V7防火墙建立IPSEC隧道失败

IPSec VPN 杨焘轩 2019-01-21 发表

组网及说明

无

问题描述

V7防火墙作为网关和出口，作为分部要与总部建立IPSEC隧道。原先是V5的防火墙成功建立，现在需要用V7的进行替换。修改配置过程中发现隧道建立失败。

过程分析

V5和V7的防火墙配置有差异，主要在于对等体的配置和ipsec策略的配置。
检查配置发现使用的是野蛮模式，以fqdn的方式隧道建立。
V5配置如下

```
# ike proposal 1
 encryption-algorithm aes-cbc 128
 dh group2
 authentication-algorithm md5
 sa duration 3600
# ike dpd 1
 interval-time 5
# ike dpd dpd
# ike peer sangfor@imicams
 exchange-mode aggressive
 proposal 1
 pre-shared-key cipher $c$3$ZFgzn2en/kB54cAmHxl/9OSoMaXOyZI5vPwrDMY=
 id-type name
 remote-name sangfor@imicams
 remote-address vpn.xnh.org.cn dynamic
 local-address 211.142.70.104
 local-name h3c@szscq.hspt
 nat traversal dpd 1
# ipsec transform-set 1
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
 esp encryption-algorithm aes-cbc-128
# ipsec policy 1 1 isakmp
 security acl 3999
 ike-peer sangfor@imicams
 transform-set 1
```

V7配置如下

```
# ipsec transform-set GE1/0/2_IPv4_1
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm md5
 # ipsec policy GE1/0/2 1 isakmp
 transform-set GE1/0/2_IPv4_1
 security acl name IPsec_GE1/0/2_IPv4_1
 local-address 211.142.70.104
 remote-address vpn.xnh.org.cn
 ike-profile GE1/0/2_IPv4_1
# ike invalid-spi-recovery enable
 ike dpd interval 10 on-demand
 ike identity fqdn
 # ike profile GE1/0/2_IPv4_1
 keychain GE1/0/2_IPv4_1
 dpd interval 5 on-demand
 exchange-mode aggressive
 local-identity address 211.142.70.104
 match remote identity fqdn sangfor@imicams
 match local address GigabitEthernet1/0/2
 proposal 1
```

ike proposal 1
encryption-algorithm aes-cbc-128
dh group2
authentication-algorithm md5
sa duration 3600
ike keychain GE1/0/2_IPv4_1
match local address GigabitEthernet1/0/2
pre-shared-key hostname sangfor@imicams key cipher c3$Rt+wQTNDV/a5PltmtQeaZHV6vf+mfQ==
检查防火墙策略都放通了没有问题。V7nat默认开启穿越，在ACL中也deny了IPSEC的数据流。
因为总部防火墙无法配置，无法得知对端总部的配置情况，只能根据V5成功的配置进行比对和调整

解决方法

更改安全策略不进行日志记录，排除多余的信息干扰，debug ike all发现有报错如下
*Jan 21 12:36:12:645 2019 SZRMYY-WW-FW-1000-AK125 IKE/7/EVENT: vrf = 0, local = 211.142.70.104, rem
te = 111.200.197.101/500
Pre-shared key matching address 111.200.197.101 not found.
*Jan 21 12:36:12:645 2019 SZRMYY-WW-FW-1000-AK125 IKE/7/ERROR: vrf = 0, local = 211.142.70.104, rem
te = 111.200.197.101/500
No available proposal.
根据debug信息来看是因为没有匹配的proposal
这个报错的原因多半是keychain和profile的配置问题。
根据官网的说明，发现分部防火墙有一条如下配置
pre-shared-key hostname sangfor@imicams key cipher c3$Rt+wQTNDV/a5PltmtQeaZHV6vf+mfQ==
查询官网得知，当设备配置hostname时，只能作为响应方，无法作为发起方。至此，怀疑是这个配置导致没有匹配的proposal
将hostname更改为地址后，再次测试成功建立隧道。