MSR 4G拨号+IPSec国密双认证案例

国密卡 3G/4G拨号 **热心市民赵先生** 2023-03-02 发表

组网及说明

MSR 3600路由器采用4G双卡单待进行拨号，与天融信防火墙建立IPSec建立隧道，IPSec采用国密双认证（加密、签名）

告警信息

无

告警信息

问题描述

配置步骤

1、 MSR路由器4 modom功能
   a) 配置4G自动拨号
   b) 配置双卡单待自动切换功能
2、 配置证书部分
   a) MSR上创建pki域
   b) 生成用于一阶段的身份认证、非对称的数字签名和验签、加密和解密的密钥对
   c) 生成证书请求码
   d) 申请证书
   e) 导入证书
3、 配置IPSec

过程分析

无

解决方法

1、MSR路由器4 modem功能

1.1、4G模块配置

主卡配置

```
dialer-group 1 rule ip permit    //创建拨号访问规则

apn-profile test                 //配置apn
apn static test@vpdn.h3c.com     //apn设置内容由客户提供
authentication-mode pap user test password simple test  /配置认证方式几用户名密码

controller Cellular 1/0:0   //进入cellular接口
eth-channel 0               //创建以太网接口通道

interface Eth-channel 1/0:0
dialer circular enable      //开启共享DDR
dialer-group 1          //关联上面创建的dialer-group 1
dialer timer idle 0     //呼叫建立后，允许链路空闲的时间,0表示永不挂断
dialer timer autodial 5     // DDR自动拨号的间隔时间。
dialer number *99#  autodial   //移动联通用*99#，电信用#777
ip address cellular-alloc       //采用Modem私有协议获取ip地址

apn-profile apply test          // 配置4G Modem参数模板
#
        副卡配置同上配置，请设置不同apn、用户名密码、认证方式
```

1.2、配置SIM卡自动切换

配置NQA，探测对方已知地址。NQA测试组周期性地探测某个目的地址是否可达、是否可以与某个目的服务器建立TCP连接等。如果在Track项和NQA测试组之间建立了关联，则当连续探测失败的次数达到指定的阈值时，NQA将通知Track模块监测对象出现异常，Track模块将与NQA测试组关联的Track项的状态置为Negative；否则，NQA通知Track模块监测对象正常工作，Track模块将Track项的状态置为Positive。

```
nqa entry 1 1          //创建nqa测试组，测试组管理员1，测试操作标签1

type icmp-echo          //类型为icmp-echo
destination ip 114.114.114.114   //探测报文目的地址为114
frequency 2000          //配置测试组测试时间间隔2000毫秒
probe timeout 2000          //探测超时时间
reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigger-only
                                    //创建监测探测持续时间的阈值告警组，当icmp报文探测失败达到5次，触发track联动

track 2 nqa entry 1 1 reaction 1      //创建与NQA测试组中指定联动项关联的Track项

ip route-static 0.0.0.0 0 Eth-channel1/0:0
ip route-static 0.0.0.0 0 Eth-channel1/1:0

controller Cellular1/0
eth-channel 0
sim backup enable track 2  （指定Track项的序号）      //配置3G/4G链路备份与Track项联
动

controller Cellular1/1
eth-channel 0
sim backup enable track  2
sim switch-back enable wait-time 5    //如果希望SIM 0作为主，当主恢复时进行回切可以配置这个，但是配置后会多1次震荡，所以建议设置时间间隔，避免链路质量不佳导致频繁震荡
nqa schedule 1 1 start-time now lifetime forever  /配置测试组的启动时间和持续时间
```

2、配置证书

配置pki域

```
pki entity ph
common-name ph

pki domain ph
certificate request from ca
certificate request entity ph
```

public-key sm2 signature name sm2sig encryption name sm2enc
//这里生成的是名称为sm2z3 的通用秘钥对，用于加密和签名。可单独配置加密秘钥对和签名秘钥对。