MSR G2 ipsec主模式+证书认证

IPSec VPN 王丽娟 2021-12-15 发表

组网及说明

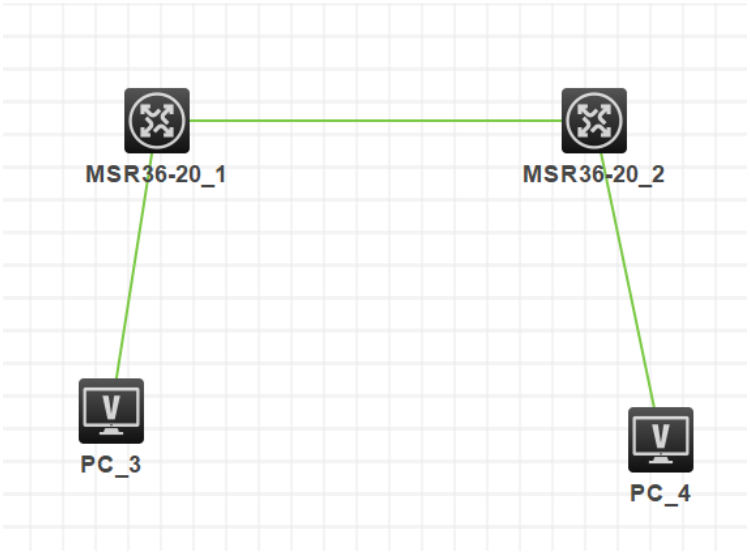
要求路由器之间之间路由可达，PC使用loopback口代替，并且有如下要求：

1、ipsec 采用主模式

2、认证方式为证书认证

3、证书需要离线导入到路由器

一、 组网图：



IP地址规划：

设备	外网口IP	内网口（loopback）IP
MSR3620-1	10.88.142.136/24	192.168.10.1
MSR3620-2	10.88.142.214/24	192.168.2.1

配置步骤

各设备上IP地址和路由的配置省略

1.1 察看路由器上时钟，是否与CA服务器时钟一致

以北京时间为准，不要相差太大，时钟不一致可能导致CA证书失效或未启用

察看修改正确时钟命令如下：

<MSR G2>display clock

23:05:18 beijing Tue 12/14/2021

Time Zone : beijing add 08:00:00

< MSR G2>clock datetime 11:15:00 12/14/2021

1.2 配置pki实体：

```
#
pki entity 123
 common-name 123
#
```

1.3 配置pki域：

```
#
pki domain 123
 certificate request from ca
 certificate request entity 123
 public-key rsa general name 123
 undo crl check enable
#
```

1.4 手工申请证书

手工申请证书，打印证书申请字符串，提供证书申请字符串给证书颁发机构：

[MSR G2]pki request-certificate domain 123 pkcs10

.

```
*** Request for encryption certificate ***
-----BEGIN CERTIFICATE REQUEST-----
MIIBazCB1QIBADAOMQwwCgYDVQQDEwMxMjMwgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAMm3ffyxMjv3s1gvkL9Ofca4R8a3wZqQFLb2sVp71aUZCShtG5eTEgGk
oQZjlh9TI/w7FdI7sBmS3kkp80mVmGZGO/wNZaU4IuYidFbwuaX6coeXqhuB7igb
rqSMNI0tCIq3s6Xz3gr5+xwr3vt7t3shdnkBw6z0EQvzBAVPiiSBAgMBAAGgHjAc
BgkqhkiG9w0BCQ4xDzANMAsGA1UdDwQEAwIEMDANBgkqhkiG9w0BAQUFAAOBgQCo
URHLeH74Kb6GXxW3JS7PJLeYmBrcxjesseuJxwhLS9dNI6bjGxQxV4pOV0V8snkE
Xee33lwaOKpATQEIsGENsltAao930AgEYyjMpS8dAks5pBXPdKyRi0ggGzkYB/CW
5zDFMermKxvnJOCfg+x4i27GfqLJaAiYaYxjgKsAVw==
-----END CERTIFICATE REQUEST-----

[MSR G2]
```

证书颁发机构根据申请字符串颁发证书。

1.5 把根证书和本地证书传输到路由器上：

（传输方式：路由器作ftp/tftp/sftp客户端，或者作为ftp/sftp服务器）

```
<MSR G2>ftp 172.33.26.100
Trying 172.33.26.100 ...
Press CTRL+K to abort
Connected to 172.33.26.100.
220 Serv-U FTP-Server v2.4 for WinSock ready...
User(172.33.26.100:(none)):f
331 User name okay, need password.
Password:
230 User logged in, proceed.

[ftp]bin
200 Type set to I.

[ftp]get CA.cer

227 Entering Passive Mode (172,33,26,100,13,48)
150 Opening BINARY mode data connection for CA.cer (816 bytes).
226 Transfer complete.
FTP: 816 byte(s) received in 0.093 second(s), 8.00K byte(s)/sec.

[ftp]get 123456.pfx

227 Entering Passive Mode (172,33,26,100,13,49)
150 Opening BINARY mode data connection for 123456.pfx (1118 bytes).
226 Transfer complete.
FTP: 1118 byte(s) received in 0.121 second(s), 9.00K byte(s)/sec.

[ftp]bye
221 Goodbye!
```

1.6 导入根证书：

[MSR G2]pki import domain 123 der ca filename CA.cer

```
The trusted CA's finger print is:
    MD5  fingerprint:39F8 33BC C02D 84E2 F3F6 15B4 7454 32A8
    SHA1 fingerprint:1651 A12B 79A8 1ECF 8093 EB67 65D2 C372 88D2 D4BA
Is the finger print correct?(Y/N):y
```

配置关键点

1. 导入证书前，一定要检查设备时间是否在证书有效期范围内。

2. 导入证书的时候需要先导入CA证书，再导入local证书，因为设备需要使用CA证书中的公钥对local证书的签名进行验证，以此来确认local证书是否真实有效。

3. 用于脱离线导入证书，设备无法向证书服务器验证CRL，因此在PKI domain中必须关闭CRL检查。

4. 而V7设备在进行证书认证的时候，除了检查对端证书的有效性之外，还需要对证书中的subject DN 进行检查。因此需要配置一个证书访问策略。

1.7 导入路由器证书：

```
[MSR G2]pki import domain 123 p12 local filename 123456.pfx
Please input the password:
The device already has a key pair. If you choose to continue, the existing key pair will be overwritten if it is used for the same purpose. The local certificates, if any, will also be overwritten.
Continue? [Y/N]:y
[MSR G2]
```

1.8 查看导入的根证书：

```
[MSR G2]dis pki certificate domain 123 ca
Certificate:
    Data:
        Version: 3 (0x2)
```