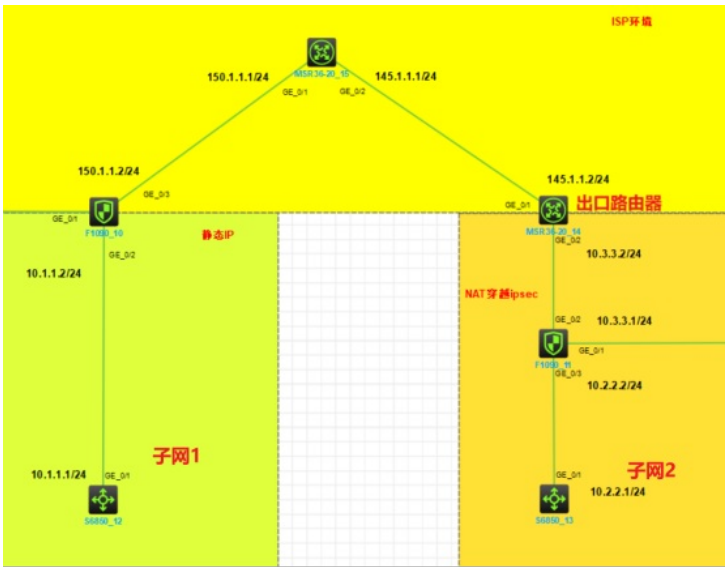
F1090 IPSEC典型组网配置案例（NAT穿越）

IPSec VPN　zhiliao_FQbqDB　2022-12-17 发表

组网及说明

本案例采用H3C HCL模拟器的F1090防火墙来模拟IPSEC NAT穿越的典型组网配置。在网络拓扑图中存在子网1和子网2。为了保障子网1和子网2相互传输数据的安全性，因此需要在FW10与FW11采用建立IPSEC VPN隧道，由于FW11的出接口地址不固定且出口路由器为NAT设备，因此采用IKE野蛮模式。



配置步骤

1、按照网络拓扑图正确配置IP地址，确保主干链路网络互通正常

2、FW10，FW11和出口路由器均配置NAT

3、FW10与FW11的互联接口加入安全域，并放通域间策略

4、FW1与FW2建立IPSEC VPN隧道，采用IKE野蛮模式

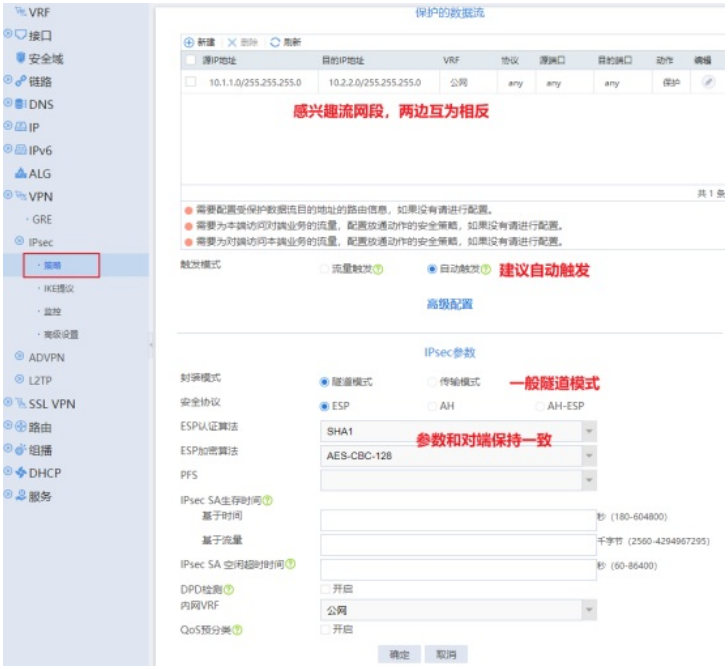
配置关键点

一、主要设备的配置（web和命令行）

出口路由器：

```
interface GigabitEthernet0/1 //配置接口地址和接口SNAT
 port link-mode route
 combo enable copper
 ip address 145.1.1.2 255.255.255.0
 nat outbound 3000
#
interface GigabitEthernet0/2 //配置接口地址
 port link-mode route
 combo enable copper
 ip address 10.3.3.2 255.255.255.0
#
 ip route-static 0.0.0.0 0 145.1.1.1 //默认路由
#
acl advanced 3000 //定义用于SNAT的ACL
 rule 1 permit ip counting
```

FW10：



interface GigabitEthernet1/0/2 //定义内网口

 port link-mode route
 combo enable copper
附件下载 ip address 10.255.255.255 255.255.255.0
 #
 interface GigabitEthernet1/0/3 //定义外网口和应用ipsec策略