某局点MSR2600-10-X1和第三方设备国密IPSec无法建立的经验处理案例

IPSec VPN 孙轶宁 2020-06-30 发表

组网及说明

MSR2600-10-X1和第三方设备建立国密IPSec

问题描述

第一阶段ike sa无法协商建立，主要配置如下

```
pki domain ph
 certificate request from ca
 certificate request entity ph
 public-key sm2 signature name sm2sig encryption name sm2enc
 undo crl check enable
#
pki entity ph
 common-name ph
#
ipsec transform-set tran1
 esp encryption-algorithm sm1-cbc-128
 esp authentication-algorithm sm3
#
ipsec policy map1 10 isakmp
 transform-set tran1
 security acl 3001
 local-address X.X.X.X
 remote-address X.X.X.X
 ike-profile profile1
#
ike profile profile1
 certificate domain ph
 exchange-mode gm-main
 local-identity address X.X.X.X
 match remote identity address X.X.X.X 255.255.255.0
 proposal 1
#
ike proposal 1
 authentication-method sm2-de
 encryption-algorithm sm1-cbc-128
 authentication-algorithm sm3
```

过程分析

1、收集debugging ike all，报错如下：

```
*Jan  1 04:25:11:447 2011 H3C IKE/7/PACKET: vrf = 0, local = X.X.X.X, remote = X.X.X.X/500
Peer ID type: DER_ASN1_DN (9).
*Jan  1 04:25:11:447 2011 H3C IKE/7/PACKET: vrf = 0, local = X.X.X.X, remote = X.X.X.X/500
Peer ID value: DN CN=XXXX
*Jan  1 04:25:11:447 2011 H3C IKE/7/PACKET: vrf = 0, local = X.X.X.X, remote = X.X.X.X/500
Started to process signature certificate payload.
*Jan  1 04:25:11:448 2011 H3C PKI/7/PKI_DEBUG: Failed to verify certificate by domain ph.
*Jan  1 04:25:11:448 2011 H3C IKE/7/ERROR: vrf = 0, local = X.X.X.X, remote = X.X.X.X/500
Failed to verify the peer certificate. Reason: certificate is not yet valid.
*Jan  1 04:25:11:448 2011 H3C IKE/7/ERROR: vrf = 0, local = X.X.X.X, remote = X.X.X.X/500
Invalid certificate.
*Jan  1 04:25:11:448 2011 H3C IKE/7/PACKET: vrf = 0, local = X.X.X.X, remote = X.X.X.X/500
Construct notification packet: INVALID_CERTIFICATE.
```

2、检查两边证书，确认都是通过设备导出pkcs10码，然后从服务器申请证书。

3、再次检查配置，发现ike profile里面没有配置证书策略，补充下面部分的配置后，成功建立

预定义一项证书属性名称为b8830047，要求证书的 subject-name的实体DN也就包含b8830047字符串（subject name的CN字段）

```
#
```

pki certificate attribute-group b8830047
 attribute 1 subject-name dn ctn **b8830047** //ctn表示包含，即dn包含b8830047字符串
预定义一项证书访问控制策略名称为b8830047，并规则放行名称为b8830047的证书属性组
#
pki certificate access-control-policy b8830047
 rule 1 permit b8830047
#
ike profile B8830047
 match remote certificate b8830047 //在ike profile调用证书访问控制策略b8830047 ，来验证对端证书是否合法

解决方法

IPSec国密证书认证的时候必须要在ike profile里面配置match证书策略，否则会导致ike profile匹配不到证书，产生INVALID_CERTIFICATE报错
预定义一项证书属性名称为b8830047，要求证书的 subject-name的实体DN也就包含b8830047字符串（subject name的CN字段）
 #
pki certificate attribute-group b8830047
 attribute 1 subject-name dn ctn **b8830047** //ctn表示包含，即dn包含b8830047字符串
预定义一项证书访问控制策略名称为b8830047，并规则放行名称为b8830047的证书属性组
#
pki certificate access-control-policy b8830047
 rule 1 permit b8830047
#
ike profile B8830047
 match remote certificate b8830047 //在ike profile调用证书访问控制策略b8830047 ，来验证对端证书是否合法