两台F5040主模式对接ipsec vpn且一端设备接口加入vpn-instance

IPSec VPN 证书 VPN实例 李欣 2019-06-17 发表

组网及说明

F5040_1-1/0/1----------专网--------reth1-F5040_2_IRF---环回lo0

其中F5040_2_IRF的外网口reth1及建立vpn使用的地址lo0加入vpn实例，与远端F5040_1对接ipsec vpn

问题描述

跨专网对接ipsec vpn时设备部分接口加入vpn-instance

过程分析

带有vpn实例的ipsec对接中注意在部分参数中必须带上vpn-instance否则vpn无法正常建立

解决方法

1、不带实例侧F5040_1配置，安全策略正常放通；

```
interface Route-Aggregation1
 ip address 10.101.1.34 255.255.255.252

 interface LoopBack999
 ip address 3.3.3.3 255.255.255.255

interface GigabitEthernet1/0/1
 ip address 117.x.x.46 255.255.255.252
ipsec apply policy uni

acl advanced 3333
rule 1 permit ip source 10.101.1.34 0 destination 10.0.54.254 0
rule 5 permit ip source 3.3.3.3 0 destination 3.3.3.4 0
#
ipsec policy uni 90 isakmp
transform-set 1
security acl 3333
local-address 117.x.x.46
remote-address 113.x.x.14
ike-profile 1
sa duration time-based 3600
#
ike profile 1
keychain 1
local-identity address 117.x.x.46
match remote identity address 111.x.x.254 255.255.255.255
match local address GigabitEthernet1/0/1
proposal 1
#
proposal 1
 #
ike keychain 1
pre-shared-key address 111.x.x.254 255.255.255.255 key cipher $c$3$yLmco62beRq851i6O68iGJal
1ZzEVj7Q2g==

ipsec transform-set 1
esp encryption-algorithm 3des-cbc
esp authentication-algorithm md5

 ip route-static 0.0.0.0 0 117.x.x.45
```

2、带实例侧F5040_2_IRF 配置，放通安全策略需要带上vrf

```
ip vpn-instance 6uffjmj4198n58iff9qvgur2oh

interface Reth1    //外网口加入实例
 ip binding vpn-instance 6uffjmj4198n58iff9qvgur2oh
 ip address 10.x.x.2 255.255.255.0
```

```
 ipsec apply policy ipsecpolicy

interface LoopBack0   //对端ipsec指向本端地址所在接口
 ip binding vpn-instance 6uffjmj4198n58iff9qvgur2oh
 ip address 113.x.x.14 255.255.255.255

ipsec policy ipsecpolicy 90 isakmp
transform-set 1
security acl 3210
local-address 113.x.x.14
remote-address 117.x.x.46
ike-profile 1
sa duration time-based 3600

ike profile 1
 keychain 1
 local-identity address 113.x.x.14
 match remote identity address 117.x.x.46 255.255.255.255 vpn-instance
6uffjmj4198n58iff9qvgur2oh   //必须带vpn-instance
 match local address 113.x.x.14   vpn-instance 6uffjmj4198n58iff9qvgur2oh  //必须带vpn-instance

proposal 1

ipsec transform-set 1
esp encryption-algorithm 3des-cbc
esp authentication-algorithm md5

ike keychain 1 vpn-instance 6uffjmj4198n58iff9qvgur2oh   //必须带vpn-instance
pre-shared-key address 117.x.x.46 255.255.255.255 key cipher $c$3$urvNF+FT3HU43MbjdvOj+RUJ
hkPoCpSpsw==

acl advanced 3210
rule 0 permit ip vpn-instance 6uffjmj4198n58iff9qvgur2oh source 10.0.54.254 0 destination
10.101.1.34 0 counting   //保护数据流带实例
rule 5 permit ip vpn-instance 6uffjmj4198n58iff9qvgur2oh source 3.3.3.4 0 destination 3.3.3.3 0    //保
护数据流带实例

 ip route-static vpn-instance 6uffjmj4198n58iff9qvgur2oh 0.0.0.0 0 10.x.x.254   //vpn-instance添加默
认路由从reth1出
```