IPSec VPN 孔德飞 2022-03-22 发表

组网及说明	
组网如下:	
中心与分支建立	IPSEC,中心使用模板的方式,并开启反向路由注入功能,使得中心
生成到分支10.1	.0.1的静态路由,下一跳是中心应用IPSEC接口的下一跳,本案例即1.1.1.2
中心与分支的公	网地址分别为1.1.1.1与1.1.1.2,中心与分支的私网地址分别为10.0.0.1与10.1.0.1

lp0:10.0.0.1		lp0:10.1.0.1
	1.1.1.1	1.1.1.2
	GE_0/1	GE_0/1
F1060_1		F1060_2
中心		分支

## 配置步骤

配置步骤 中心: 安全域及安全策略的配置 security-zone name Trust import interface GigabitEthernet1/0/1

security-policy ip rule 0 name 0 action pass

接口配置 interface LoopBack0 ip address 10.0.0.1 255.255.255.255

interface GigabitEthernet1/0/1 port link-mode route combo enable copper ip address 1.1.1.1 255.255.255.0 ipsec apply policy map1

## IKE与IPSEC的配置(关键是要在ipsec策略模板视图下开启反向路由注入功能)

ipsec transform-set tran1 esp encryption-algorithm des-cbc esp authentication-algorithm sha1 # ipsec policy-template temp1 1 transform-set tran1 ike-profile profile1 reverse-route dynamic reverse-route preference 100 reverse-route tag 1000 # ipsec policy map1 10 isakmp template temp1 # ike profile profile1 keychain key1 match remote identity address 1.1.1.2 255.255.255.0 # ike proposal 1 # ike keychain key1 pre-shared-key address 1.1.1.2 255.255.255.255 key simple 123456

## 分支:

安全域及安全策略的配置 security-zone name Trust import interface GigabitEthernet1/0/1

security-policy ip rule 0 name 0 action pass

## 接口配置

interface LoopBack0

配置态键感 10.1.0.1 255.255.255.255

配置关键点: ihterfate/Coig 始紀唐朗模板/0/1 port link小的UBSGCG策略中需要开启反向路由注入功能 comb的或需要 运动中心私网地址的路由 ip address 1.1.1.2 255.255.255.0 ipsec apply policy map1