**IPSECVPN冗余双中心备份配置方法**

**2023年4月3日**

目录

[1、测试需求 3](#_Toc131426254)

[2、测试网络拓扑示意图 3](#_Toc131426255)

[3、配置过程 3](#_Toc131426256)

[3.1、分支防火墙（模拟北京） 3](#_Toc131426257)

[3.1.1、配置网口IP 3](#_Toc131426258)

[3.1.2、配置默认路由 4](#_Toc131426259)

[3.1.3、配置去往总部防火墙1阶段1 4](#_Toc131426260)

[3.1.4、配置去往总部防火墙1阶段2 5](#_Toc131426261)

[3.1.5、配置去往总部防火墙2阶段1 5](#_Toc131426262)

[3.1.6、配置去往总部防火墙2阶段2 5](#_Toc131426263)

[3.1.7、配置去往总部IPSECVPN隧道路由 6](#_Toc131426264)

[3.1.8、配置安全策略 6](#_Toc131426265)

[3.2、配置总部防火墙1（天津） 7](#_Toc131426266)

[3.2.1、配置网口IP 7](#_Toc131426267)

[3.2.2、配置默认路由 7](#_Toc131426268)

[3.2.3、配置去往分支IPSECVPN阶段1 7](#_Toc131426269)

[3.2.4、配置去往分支IPSECVPN阶段2 8](#_Toc131426270)

[3.2.5、配置去往分支IPSECVPN隧道路由 8](#_Toc131426271)

[3.2.6、配置安全策略 9](#_Toc131426272)

[3.3、配置总部防火墙2（上海） 9](#_Toc131426273)

[3.3.1、配置网口IP 9](#_Toc131426274)

[3.3.2、配置默认路由 9](#_Toc131426275)

[3.3.3、配置去往分支IPSECVPN阶段1 10](#_Toc131426276)

[3.3.4、配置去往分支IPSECVPN阶段2 10](#_Toc131426277)

[3.3.5、配置去往去往分支IPSECVPN隧道路由 11](#_Toc131426278)

[3.3.6、配置安全策略 11](#_Toc131426279)

[4、测试效果 12](#_Toc131426280)

[4.1、配置IPSECVPN状态监控 12](#_Toc131426281)

[4.3、删除monitor。 13](#_Toc131426282)

[4.4、重新配置monitor。 13](#_Toc131426283)

[4.5、关闭总部防火墙1的外网口 14](#_Toc131426284)

[5、注意事项 15](#_Toc131426285)

# 1、概述

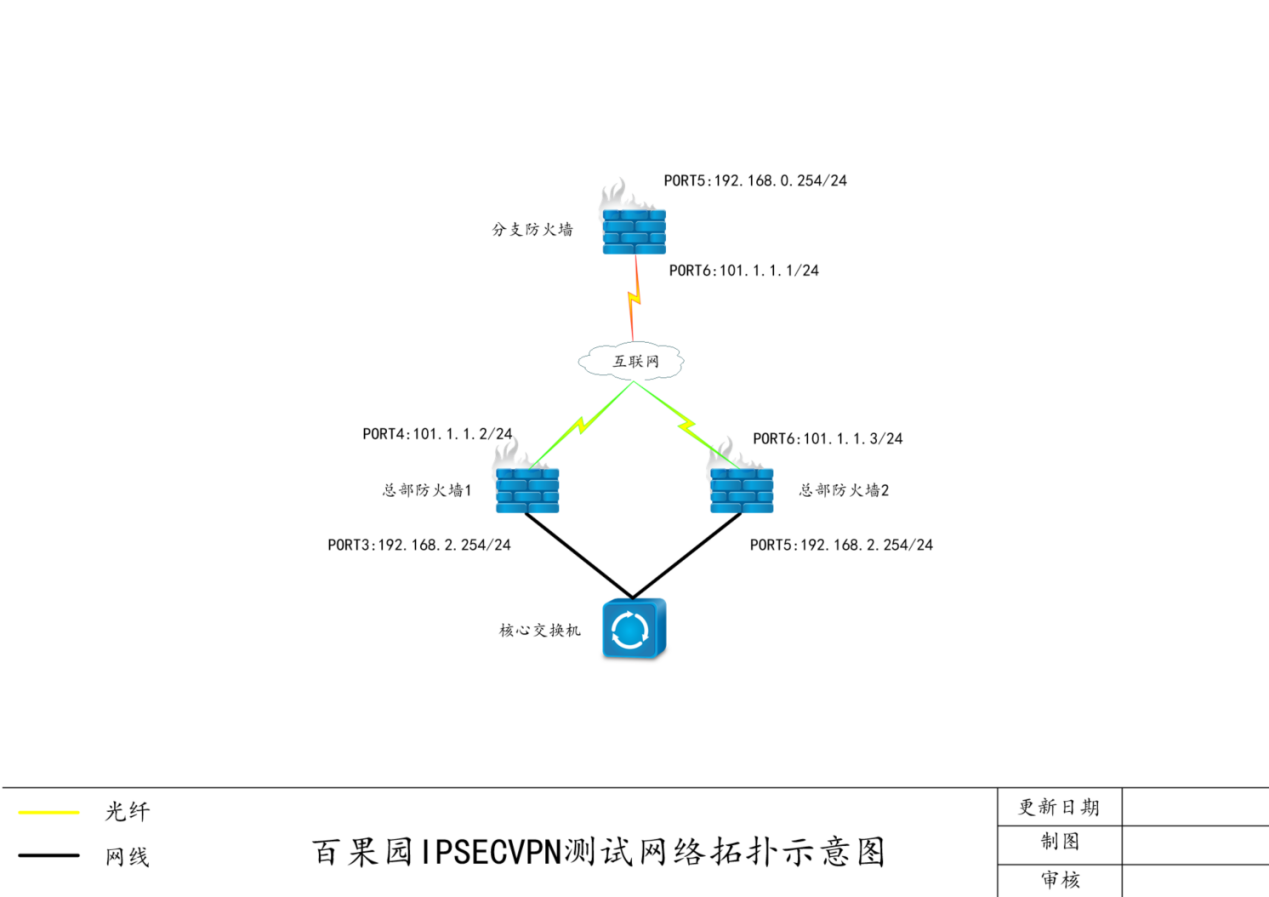
由于有多个分支需要跟总部对接IPSECVPN，预计总部防火墙压力较大，准备在总部部署两台防火墙和分支对接，并且指定一部分分支主连接总部防火墙1，一部分分支主连接总部防火墙2，如果总部防火墙1出问题，主连接总部防火墙1的分支还可以和总部防火墙2对接，如果总部防火墙2出问题，主连接总部防火墙2的分支还可以和总部防火墙1对接。实现总部防火墙和多个分支对接IPSECVPN可以负载分担和相互备份，尽力保证业务的稳定性和高可用性。

配置方法有两种方法：

方法一、在分支机构配置两个ipsec通道，分别连接到两个中心端，这样就可以起到备份作用。

方法二、在分支机构配置两个ipsec通道，设置一个通道monitor另外一个通道，当被monitor通道down时，备份通道就可以启动起来。该方法与方法一区别在于，备份通道在备份状态下是不连接到中心端的，可以为中心端节省通道资源。

# 2、网络拓扑示意图

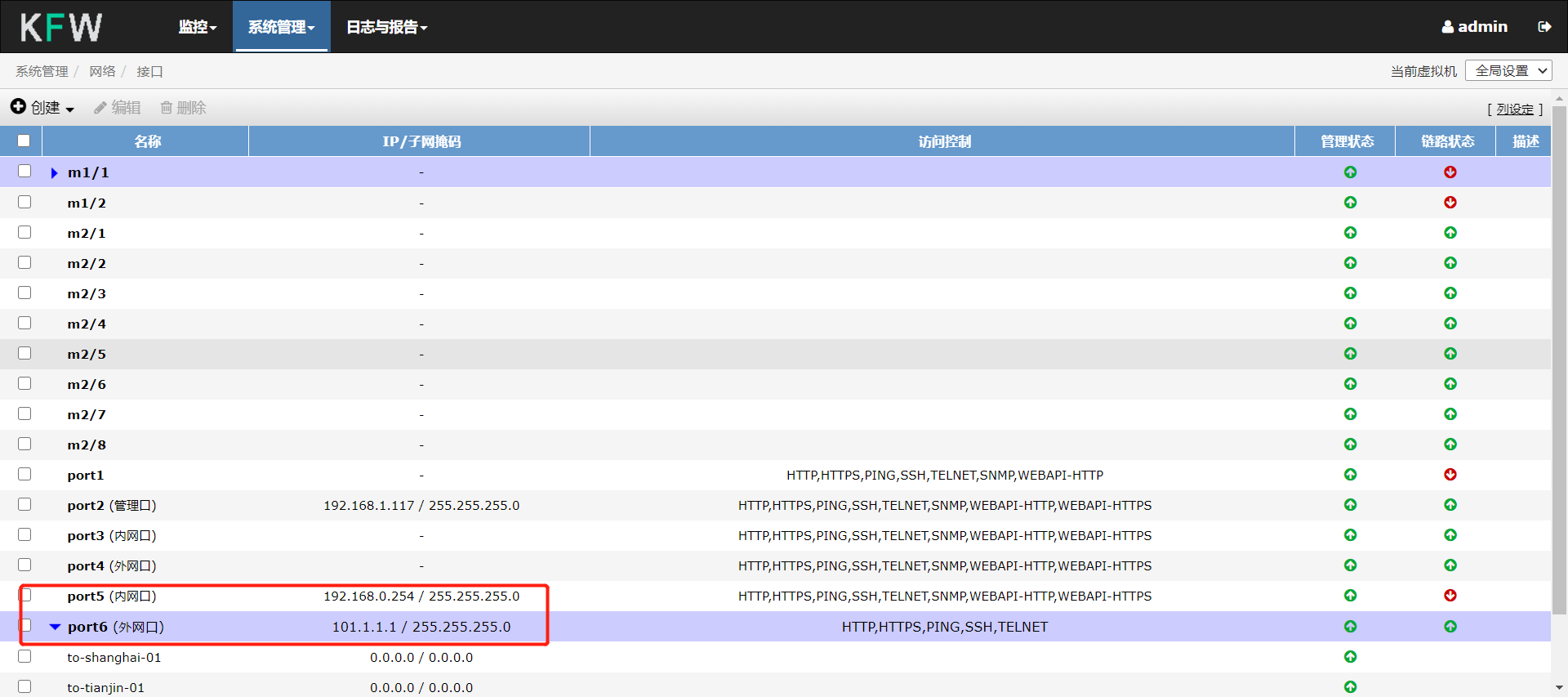


# 3、配置过程

## 3.1、分支防火墙（模拟北京）

### 3.1.1、配置网口IP

配置分支内网口地址为192.168.0.254/255.255.255.0。外网口地址为101.1.1.1/255.255.255.0。



### 3.1.2、配置默认路由

配置默认路由下一跳指向101.1.1.254，



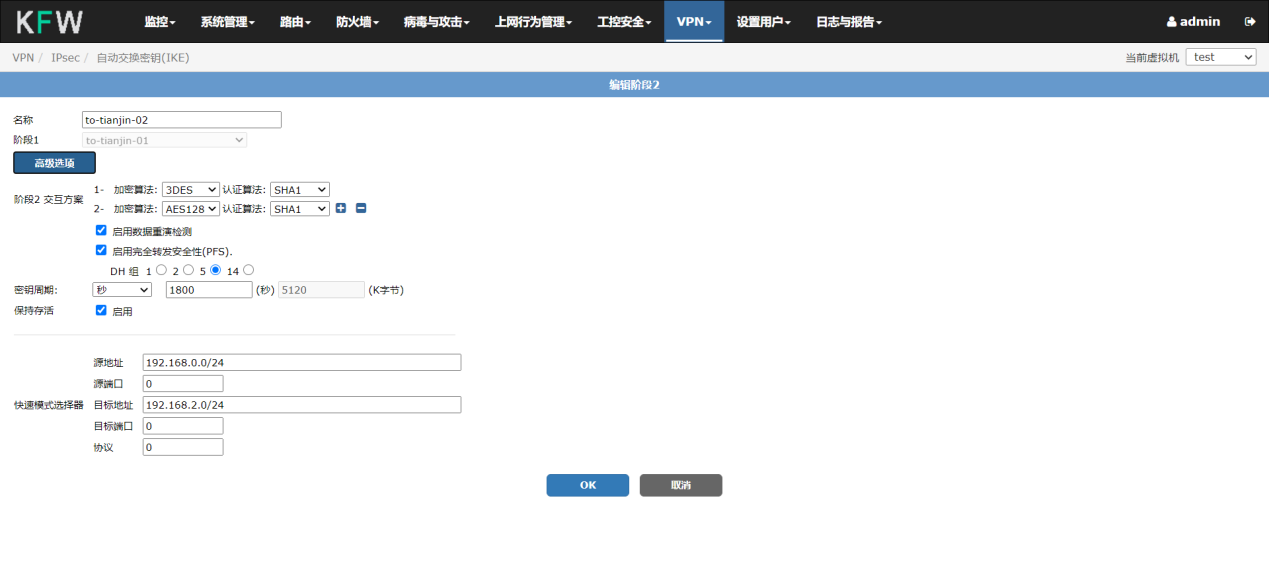
### 3.1.3、配置去往总部防火墙1阶段1

配置去往总部防火墙1的接口模式IPSECVPN阶段1。



### 3.1.4、配置去往总部防火墙1阶段2

配置去往总部防火墙1的接口模式IPSECVPN阶段2。



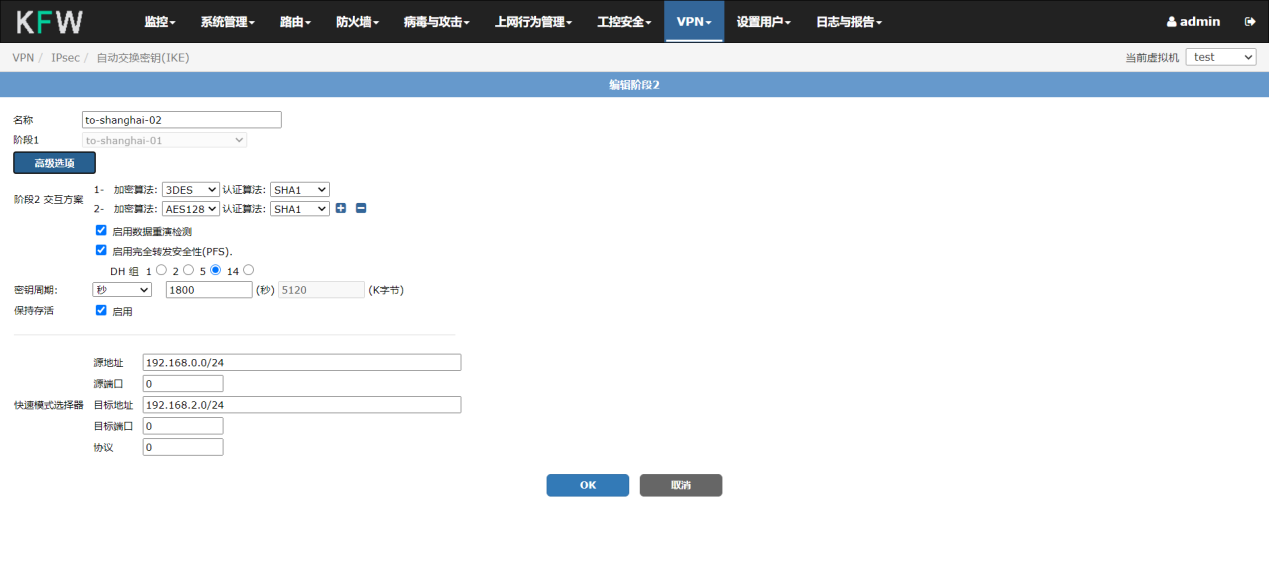
### 3.1.5、配置去往总部防火墙2阶段1

配置配置去往总部防火墙2的接口模式IPSECVPN阶段1。



### 3.1.6、配置去往总部防火墙2阶段2

配置去往总部防火墙2的接口模式IPSECVPN阶段2。



### 3.1.7、配置去往总部IPSECVPN隧道路由

配置去往总部内网网段的路由下一跳分别交给两条IPSECVPN隧道。



### 3.1.8、配置安全策略

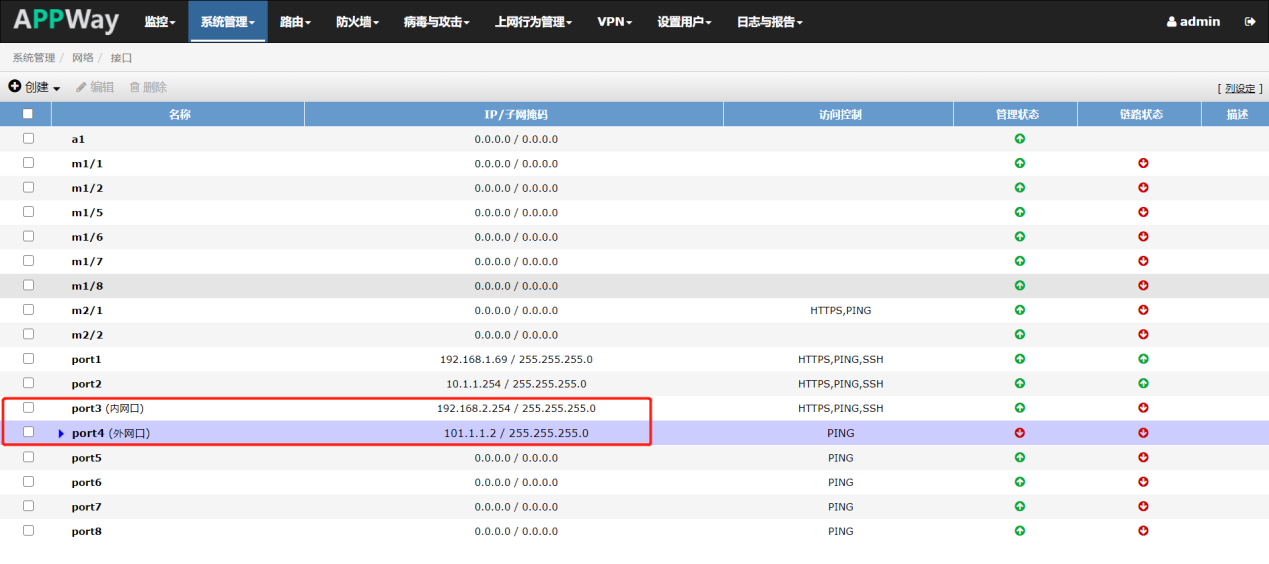
配置内网到两个VPN隧道的双向放通策略。



## 3.2、配置总部防火墙1（天津）

### 3.2.1、配置网口IP

配置内网口IP为192.168.2.254/255.255.255.0，外网口IP为101.1.1.2/255.255.255.0。



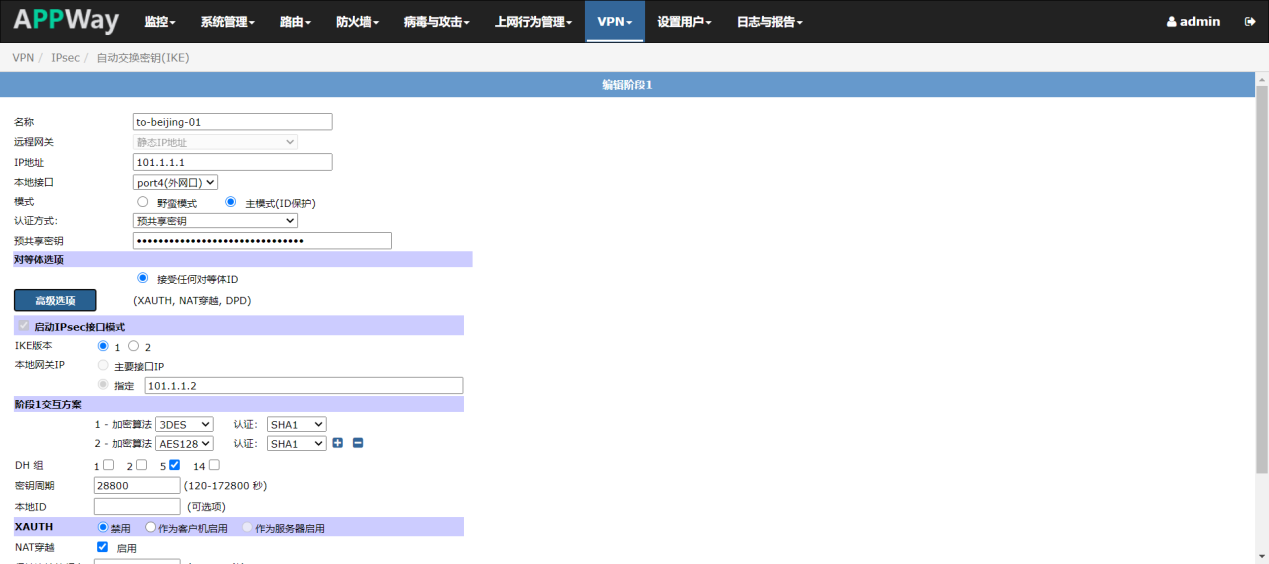
### 3.2.2、配置默认路由

配置默认路由，下一跳指向101.1.1.254。



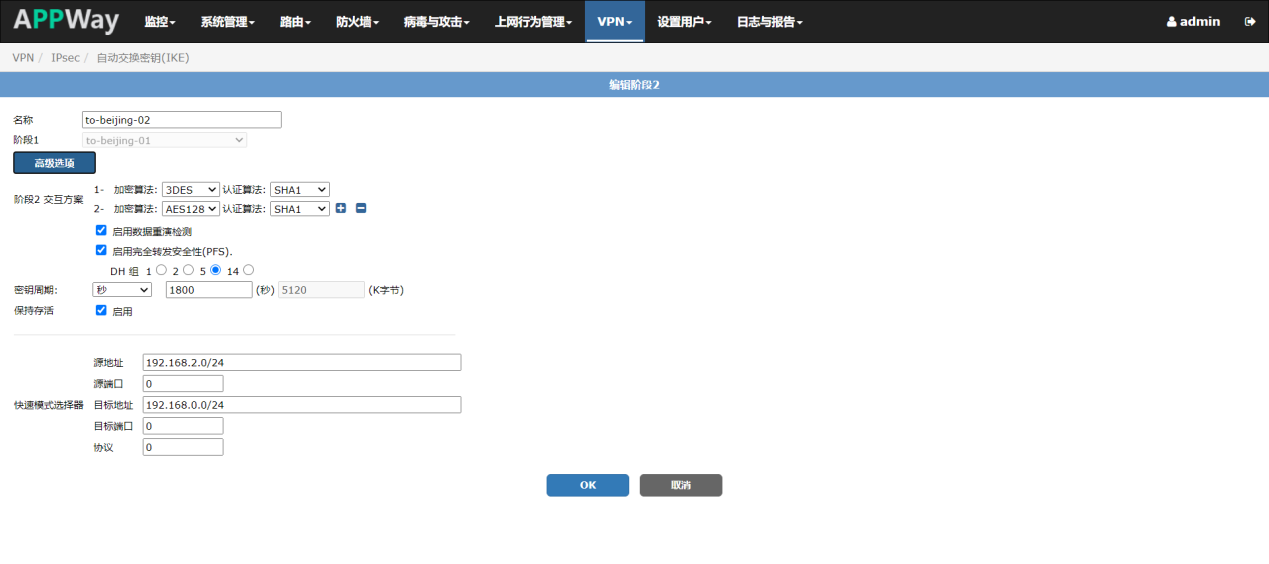
### 3.2.3、配置去往分支IPSECVPN阶段1

配置去往分支的IPSECVPN接口模式阶段1。



### 3.2.4、配置去往分支IPSECVPN阶段2

配置去往分支的IPSECVPN接口模式阶段2。



### 3.2.5、配置去往分支IPSECVPN隧道路由

配置去往分支内网网段路由，下一跳交给IPSECVPN隧道。



### 3.2.6、配置安全策略

放通总部内网网段到IPSECVPN内网网段的安全策略。



## 3.3、配置总部防火墙2（上海）

### 3.3.1、配置网口IP

配置内网口IP为192.168.2.254/255.255.255.0。外网口IP为101.1.1.3/255.255.255.0。



### 3.3.2、配置默认路由

配置默认路由，下一跳交给192.168.1.1（此处为模拟测试环境，设备外网口都是通过交换机直连，网关可以随意配置，实际生产环境应指向网络的外网网关地址）。



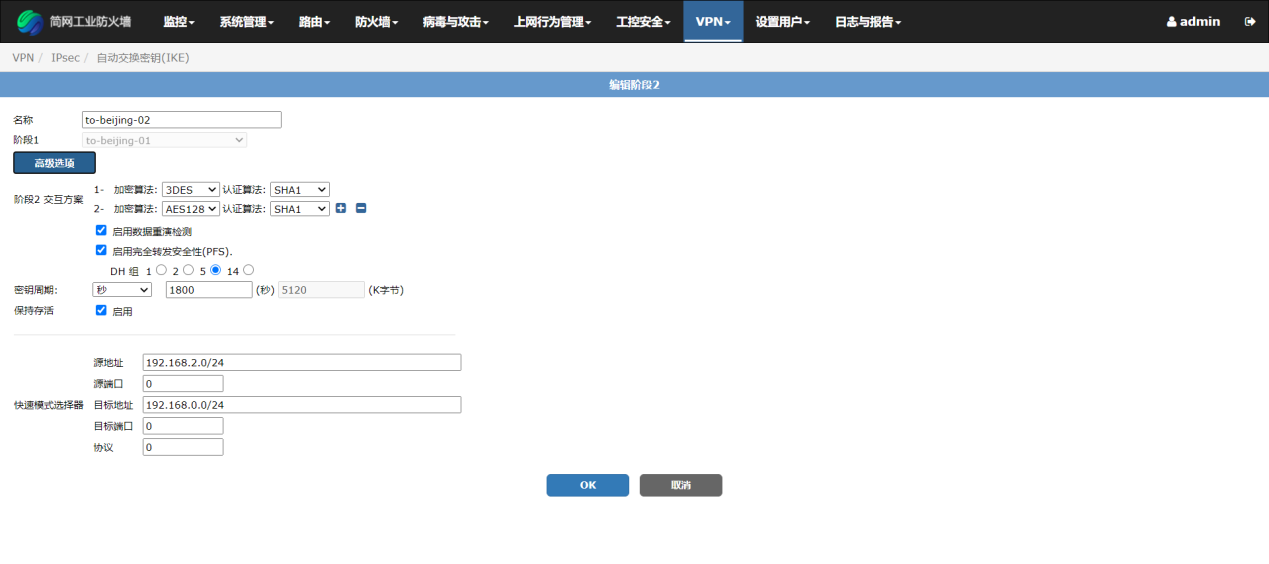
### 3.3.3、配置去往分支IPSECVPN阶段1

配置和分支对接IPSECVPN接口模式阶段1。



### 3.3.4、配置去往分支IPSECVPN阶段2

配置和分支对接IPSECVPN接口模式阶段2。



### 3.3.5、配置去往去往分支IPSECVPN隧道路由

配置去往分支内网网段的路由，下一跳交给IPSECVPN隧道。



### 3.3.6、配置安全策略

配置总部内网网段到分支内网网段的双向放通安全策略。



# 4、测试效果

## 4.1、配置IPSECVPN状态监控

在分支去往总部防火墙2阶段1中通过命令set monitor-phase1 to-tianjin-01，让分支去往总部防火墙2阶段1监控总部防火墙1IPSECVPN阶段1状态，实现分支（去往总部防火墙1IPSECVPN状态正常时，去往总部防火墙2阶段1关闭，一旦检测分支去往总部防火墙1IPSECVPN状态不正常，去往总部防火墙2阶段1立即开启。保证实现一部分分支主对接总部防火墙1 IPSECVPN。一部分分支主对接总部防火墙2 IPSECVPN。一旦主对接有问题，切换到另一台总部防火墙对接IPSECVPN。

配置命令截图

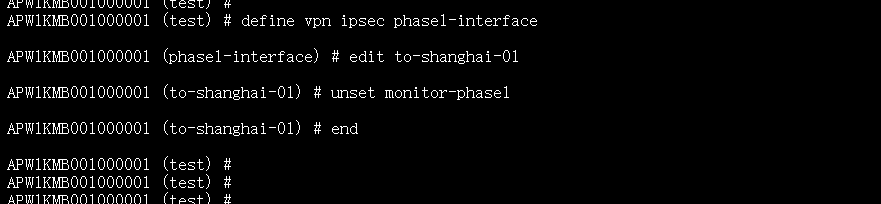


**4.2、查看配置monitor后VPN状态**

配置监控后，IPSECVPN正常状态为去往总部防火墙1VPN状态正常，去往总部防火墙2VPN状态关闭。



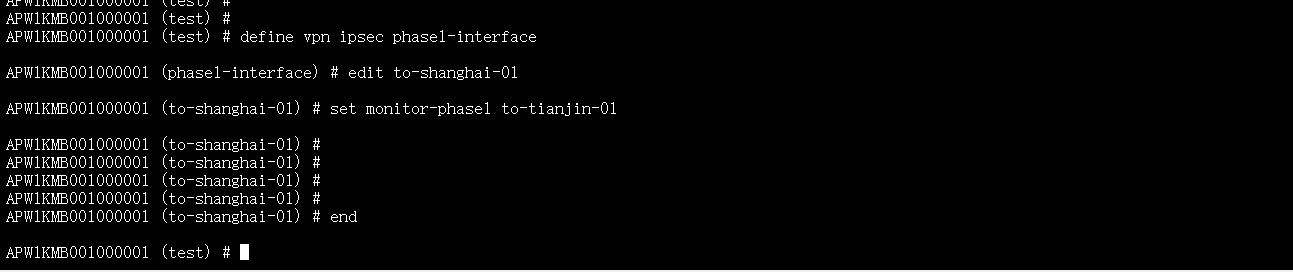
## 4.3、删除monitor。



查看两条VPN都能建立。



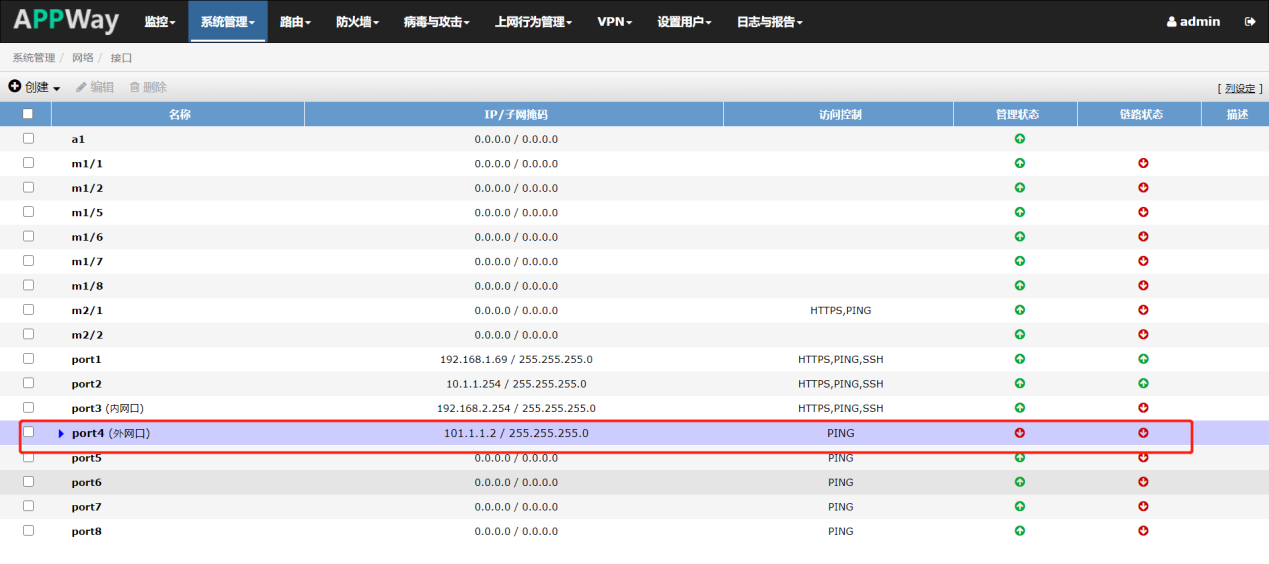
## 4.4、重新配置monitor。



去往总部防火墙1状态正常，去往总部防火墙2状态关闭。



## 4.5、关闭总部防火墙1的外网口



查看去往总部防火墙1状态关闭，去往总部防火墙2状态开启。



# 5、注意事项

1、必须配置为接口模式IPSECVPN，因为只有接口模式IPSECVPN支持配置阶段1 monitor,策略模式不支持。

2、IPSECVPN排障

可以在命令行使用debug命令查看VPN建立过程和出现的报错。

debug ipsecvpn命令

dump debug enable

dump debug app ike -1