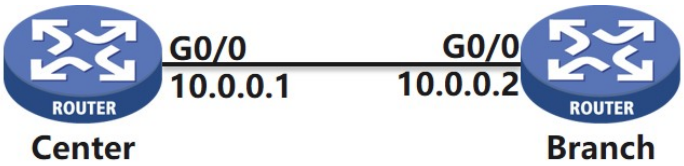
MSR5660证书加国密算法方式ipsec典型配置

IPSec VPN 郭昊 2019-07-17 发表

组网及说明



两台V7 MSR设备通过证书加国密算法的方式建立ipsec，下面介绍该场景的典型配置。

配置步骤

密钥生成、证书在线申请或离线导入过程略。

分支ipsec主要配置：

```
#
pki domain 1
 public-key sm2 general name abc
//abc是生成sm2密钥时自己定义的名字，可以dis public-key local sm2来看密钥名称
 undo crl check enable
#
ipsec transform-set 1
 esp encryption-algorithm sm4-cbc
//sm1需要国密卡，sm2-sm4是软件实现
 esp authentication-algorithm sm3
#
ipsec policy 1 1 isakmp
 transform-set 1
 security acl 3000
 local-address 10.0.0.2
 remote-address 10.0.0.1
 ike-profile 1
#
ike profile 1
 certificate domain 1
 exchange-mode gm-main
//注意国密算法的ipsec要有这条配置
 local-identity address 10.0.0.2
 match remote identity address 0.0.0.0 0.0.0.0
 proposal 1
#
ike proposal 1
 authentication-method sm2-de
 encryption-algorithm sm4-cbc
 authentication-algorithm sm3
#
```

总部ipsec配置：

```
#
pki domain 1
 public-key sm2 general name abc
 undo crl check enable
#
ipsec transform-set 1
 esp encryption-algorithm sm4-cbc
 esp authentication-algorithm sm3
#
ipsec policy-template 1 1
 transform-set 1
```

```
 security acl 3000
 ike-profile 1
#
ipsec policy 1 1 isakmp template 1
#
ike profile 1
 certificate domain 1
 exchange-mode gm-main
 match remote identity address 0.0.0.0 0.0.0.0
 proposal 1
#
ike proposal 1
 authentication-method sm2-de
 encryption-algorithm sm4-cbc
 authentication-algorithm sm3
#
```

配置关键点

如国密算法ipsec配置不通，请先参考上述最简配置协商起来ipsec，之后再逐步增加其他参数。