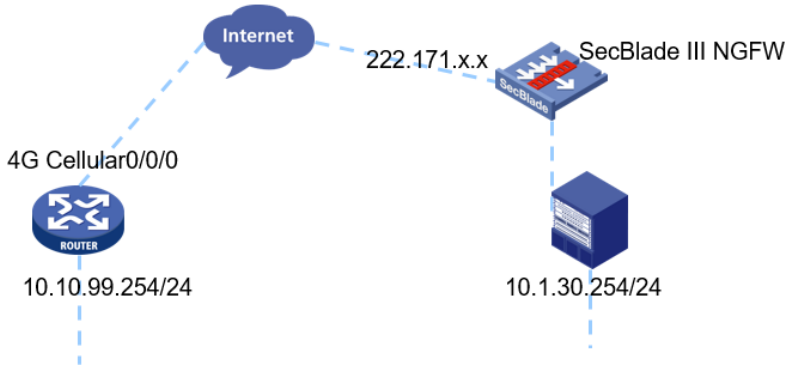
SecBlade III NGFW与华为AR100路由器野蛮模式ipsec对接不成功问题分析

IPSec VPN 刘宏宇 2019-11-26 发表

组网及说明

组网



问题描述

防火墙板卡G1/0/1接口固定ip作为总部与分支设备建ipsec，之前与分支H3C路由器固定ip主模式建立ipsec都成功，

目前新加了一个4G拨号的华为AR100路由器作为分支，使用野蛮模式总部模板方式建立ipsec不成功，查看没有ike sa。

过程分析

1、 查看FW策略配置，全部放通，且两端设备ping测试能通，说明两端公网可通；

```
#
object-policy ip Any-Any
rule 0 pass
#
object-policy ip any-local
rule 0 pass
#
object-policy ip local-any
rule 0 pass
#
zone-pair security source Any destination Any
object-policy apply ip Any-Any
#
zone-pair security source Any destination Local
object-policy apply ip any-local
#
zone-pair security source Local destination Any
object-policy apply ip local-any
#
```

2、 查看两端ike相关配置

本端FW：总部模板方式

```
#
acl advanced 3299
rule 0 permit ip source 10.1.30.0 0.0.0.255 destination 10.10.99.0 0.0.0.255
#
ipsec transform-set tran1
esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm sha1
#
ipsec policy-template 1 3
transform-set tran1
 security acl 3299
 local-address 222.171.x.x
ike-profile profile99
```

```
#
ipsec policy use1 10 isakmp
……
#
ipsec policy use1 20 isakmp
……
#
ipsec policy use1 100 isakmp template 1
#
ike profile profile99
keychain keychain99
dpd interval 10 retry 6 on-demand
exchange-mode aggressive
local-identity fqdn center
match remote identity fqdn branch_vpn
match local address GigabitEthernet1/0/1
#
ike keychain keychain99
match local address GigabitEthernet1/0/1
pre-shared-key hostname branch_vpn key cipher $c$3$rdbNXhHC0lKlegCJcjAU5hGziDVv8SvZEKkx
#
```

对端华为AR100配置：

```
#
acl name b_Cellular0/0/0_1 3999
 rule 5 permit ip source 10.10.99.0 0.0.0.255 destination 10.1.30.0 0.0.0.255
#
ike proposal 1
encryption-algorithm des
 dh group1
 authentication-algorithm sha1
 authentication-method pre-share
integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer branch_vpn1
undo version 2
 exchange-mode aggressive
pre-shared-key cipher %^%#J3M^8JnobMfrxmD,ic]4,`bq%:$!dTo@pBC{i>QK%^%#
ike-proposal 1
remote-id fqdn center
local-id fqdn branch_vpn
remote-address 222.171.x.x
#
ipsec policy branch_vpn 1 isakmp
security acl 3999
ike-peer branch_vpn1
proposal branch_vpn1
#
```

3、 FW的debug ike信息

```
*May 24 09:12:22:813 2019 CHIP-FW IKE/7/PACKET: -COntext=1; vrf = 0, src = 222.171.137.145, d
st = 113.5.7.104/11048
Peer ID type: IPV4_ADDR (1).                    //ip地址标识
*May 24 09:12:22:813 2019 CHIP-FW IKE/7/PACKET: -COntext=1; vrf = 0, src = 222.171.137.145, d
st = 113.5.7.104/11048
Peer ID value: address 10.105.62.235.
*May 24 09:12:22:813 2019 CHIP-FW IKE/7/PACKET: -COntext=1; vrf = 0, src = 222.171.137.145, d
st = 113.5.7.104/11048
No profile is matched.                  //没有profile匹配
```

对端为何使用IP地址标识，排查华为侧发现

```
#
ike peer branch_vpn1
```

undo version 2
 exchange-mode aggressive
pre-shared-key cipher %^%#J3M^8JnobMfrxmD,ic]4,`bq%:$!dTo@pBC{i>QK%^%#
ike-proposal 1
remote-id fqdn center
local-id fqdn branch_vpn
 remote-address 222.171.x.x
#
local-id-type name //配置IKE协商时本端的ID类型。V200R008及之后的版本，**name**参数修改为**fqdn**

在华为侧ike peer下增加local-id-type fqdn以及remote-id-type fqdn；

4、 添加后问题依旧，收集FW的debug ike信息
*May 24 14:37:44:683 2019 CHIP-FW IKE/7/PACKET: -COntext=1; vrf = 0, src = 222.171.137.145, d
st = 113.5.4.41/13797
Peer ID type: FQDN (2).
*May 24 14:37:44:683 2019 CHIP-FW IKE/7/PACKET: -COntext=1; vrf = 0, src = 222.171.137.145, d
st = 113.5.4.41/13797
Peer ID value: FQDN fqdn branch_vpn.
*May 24 14:37:44:683 2019 CHIP-FW IKE/7/PACKET: -COntext=1; vrf = 0, src = 222.171.137.145, d
st = 113.5.4.41/13797
No profile is matched.

已经能识别出FQDN，但是本地根据FQDN匹配不到profile，查看配置是有的，两端也是互指对应的，于是想测试修改FQDN标识看下，结果在华为侧修改fqdn名称时发现
remote-id-type fqdn
local-id-type fqdn
remote-id fqdn center //黄色底纹为一个整体ID标识，华为的FQDN名称中可以包含空格

 local-id fqdn branch_vpn

5、修改如下配置后两端建立ike和ipsec sa正常
ike peer branch_vpn1
undo version 2
 exchange-mode aggressive
pre-shared-key cipher %^%#J3M^8JnobMfrxmD,ic]4,`bq%:$!dTo@pBC{i>QK%^%#
ike-proposal 1
remote-id-type fqdn
local-id-type fqdn
remote-id center
local-id branch_vpn
 remote-address 222.171.x.x
#

解决方法

华为侧修改ike peer配置
1、 添加local-id-type fqdn以及 remote-id-type fqdn
2、 将local-id fqdn branch_vpn 改为local-id branch_vpn
将remote-id fqdn center 改为 remote-id center