H3C与飞塔对接IPsec异常

IPSec VPN 刘平泽 2023-12-20 发表

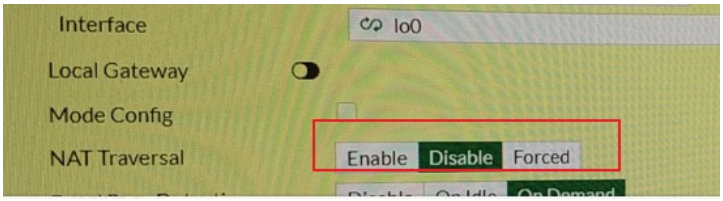
问题描述

当前H3C设备与飞塔设备建立IPSec，H3C侧关键配置如下，在下面配置中，第一阶段也建立不起来。

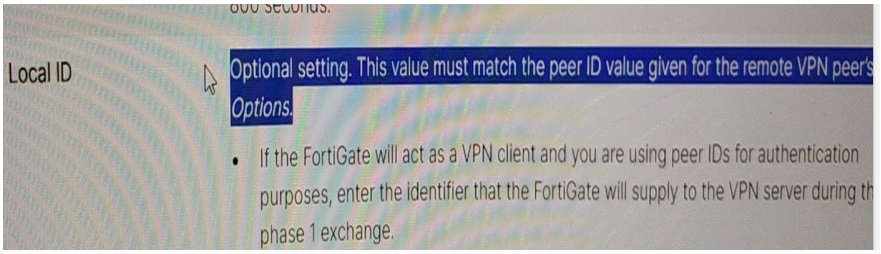
```
ipsec policy map1 10 isakmp
 transform-set To-ALTO-tran1
 security acl 3100
 remote-address  1.1.1.1
 ikev2-profile ALTO-profile1
#
ikev2 keychain keychain1
 peer ALTO-peer1
  address  1.1.1.1
  identity address 2.2.2.2
  pre-shared-key ciphertext $c$3$zI5r1IYKbOi8yhgA/S26pyc1n5CxkB4ESdqPOdwSRw==
#
ikev2 profile ALTO-profile1
 authentication-method local pre-share
 authentication-method remote pre-share
 keychain keychain1
 match remote identity address 1.1.1.1
#
ikev2 proposal 1
 encryption aes-cbc-256
 integrity sha256
 dh group19
 prf sha256
#
ikev2 policy 1
 proposal 1
#
```

过程分析

该组网中，飞塔设备在nat后面，为nat穿越场景。前期在调试过程中，飞塔侧未进行nat穿越配置勾选，后续建议飞塔勾选nat穿越，勾选nat穿越后。



飞塔侧设备，需要配置本地标志符，标识符为地址形式，文档中介绍，他们的local id 需要与H3C侧匹配，现场飞塔local id配置了本端的公网地址 2.2.2.2。



后续进行对接测试，依旧不能起来，H3C侧进行debug分析，报错如下：

```
*Dec 14 23:28:52:057 2023 y03-0202-tsdc-intdmz-rt3600-01 IKEV2/7/FSM: vrf = 0, src = xxxx, dst = x
xxx
 Searching profile based on peer's identity ID_FQDN of type xxxx
*Dec 14 23:28:52:057 2023 y03-0202-tsdc-intdmz-rt3600-01 IKEV2/7/ERROR: vrf = 0, src =xxxx, dst
= xxxxx
 None profile matched.
```

从报错来看，是本端校验对端身份的时候失败，导致没有profile被匹配。当前本端配置校验为如下命令：

match remote identity address 1.1.1.1
但是对端携带的被校验的标识符为2.2.2.2，且该格式为 fqdn格式，所以，本端修改配置，为，
match remote identity fqdn 2.2.2.2 后，问题解决。

解决方法

IKEv2对等体需要根据对端的身份信息查找一个本端的IKEv2 profile，然后使用此IKEv2 profile中的信息验证对端身份。对端身份信息若能满足本地某个IKEv2 profile中指定的匹配规则，则该IKEv2 profile为查找的结果。该问题中，飞塔设备作为client端，H3C设备需要对飞塔身份进行校验，而此时，飞塔的配置local id信息，为2.2.2.2，故，H3C设备必须配置match fqdn 2.2.2.2，才能匹配上，完成身份校验，从而进入ipsec的协商。需要指出，match remote identity fqdn XXXX命令是响应方对触发方的校验，只需要两边信息一致即可。