# M9K系列多WAN链路负载均衡配置方法（WEB）

outbound链路负载均衡　zhiliao_5ilsv　2019-09-23 发表

## 组网及说明

**1 配置需求及说明**

**1.1 适用的产品系列**

本案例适用于如M9006、M9010、M9014等M9K系列的防火墙。

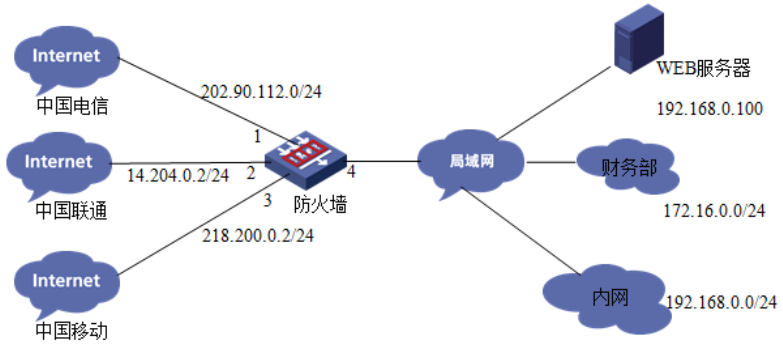
**1.2 配置需求及实现的效果**

某公司为达到业务流量快速转发和链路冗余需求申请了三条不同运营商的外网线路，需要实现如下需求：

1）要求内网用户访问目的地址为移动链路数据从移动链路转发、访问目的地址为联通链路数据从联通链路转发、访问目的地址为电信链路数据从电信链路转发需求。

2）财务部门因为经常访问网银等支付平台，目前不希望出口IP地址经常变化。指定财务数据从电信转发并希望当电信流量负载到带宽的90%后，后面流量负载到联通链路上。

**2 组网图**




说明：

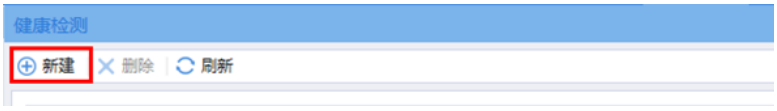
| ISP | 外网接口 | 公网地址/掩码 | 公网网关 |
|---|---|---|---|
| 移动 | 1/0/3 | 218.200.5.8/24 | 218.200.5.9 |
| 联通 | 1/0/2 | 14.204.0.2/24 | 14.204.0.1 |
| 电信 | 1/0/1 | 202.90.112.2/24 | 202.90.112.1 |

## 配置步骤

# 3 配置步骤

**3.1 创建链路健康监测条件**

#在防火墙界面“对象”>”健康监测”中创建健康检测策略。




#创建移动链路的健康性检测策略，目的地址为移动链路网关。


#创建联通链路的健康性检测策略，目的地址为联通链路网关。


#创建电信链路的健康性检测策略，目的地址为电信链路网关。


注：

1）防火墙早期版本健康检测选项位于“策略”>“负载均衡”>“全局配置”中，配置方法相同。

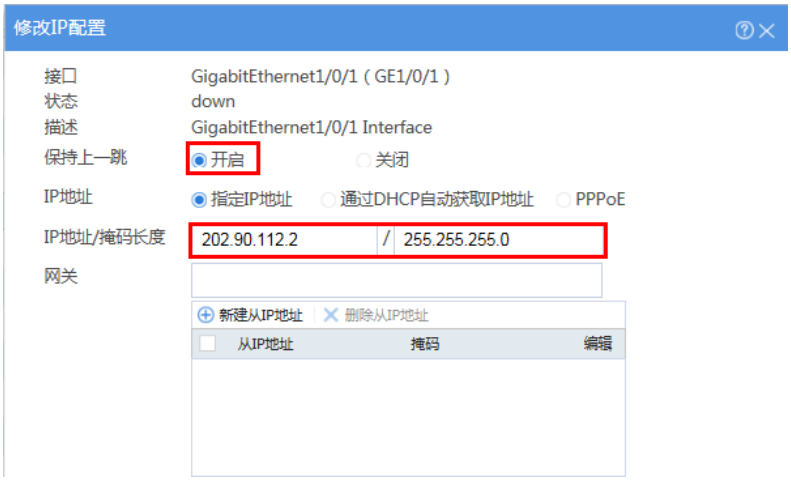
2）健康检测目的地址未添加情况下可以条用在不同的链路，默认检测直联下一跳是否可达。

**3.2 外网接口配置**

#在“网络”>”IP”中配置移动链路接口地址，并开启保存上一跳功能。


#在“网络”>”IP”中配置联通链路接口地址，并开启保存上一跳功能。


#在“网络”>”IP”中配置电信链路接口地址，并开启保存上一跳功能。




**3.3 开启各链路Nat地址转换功能**

#在“策略”>”NAT” >”NAT动态转换”中添加三条链路的地址转换策略。

配置电信接口NAT转换策略：


配置联通接口NAT转换策略：

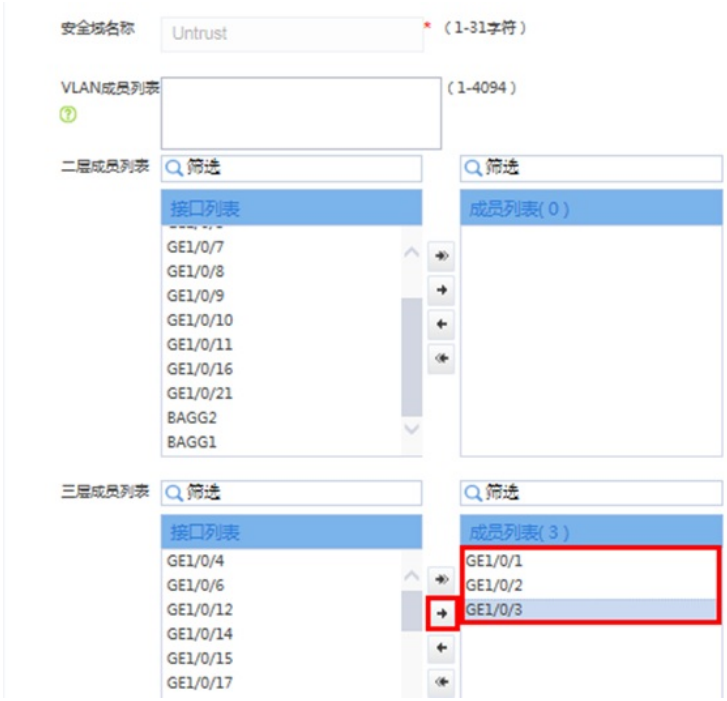

配置移动接口NAT转换策略：


### 3.4 内网网段及安全域配置

（略）

### 3.5 安全域及安全策略配置

#在“网络”>”安全域”中将三条外网链路接口移动至不信任（untrust）区域。




#在"策略">"安全策略"中选择新建安全策略。


#创建全放通的安全策略，因为本章内容重点涉及负载均衡，安全策略采用最简配置，策略名称为"pass"、源安全域为"any"、目的安全域为"any"，其余配置均为默认，配置完成后点击确定。


注：

1）防火墙早期版本在源安全域和目的安全域中没有名称为"any"安全域，建议源安全域将所有安全域勾选、目的安全域将所有安全域勾选的方法实现流量放通。

2）安全策略请按照现场需求进行调整，防火墙不建议配置全放通的安全策略。

**3.6 路由设置**

#在"网络">"路由">"静态路由"中新建IPV4静态路由，并设置路由优先级，防止负载均衡策略异常导致网络中断，设置电信为流量转发的默认路径。

配置电信链路路由：

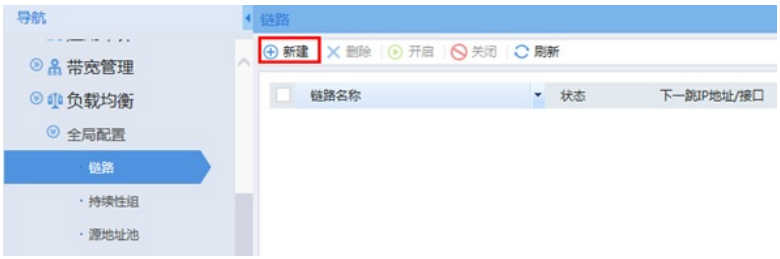

配置联通链路路由：


配置移动链路路由：


注：路由优先级越小路由越优先。

**3.7 创建负载均衡中的链路**

#在“策略”>“负载均衡”>“全局配置”>“链路”中新建三条链路。




**3.7.1 创建电信链路**

将电信链路带宽调整为100M，设置带宽繁忙比当带宽利用率超过90%*100M=90M，新建session会负载到其他链路。


### 3.7.2 创建联通链路

将链路名称设置为“联通链路”、下一跳地址设置为联通链路对应的网关地址：14.204.0.1。


### 3.7.3 创建移动链路

将链路名称设置为“移动链路”、下一跳地址设置为移动链路对应的网关地址：218.200.5.9。


### 3.7.4 配置财务链路

将链路名称设置为“财务链路”、下一跳地址设置为电信链路对应的网关地址：202.90.112.1。


### 3.8 导入运营商ISP路由表

防火墙运营商ISP路由表下载链接：

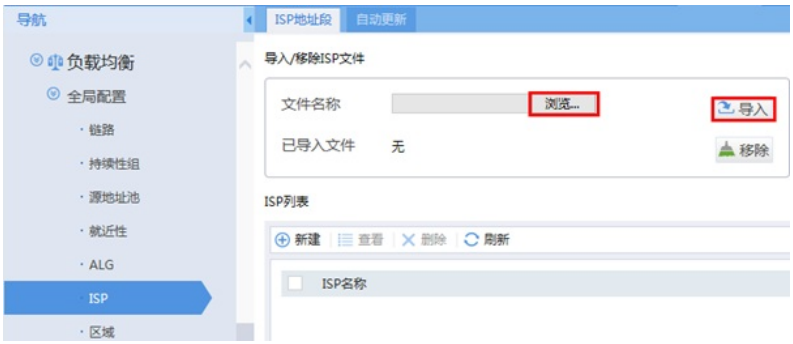
http://www.h3c.com/cn/Service/Document_Software/Software_Download/IP_Security/ISP_File/LB_ISP_File/

官网ISP路由表文件路径：

首页>产品支持与服务>文档与软件>软件下载>安全>H3C ISP地址表项文件


注：下载账号密码为：yx800/01230123

#在“策略”>“负载均衡”>“全局配置”>“ISP”中将下载的IPS文件选中后导入。




导入成功后在ISP列表中出现各运营商的路由表：


### 3.9 创建负载均衡规则流量匹配特征

#在“策略”>“负载均衡”>“链路负载均衡 ”>“流量特征”中新建流量特征规则。


#### 3.9.1 建立电信负载规则匹配电信ISP表

#在Match规则中新建匹配规则，其中类型为ISP、ISP为chinatel（电信）。


### 3.9.2 建立联通负载规则匹配联通ISP表

#在Match规则中新建匹配规则，其中类型为ISP、ISP为cnc（联通）。


### 3.9.3 建立移动负载规则匹配移动ISP表

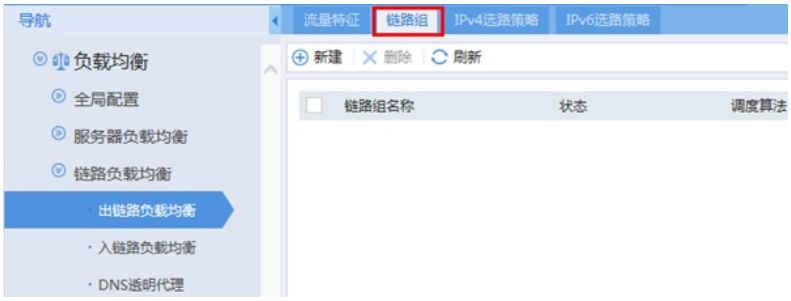
#在Match规则中新建匹配规则，其中类型为ISP、ISP为cmcc（移动）。


### 3.9.4 建立财务负载规则匹配172.16.0.0财务网段

#在Match规则中新建匹配规则，其中类型为源IPV4、IPV4地址为172.16.0.0、掩码长度为24。


### 3.10 创建链路组与链路绑定

#在“策略”>“负载均衡”>“链路负载均衡 ”>“出链路负载均衡 ” >“链路组”中点击新建。




#### 3.10.1 配置电信链路组

链路组名称设置为“电信链路组”、健康性检测方法设置选择“china-nqa”、成员列表中点击添加按钮添加电信链路、链路故障处理方式为”重定向连接”。


#### 3.10.2 配置联通链路组

链路组名称设置为“联通链路组”、健康性检测方法设置选择“cnc-nqa”、成员列表中点击添加按钮添加联通、链路故障处理方式为”重定向连接”。


### 3.10.3 配置移动链路组

链路组名称设置为“移动链路组”、健康性检测方法设置选择“cmcc-nqa”、成员列表中点击添加按钮添加移动链路、链路故障处理方式为”重定向连接”。


### 3.10.4 配置财务链路组

链路组名称设置为“财务链路组”、健康性检测方法设置选择“china-nqa”、成员列表中点击添加按钮添加财务链路、链路故障处理方式为”重定向连接”。


注：

设置链路失败的reschedule：重定向连接，即把连接重定向到链路组中其它可用的链路上。

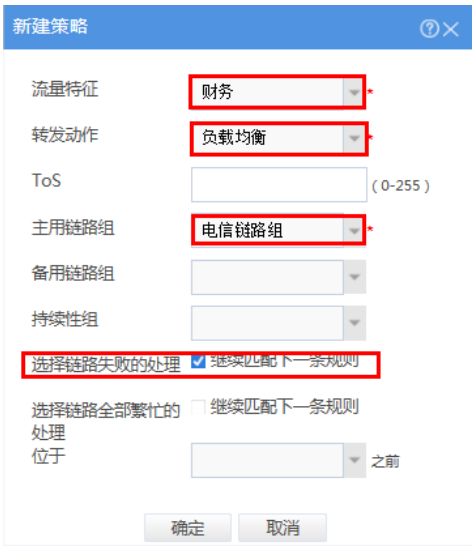
### 3.11 创建IPV4选路策略

#在“策略”>“负载均衡”>“链路负载均衡 ”>“出链路负载均衡 ” >“IPV4选路策略”中开启负载均衡服务并新建策略。


注：default为系统默认策略无法删除。

#### 3.11.1 创建财务链路的选路策略

流量特征选择”财务”、转发动作选择“负载均衡”、主用链路选择“电信链路组”、选择链路失败处理方式为继续匹配下一条策略。

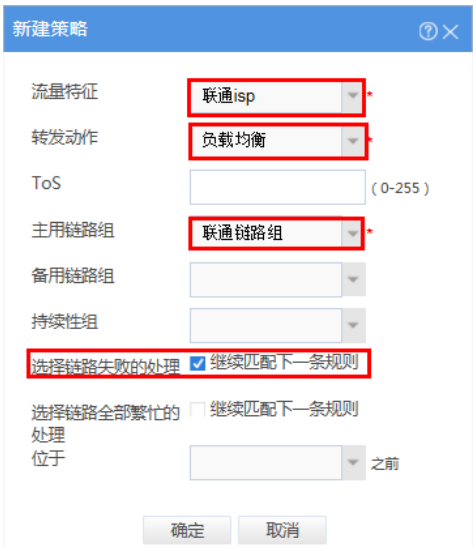



#### 3.11.2 创建电信链路的选路策略

流量特征选择电信ISP、转发动作选择“负载均衡”、主用链路选择“电信链路组”、选择链路失败处理方式为继续匹配下一条策略。


### 3.11.3 创建联通链路的选路策略

流量特征选择联通ISP、转发动作选择“负载均衡”、主用链路选择“联通链路组”、选择链路失败处理方式为继续匹配下一条策略。




### 3.11.4 创建移动链路的选路策略

流量特征选择移动ISP、转发动作选择“负载均衡”、主用链路选择“移动链路组”、选择链路失败处理方式为继续匹配下一条策略。


### 3.11.5 将默认的“default”策略转发规则设置为转发

将默认的“default”策略转发规则设置为转发，使既不匹配财务也不匹配ISP流量特征的数据按照路由表转发。


### 3.12 保存配置

在设备右上角选项卡中保存配置。


### 3.13 配置验证

#### 3.13.1 测试电信链路

在内网找一台地址为192.168.0.2的电脑，访问外网一个地址看是从哪个接口出？用来判断ISP路由是否配置正确？将外网模拟设备的IP地址修改为1.4.1.1进行测试。

设备内置的电信路由表：


Teacert结果：


防火墙会话：

```
Initiator:
  Source      IP/port: 192.168.0.2/1
  Destination IP/port: 1.4.1.1/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/15
  Source security zone: Trust
Responder:
  Source      IP/port: 1.4.1.1/5
  Destination IP/port: 202.90.112.2/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: Untrust
State: ICMP_REPLY
Application: ICMP
Start time: 2017-11-24 18:09:27  TTL: 29s
Initiator->Responder:            0 packets          0 bytes
Responder->Initiator:            0 packets          0 bytes
```

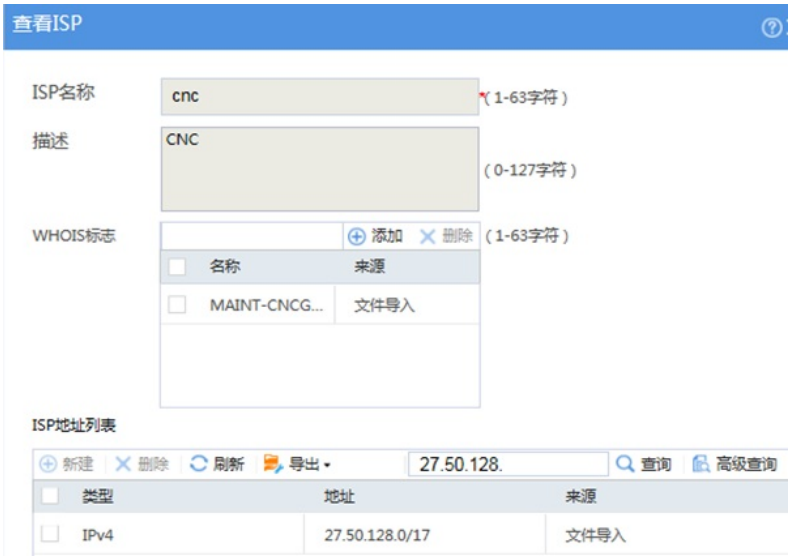
查看数据是否从对应链路组转发。

```
<FW>display loadbalance link statistics
Slot 1:
Loadbalance link: chinanet-isp
  Total connections: 1
  Active connections: 1
  Max connections: 1
  Connections per second: 0
  Max connections per second: 1
  Downstream traffic: 240 bytes
  Upstream traffic: 240 bytes
  Throughput: 0 bytes/s
  Inbound throughput: 0 bytes/s
  Outbound throughput: 0 bytes/s
  Max throughput: 120 bytes/s
  Max inbound throughput: 60 bytes/s
  Max outbound throughput: 60 bytes/s
  Received packets: 4
  Sent packets: 4
  Dropped packets: 0
```

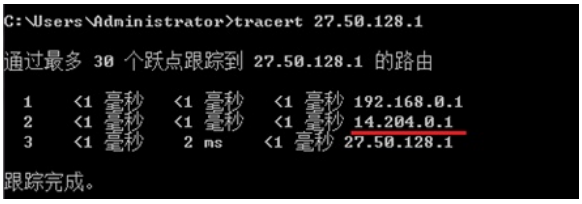
### 3.13.2 测试联通链路

在内网找一台地址为192.168.0.2的电脑，访问外网一个地址看是从哪个接口出？用来判断ISP路由是否配置正确？将外网模拟设备的IP地址修改为27.50.128.1进行测试。

设备内置的联通路由表：




Teacert结果：




防火墙会话：

```
Initiator:
  Source      IP/port: 192.168.0.2/1
  Destination IP/port: 27.50.128.1/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/15
  Source security zone: Trust
Responder:
  Source      IP/port: 27.50.128.1/22
  Destination IP/port: 14.204.0.2/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/2
  Source security zone: Untrust
State: ICMP_REPLY
Application: ICMP
Start time: 2017-11-24 18:23:32  TTL: 29s
Initiator->Responder:            0 packets          0 bytes
Responder->Initiator:            0 packets          0 bytes
```

.

### 3.13.3 测试移动链路

在内网找一台地址为192.168.0.2的电脑，访问外网一个地址看是从哪个接口出？用来判断ISP路由是否配置正确？将外网模拟设备的IP地址修改为43.251.244.1进行测试。

设备内置的移动路由表：


Teacert结果：

```
C:\Users\Administrator>tracert 43.251.244.1

通过最多 30 个跃点跟踪到 43.251.244.1 的路由

  1    <1 毫秒   <1 毫秒   <1 毫秒 192.168.0.1
  2    <1 毫秒   <1 毫秒   <1 毫秒 218.200.5.8
  3    <1 毫秒   <1 毫秒   <1 毫秒 43.251.244.1

跟踪完成。
```

防火墙会话：

```
Initiator:
  Source      IP/port: 192.168.0.2/1
  Destination IP/port: 43.251.244.1/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/15
  Source security zone: Trust
Responder:
  Source      IP/port: 43.251.244.1/2
  Destination IP/port: 218.200.5.9/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/3
  Source security zone: Untrust
State: ICMP_REPLY
Application: ICMP
Start time: 2017-11-24 18:17:10  TTL: 29s
Initiator->Responder:            0 packets          0 bytes
Responder->Initiator:            0 packets          0 bytes
```

### 3.13.4 测试总结

测试结果符合需求预期，可以达到数据的准确转发。

## 配置关键点