某局点V7防火墙ipsec隧道建立不成功

IPSec VPN　姜霁琛　2019-05-23 发表

组网及说明

总部和分部都为H3C 的V7防火墙设备

问题描述

现场在防火墙之间建立ipsec隧道，分部采用拨号口上网，现场ipsec建立失败，分部ike sa为unknown状态，总部没有ike sa，查看配置，两端加密算法、安全策略均配置正常，经过nat的acl也都deny了，且两端ipsec感兴趣流配置正确，查看debug信息提示ike 协商失败

总部

```
# ipsec transform-set g1/0/3-ipv4
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm sha1
# ipsec policy-template g1/0/3 1
 transform-set g1/0/3-ipv4
 security acl 3888
 local-address  x.x.x.x
 ike-profile 1
#
 ipsec policy g1/0/3 1 isakmp template g1/0/3
# ike profile 1
 keychain 1
 exchange-mode aggressive
 local-identity fqdn center
 match remote identity address 0.0.0.0 0.0.0.0
 match remote identity fqdn branch
 proposal 200
# ike proposal 200
# ike keychain 1
 pre-shared-key address 0.0.0.0 0.0.0.0 key cipher
$c$3$nxM5T3cq3VchxBxjkFdjgLk+AW3Sv/U5U56i
```

分支

```
#
ipsec transform-set g1/0/3-ipv4
 esp encryption-algorithm
aes-cbc-128 esp
authentication-algorithm sha1
 #
ipsec policy g1/0/3 1 isakmp
 transform-set g1/0/3-ipv4
 security acl 3999
 remote-address x.x.x.x
 ike-profile 1
#
 ike profile 1
 keychain 1
 exchange-mode aggressive
 local-identity fqdn branch
 match remote identity fqdn center
 match remote identity address  x.x.x.x   255.255.255.255
 proposal 200
 #
 ike proposal 1
#
 ike proposal 200
#
ike keychain 1
 pre-shared-key address x.x.x.x 255.255.255.255 key cipher $c$3$Na7jkHl20CoBKWSJRcBImqCQ1
MVLFs45qnlR
```

分部这边debug ike报错

```
*May 21 16:27:08:017 2019 H3C IKE/7/EVENT: -COntext=1; vrf = 0, local =  x.x.x.x  , remote = x.x.x.
```

x/500
Retransmission of phase 1 packet timed out.
*May 21 16:27:08:018 2019 H3C IKE/7/ERROR: -COntext=1; vrf = 0, local = x.x.x.x , remote = x.x.x.x /500
Failed to negotiate IKE SA.

过程分析

查看debug报错提示第一阶段协商报文超时，ike sa协商失败，但是没有报是什么字段或密钥协商失败，怀疑不是参数配置问题，而是连通性问题，并且在分部这边debug看是总部没有回包，询问现场两端设备公网是通的，网络连通性没问题，此时怀疑是否是ipsec的端口被占用或被拒绝导致协商失败，查看现场配置，发现总部这边ipsec接口下配置了两条nat server，把ipsec的udp500和4500端口做了映射，这样的话ipsec流量会匹配到nat server映射到内网，因此导致ipsec报文无法正确传输，协商失败

```
# interface GigabitEthernet2/0/3
 port link-mode route
 ip address x.x.x.x 255.255.255.252
 nat server protocol udp global x.x.x.x 500 inside 10.60.32.x 500
nat server protocol udp global x.x.x.x 4500 inside 10.60.32.x 4500
ipsec apply policy g1/0/3
```

解决方法

让现场把总部接口下关于udp500和4500端口的nat server配置去掉正常建立隧道