MSR-G2系列路由器手工导入证书建立IPSEC典型配置

IPsec 证书 高贵贤 2013-07-26 发表

MSR-G2系列路由器手工导入证书建立IPSEC典型配置

一、 组网需求

在Router1和Router3之间建立一个IPSEC隧道，对Router1所在子网（1.1.1.1/32）和Router3所在的子网（3.3.3.3/32）之间的数据流进行安全保护

1. Router1和Router3之间采用IKE协商的方式建立IPSEC SA；
2. Router1和Router3的隧道建立方式为RSA数字签名方式；
3. IKE第一阶段协商模式采用主模式。

设备清单：MSR-G2路由器3台

二、 组网图

图一 MSR-G2手工导入证书建立IPSEC组网图

三、 配置步骤

Router1配置：

```
[Router1]display  current-configuration
#
 version 7.1.042, ESS 0006P05
#
 sysname Router1
#
//创建环回口模拟内网用户
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 12.1.1.1 255.255.255.0
 ipsec apply policy 123
#
 ip route-static 0.0.0.0 0 12.1.1.2
#
acl number 3000
 rule 0 permit ip source 1.1.1.1 0 destination 3.3.3.3 0
#
//配置PKI域，关闭CRL检查，否则导入本地证书失败
pki domain h3c
 public-key rsa general name ggx
 undo crl check enable
#
pki entity h3c
 common-name h3c
#
ipsec transform-set 123
 esp encryption-algorithm des-cbc
 esp authentication-algorithm md5
#
ipsec policy 123 1 isakmp
 transform-set 123
 security acl 3000
 remote-address 23.1.1.2
 ike-profile 123
#
//此处指定了使用h3c作为验证域，若不指定也可，和V5有所不同
```

```
ike profile 123
certificate domain h3c
 match remote identity address 23.1.1.2 255.255.255.255
 proposal 123
#
//配置使用数字签名方式建立IPSEC隧道，默认为预共享密钥方式
ike proposal 123
 authentication-method rsa-signature
#
Return
```

Router3配置：

```
display current-configuration
#
 version 7.1.042, ESS 0006P05
#
 sysname Router3
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 23.1.1.2 255.255.255.0
 ipsec apply policy 123
#
 ip route-static 0.0.0.0 0 23.1.1.1
#
acl number 3000
 rule 0 permit ip source 3.3.3.3 0 destination 1.1.1.1 0
#
pki domain h3c
 public-key rsa general name qu
 undo crl check enable
#
pki entity h3c
 common-name h3c
#
ipsec transform-set 123
 esp encryption-algorithm des-cbc
 esp authentication-algorithm md5
#
ipsec policy 123 1 isakmp
 transform-set 123
 security acl 3000
 remote-address 12.1.1.1
 ike-profile 123
#
ike profile 123
 certificate domain h4c
 certificate domain h3c
 match remote identity address 12.1.1.1 255.255.255.255
 proposal 123
#
ike proposal 123
 authentication-method rsa-signature
#
Return
```

证书导入过程：

```
//导入根证书
[Router3]pki import domain h3c der ca filename certnew.cer
```

```
The trusted CA's finger print is:
    MD5  fingerprint:AD2B A928 850E BB26 1F56 6C98 12EB 97C0
    SHA1 fingerprint:34B7 0FAC 121B E7F2 CCFA 7042 A737 1668 400D 0E3E
Is the finger print correct?(Y/N):y

//导入本地证书
[R3]pki import domain h3c p12 local filename server.pfx
Please input the password:                  //此处输入证书密钥123456
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
```

四、　　配置验证

```
ping -a 1.1.1.1 3.3.3.3
Ping 3.3.3.3 (3.3.3.3) from 1.1.1.1: 56 data bytes, press escape sequence to break
Request time out
56 bytes from 3.3.3.3: icmp_seq=1 ttl=255 time=0.773 ms
56 bytes from 3.3.3.3: icmp_seq=2 ttl=255 time=0.322 ms
56 bytes from 3.3.3.3: icmp_seq=3 ttl=255 time=0.291 ms
56 bytes from 3.3.3.3: icmp_seq=4 ttl=255 time=0.281 ms

[R1]display ike  sa
    Connection-ID   Remote              Flag        DOI
-----------------------------------------------------------------------
    32              23.1.1.2            RD          IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING

[R1]display ipsec  sa
-------------------------------
Interface: GigabitEthernet0/0
-------------------------------

  ------------------------------
  IPsec policy: 123
  Sequence number: 1
  Mode: isakmp
  ------------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect forward secrecy:
    Path MTU: 1443
    Tunnel:
        local  address: 12.1.1.1
        remote address: 23.1.1.2
    Flow:
    sour addr: 1.1.1.1/255.255.255.255  port: 0  protocol: ip
    dest addr: 3.3.3.3/255.255.255.255  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 1605634541 (0x5fb409ed)
      Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/1665
      Max received sequence-number: 4
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for nat traversal: N
      Status: active

    [Outbound ESP SAs]
      SPI: 741008824 (0x2c2ae5b8)
      Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
```

SA remaining duration (kilobytes/sec): 1843199/1665
Max sent sequence-number: 4
UDP encapsulation used for nat traversal: N
Status: active

五、 配置关键点

1. PKI域中要配置undo crl check enable,否则在导入本地证书的时候会由于获取不到CRL列表而导致导入失败；

2. 在MSR-G2中，IKE profile中也可以不指定认证的PKI域，若指定，则使用指定的PKI域发送本端证书请求、验证对端请求等；若未指定，则使用设备上配置的PKI域进行以上相关操作，这一点和V5设备有所区别。具体说明可以查看V5和V7的命令手册。