择**目的 IP**。
5. 选择日志**时间**段。
6. 点击**提交。**

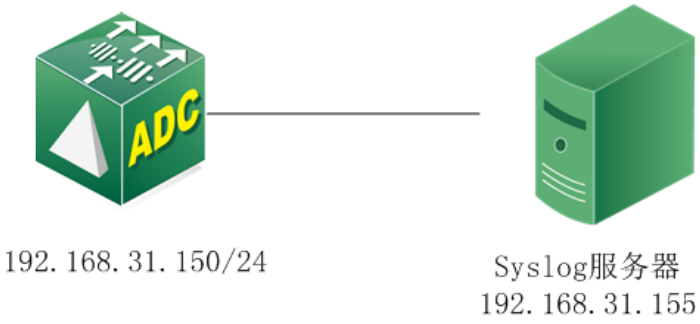
## 76.4 配置案例

### 76.4.1 配置案例：配置健康检查模块 SYSLOG日志

**案例描述：**

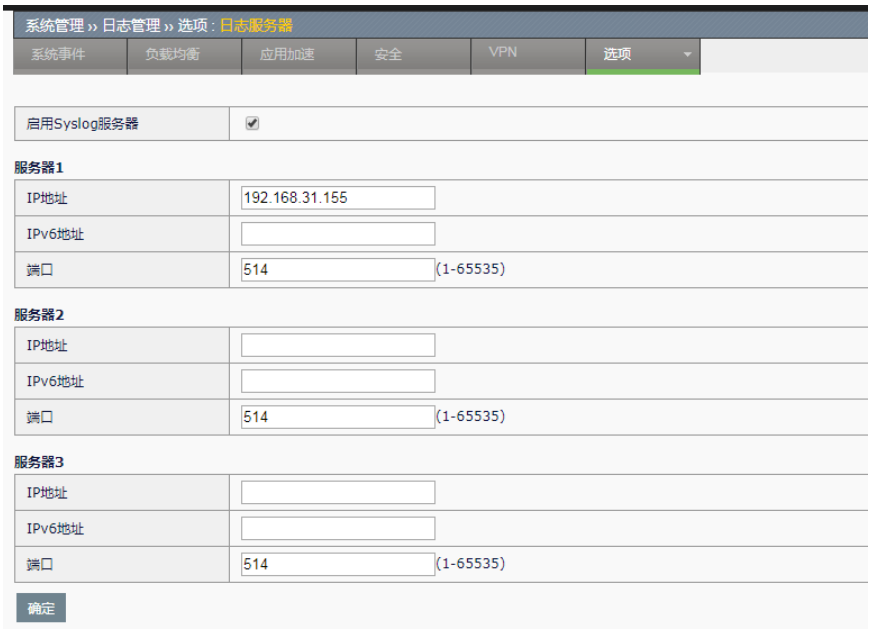
配置健康检查模块发送到日志服务器。

**案例组网图：**




**配置步骤：**

1. 进入**系统管理>日志管理>选项：日志服务器：**



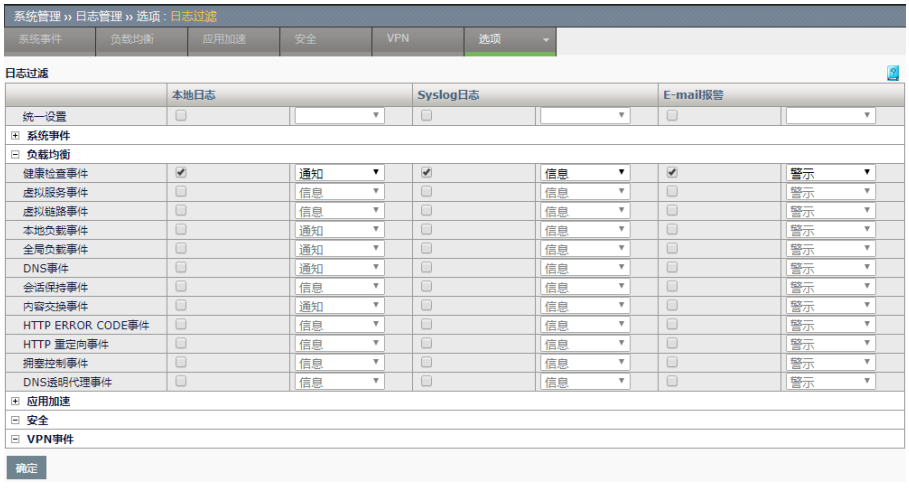

2.设置配置参数

**IP 地址**：Syslog 服务器地址为”192.168.31.155”。

**端口**：Syslog 服务器端口为”514”。

**启用**：选中表示启用，点击**提交**完成设置。

3.进入**系统管理>日志管理>选项：日志过滤：**




4. 设置参数。

5. 点击**提交**完成设置。

注意

进行健康检查相关操作后，在 Syslog 服务器上能够看到健康检查模块产生的日志信息。

## 76.5 常见故障分析

### 76.5.1 故障现象1：SYSLOG日志失效

| | |
|---|---|
| 现象 | 在SYSLOG服务器上看不到对应模块日志 |
| 分析 | 1. 是否正确配置SYLOG服务器的地址和端口号<br>2. 是否指定模块的日志类别和等级到SYSLOG Server |
| 解决 | 1. 正确配置SYSLOG服务器的地址和端口号<br>2. 指定模块的日志类别和等级到SYSLOG Server |

### 76.5.2 故障现象2：E-mail日志失效

| | |
|---|---|
| 现象 | 没有收到对应模块日志信息的邮件 |
| 分析 | 1. 是否正确配置告警邮件配置参数<br>2. 是否启用对应模块发送E-mail日志<br>3. 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 | 1. 正确配置告警邮件配置参数，以及发送邮件需要的路由和dns配置，保证告警邮件功能中的测试邮件能够发送成功<br>2. 启用对应模块发送E-mail日志<br>3. 保证所需要发送E-mail告警日志的模块产生的日志是警示或以上级别。如果无法产生对应级别日志，则无法邮件告警。 |

# 77 第77章 报表功能

## 77.1 报表概述

报表模块可以根据需求统计“**服务器负载、链路负载、本地负载、全局负载、应用优化、系统信息**”相关的各种数据，生成内容丰富的 HTML 和 PDF 格式文件，以图表形式直观的展示各项统计结果。

## 77.2 全局配置

进入**报表功能>报表配置>全局配置**，如下图：


- **统计引擎：**开启设备统计报表数据的功能（**默认不开启**）。
- **报表统计数据：**显示当前已经记录的报表相关数据容量，以及最后一次初始化的时间。
- **磁盘信息：** 展示当前硬盘使用情况。
- **磁盘空间控制：**开启报表数据容量控制，限定报表数据存储最大容量（**默认不勾选**）；“立即初始化”按钮，可主动初始化报表数据库，清空当前所有报表数据。
- **操作：**配置报表数据最大容量，当数据达到这个限定值时，将会删除最早日期的一天的数据。
- 点击**提交：**下发当前配置。

注意

报表模块中，有个隐藏限制：

1、 当硬盘剩余容量小于 10G 时，将停止记录数据，而不是删除最早数据。

2、 当硬盘剩余容量小于 10G 时，报表任务也不可执行。

## 77.3 手动报表任务

手动报表任务可自定义明确的起止时间，并可从手动任务列表中触发立即执行该任务。

### 77.3.1 配置手动报表任务

**配置步骤：**

进入**报表功能>报表配置>手动任务**，如下图：

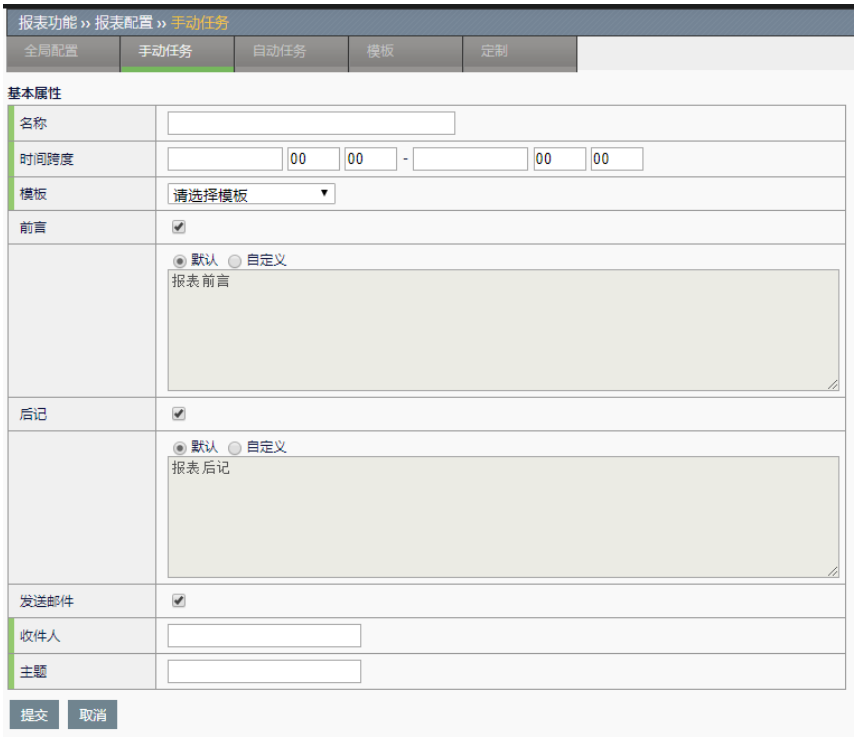

新建：添加一个手动报表任务。

：立即执行报表任务。

：删除掉该任务。

点击名称，可以对已配置的手动报表任务内容进行编辑。

点击**新建。**




- **名称：**该任务的名称。

- **时间跨度**：手动报表任务所要统计数据的时间范围。（若选择的起止日期跨度超过 7 天，则分钟参数变为 00 分且不可编辑）。
- **模板**：手动报表任务所用的报表模板。（详情请查看**报表模板**章节）
- **发送邮件**：任务完成后是否要发送邮件（默认不选中）。
- **收件人**：要发送邮件的收件人。
- **主题**：邮件的主题。
- **前言**：报表内容中是否要加前言（默认不选中）。
- **后记**：报表内容中是否要加后记（默认不选中）。

点击**提交**：下发当前配置。


要发送邮件需要在系统管理>配置>告警邮件配置中对邮件进行相应的配置。

## 77.4 自动报表任务

自动报表任务与手动任务不同的地方，在于统计的时间范围的选择，以及只能自动触发生成报表，无法手动触发；

自动报表任务可创建周期性自动生成报表的任务，有四种周期可选择：**天、周、月、年**，系统会在到达相应周期的开始时刻，自动生成以上一个周期的起止时间为统计范围的报表文件。

### 77.4.1 配置自动报表任务

**配置步骤：**

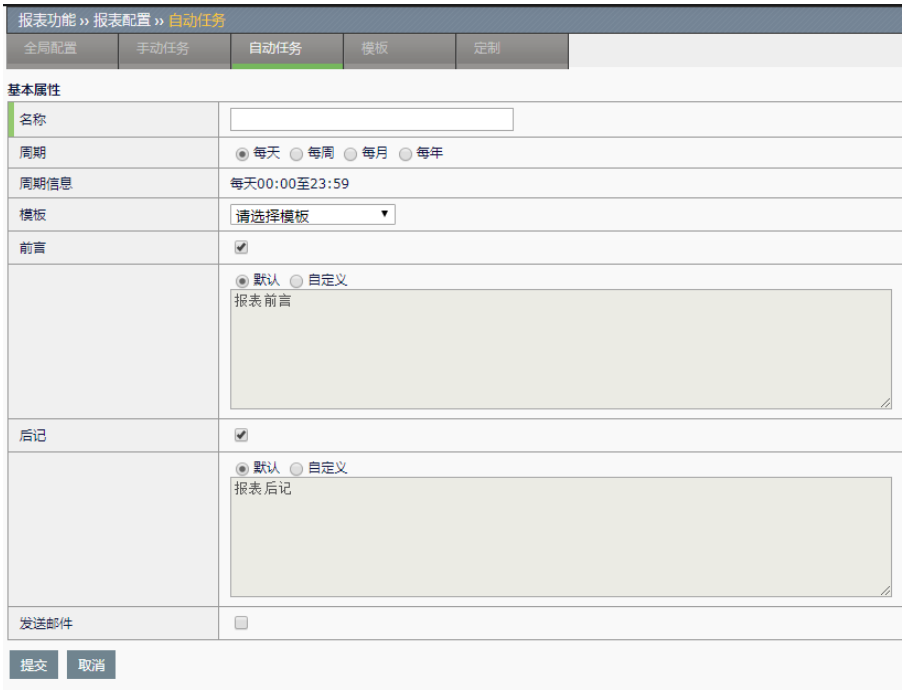
进入**报表功能>报表配置>自动任务**，如下图：


新建：添加一个自动报表任务。

：删除掉该任务。

点击名称，可以对已配置的自动报表任务内容进行编辑。

点击**新建**，如下图：




- **名称：**该任务的名称。
- **周期：**自动报表任务所统计数据的时间范围。
- **模板：**自动报表任务所用的报表模板。
- **发送邮件：**任务完成后是否要发送邮件（默认不选中）。
- **收件人：**要发送邮件的收件人。
- **主题：**邮件的主题。
- **前言：**报表内容中是否要加前言（默认不选中）。
- **后记：**报表内容中是否要加后记（默认不选中）。
- 点击**提交**：使当前配置下发。

提示

要发送邮件需要在系统管理>配置>告警邮件配置中对邮件进行相应的配置。

## 77.5 报表模板

每一个报表任务都必须引用一个报表模板，根据模板来确定所要统计的模块和统计对象：

**服务器负载**模块下可统计“当前连接数”“新建连接数”“上行流量”“下行流量”“HTTP”“SSL”“服务器健康状态”等内容；

**链路负载**模块可统计“当前连接数”“新建连接数”“上行流量”“下行流量”“丢包率(%)”“延时(ms)”“抖动(ms)”等内容；

**本地负载**模块可统计“调度结果”“来源 ISP”等内容；

**全局负载**模块可统计“调度结果”“来源 ISP/地域”等内容；

**应用优化**模块可统计“缓存”“压缩”等内容；

**系统信息**模块可统计“当前连接数”“新建连接数”“上行流量”“下行流量”“HTTP 请求数”“SSL 交易数”“CPU”“内存”等内容；


正在被引用的模板无法被删除，但是可以对其配置进行修改。

### 77.5.1 配置报表模板

**配置步骤：**

进入**报表功能>报表配置>模板**，如下图：


新建：添加一个报表模板。

：删除掉该模板。

点击名称，可以对已配置的模板内容进行编辑。

点击**新建**，如下图：

**1. 服务器负载模板：**


- **名称：**该模板的名称。
- **类型：**可选择统计服务器负载/链路负载/本地负载/全局负载/应用优化/系统信息模块。
- **统计项：**可选择统计“当前连接数”“新建连接数”“上行流量”“下行流量”“HTTP”“SSL”等数据。
- **统计内容：**可选择统计均值或者峰值数据。
- **虚拟服务：**选择要统计的虚拟服务对象。
- **统计池：**选择是否要统计服务池数据。
- **统计成员：**选择是否要统计服务成员数据。
- **统计对象：**选择要统计的虚拟服务对象，“**默认**”即是统计该虚拟服务下所有的池与成员，“**自定义**”是手动选择将要统计的池与成员。
- **服务池&服务成员：**选择要统计的服务池&服务成员对象。

- **服务节点：**选择要统计的服务器节点对象。

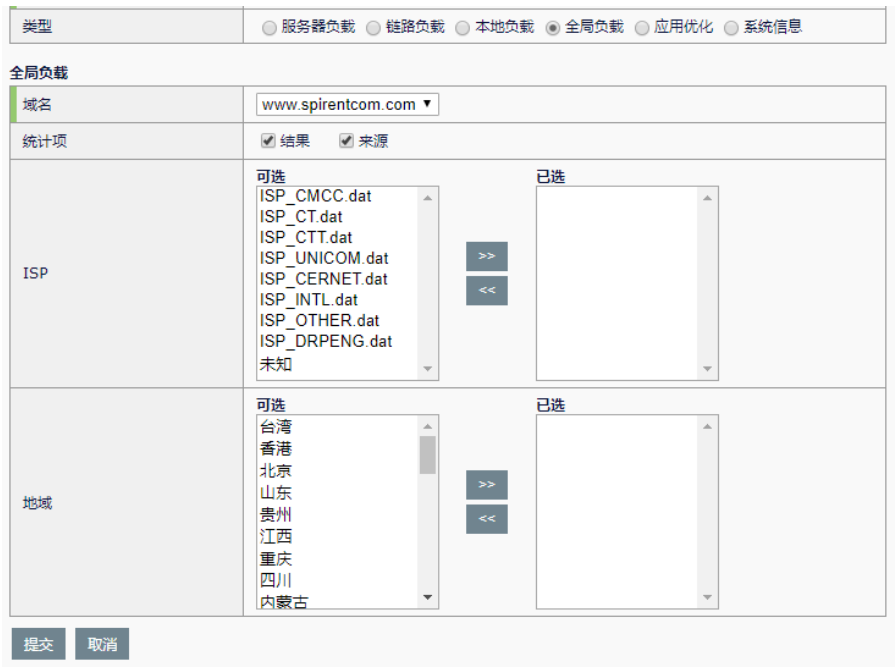
**2. 链路负载模板：**


- **统计项：**可选择统计“当前连接数”“新建连接数”“上行流量”“下行流量”“丢包率(%)”“延时(ms)”“抖动(ms)”等数据。
- **统计内容：**可选择统计均值或者峰值数据。
- **虚拟链路：**选择要统计的虚拟链路对象。
- **统计池：**选择是否要统计链路池数据。
- **统计节点：**选择是否要统计链路节点数据。
- **统计对象：**选择要统计的虚拟链路对象，“**默认**”即是统计该虚拟链路下所有的池与节点，“**自定义**”是手动选择将要统计的池与节点。
- **链路池：**选择要统计的链路池对象。
- **链路节点：**选择要统计的链路节点对象。

**3. 本地负载模板：**

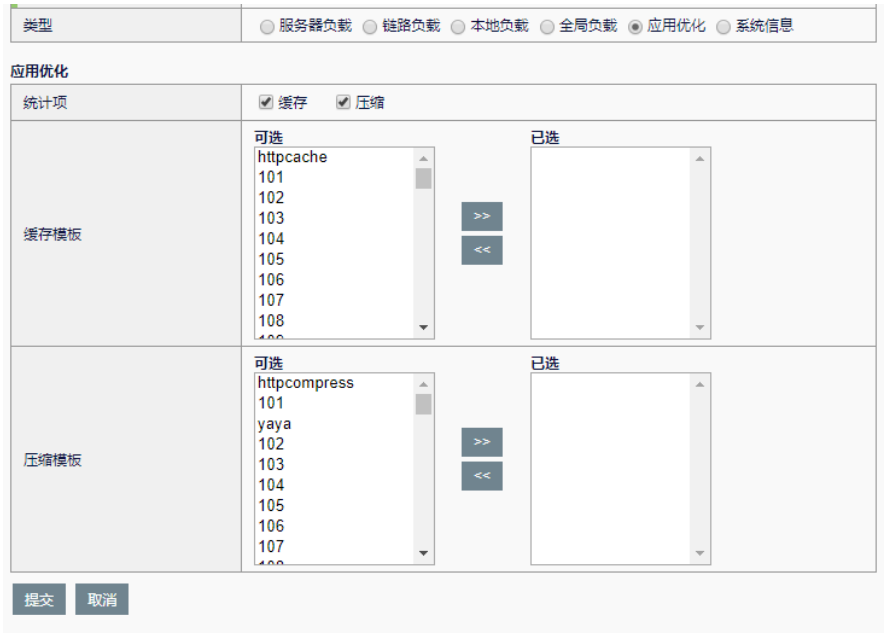

- **统计项**：选择统计“调度结果”“来源 ISP”数据。
- **域名**：选择要统计哪个本地负载对象的数据。
- **ISP**：选择要统计的 ISP 对象。

**4. 全局负载模板：**




- **统计项**：选择统计“调度结果”“来源 ISP/地域”数据。
- **域名**：选择要统计哪个全局负载对象的数据。
- **ISP**：选择要统计的 ISP 对象。
- **地域**：选择要统计的地域范围。

**5. 应用优化模板：**




- **统计项**：选择统计“缓存”“压缩”数据。
- **缓存模板**：选择要统计的缓存模板对象。
- **压缩模板**：选择要统计的压缩模板对象。

**6. 系统信息模板：**


- **统计项**：选择统计“CPU”“内存”“上行流量”“下行流量”“当前连接数”“新建连接数”“HTTP 请求数”“SSL 交易数”等数据。
- **统计内容**：选择统计“均值”“峰值”数据。

点击**提交**：将当前配置下发。

## 77.6 报表定制

报表定制功能可设定报表中的前言和后记的内容，作为报表内容的开始和

结束语。

**配置步骤：**

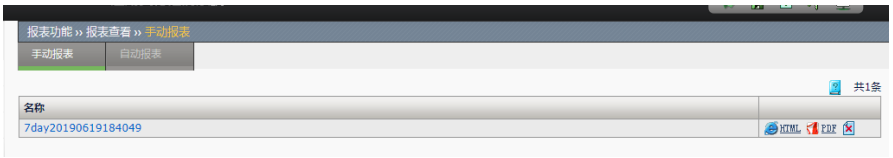
进入**报表功能>报表配置>定制**，如下图：


- **前言**：报表内容中的前言。
- **后记**：报表内容中的后记。

## 77.7 查看手动报表

手动报表列表页面可查看手动报表任务所生成的报表文件。

进入**报表功能>报表查看>手动报表**，如下图：




HTML：下载该报表的 HTML 格式的文件。

PDF：下载该报表的 PDF 格式的文件。

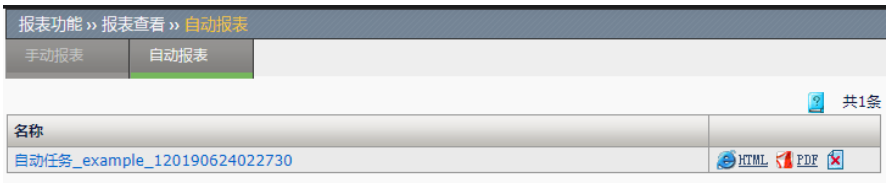
：删除掉该报表。

点击名称，可以在浏览器中浏览 HTML 格式的报表内容。

## 77.8 查看自动报表

自动报表列表页面可查看自动报表任务所生成的报表文件。

进入**报表功能>报表查看>自动报表**，如下图：




HTML：下载该报表的 HTML 格式的文件。

PDF：下载该报表的 PDF 格式的文件。

：删除掉该报表。

点击名称，可以在浏览器中浏览 HTML 格式的报表内容。

## 77.9 配置案例

### 77.9.1 手动任务

**案例描述**

报表任务需要引用一个报表模板，要先创建一个报表模板才可创建任务。

**配置方法：**

**新建**报表模板“模板_example_1”。

**新建**手动报表任务“手动任务_example_1”，并引用模板“模板_example_1”。

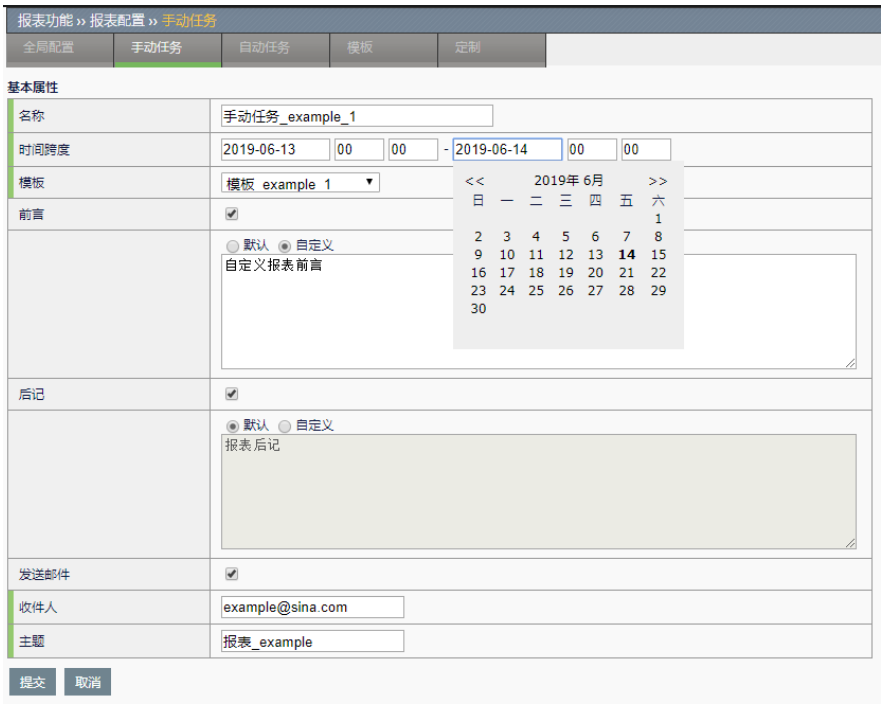
若需要给报表添加前言后记，则在报表定制页面设定报表的前言后记，或在报表任务中自定义单独的前言后记。

**配置步骤：**

**新建**报表模板，选择虚拟服务模块进行统计，选择“当前连接数”“新建连接数”“上行流量”等需要统计的若干项，勾选统计均值，勾选统计成员数据，统计对象选择默认统计该虚拟服务下所有池和成员，**提交**配置，如下图：

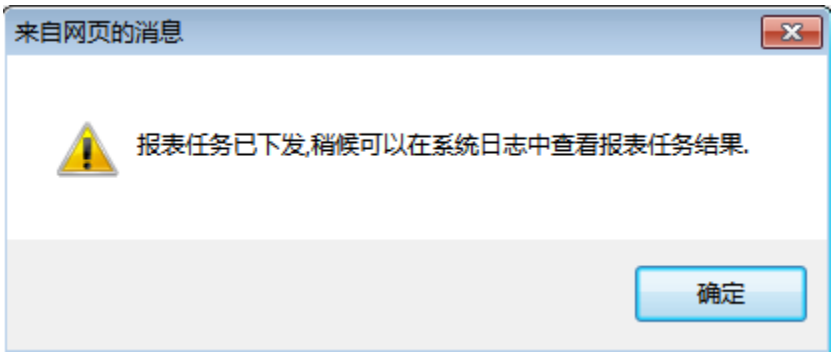

**定制**报表的前言后记


**新建**手动报表任务，指定统计的时间范围，选择刚刚创建的报表模板（勾选**发送邮件**，设定**收件人**和**邮件主题**，勾选前言和后记，设定一个自定义的前言，后记引用全局的后记内容），**提交**配置。

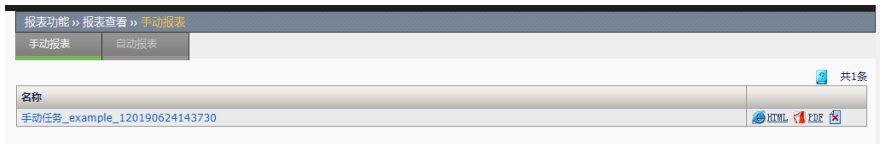



进入**报表功能>报表配置>手动任务**，可看到刚刚创建的手动任务，如下图：


点击  ，立即执行该任务，会弹出提示框，如图：




等待报表任务执行完成，进入**报表功能>报表查看>手动报表**，可看到生成出来的报表，如图：



## 77.9.2 自动任务

**案例描述**

自动任务创建完成后，会在每天凌晨 2：15 判断哪些任务到了执行的时间，并自动开始执行。

**配置方法：**

**新建**报表模板“模板_example_1”；

**新建**自动报表任务“自动任务_example_1”，并引用模板“模板_example_1”，

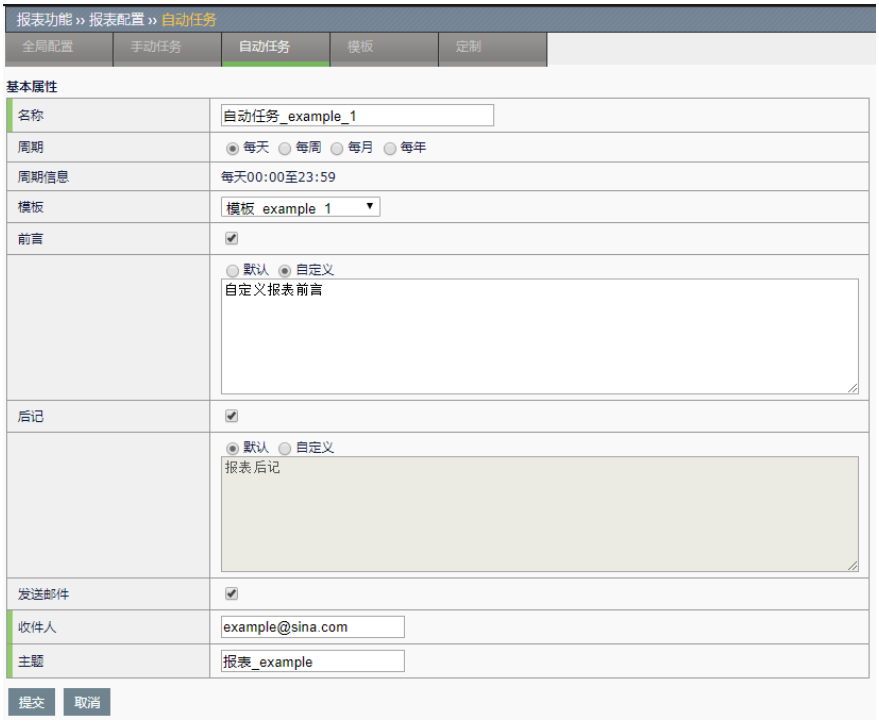
若需要给报表添加前言后记，则在报表定制页面设定报表的前言后记，或者在报表任务中自定义单独的前言后记。

**配置步骤：**

**新建**报表模板，选择虚拟服务模块进行统计，选择“当前连接数”“新建连接数”“上行流量”等需要统计的若干项，勾选统计均值，勾选统计成员数据，统计对象选择“默认“即统计该虚拟服务下所有池和成员，**提交**配置，如下图：


**定制**报表的前言后记。

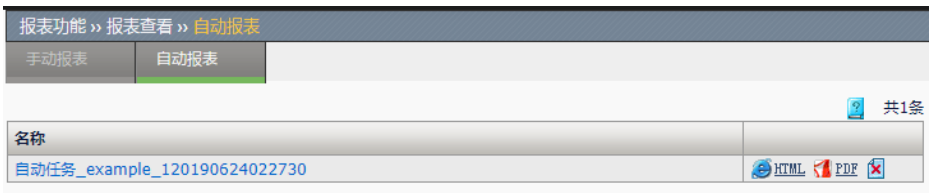

**新建**自动报表任务，选择任务执行的周期，选择刚刚创建的报表模板（勾选**发送邮件**，设定**收件人**和**邮件主题**，勾选前言后记，设定一个自定义的前言，后记引用全局的后记内容），**提交**配置。




进入**报表功能>报表配置>自动任务**，可看到刚刚创建的自动任务，如下图：


等待报表任务自动执行完成，在**报表功能>报表查看>自动报表**页面中，可

看到生成的报表，如图：


报表功能 ›› 报表查看 ›› 自动报表
手动报表
自动报表
共1条
名称
自动任务_example_120190624022730
HTML
PDF