MSR-G2系列路由器 RSA方式建立IPSEC的典型配置

高贵贤 2013-07-22 发表

MSR-G2系列路由器 RSA方式建立IPSEC的典型配置

一、 组网需求：

在Router1和Router2之间建立一个IPsec隧道，对Router1所在的子网（1.1.1.1/32）与Router2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Router2之间采用IKE协商方式建立IPsec SA；

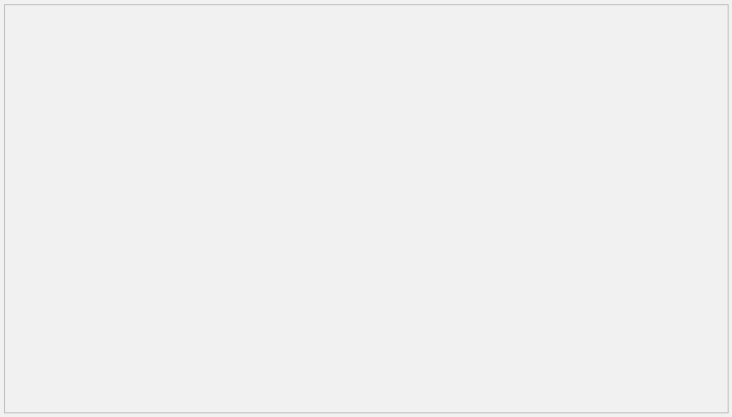
2.Router1和Router2均使用RSA数字签名的认证方法；

3.IKE第一阶段的协商模式为野蛮模式；

4.使用windows2008 server搭建CA服务器。

设备清单：MSR G2路由器2台

二、 组网图：



图一 MSR-G2路由器 RSA方式建立IPSEC典型配置组网图

三、 配置步骤：

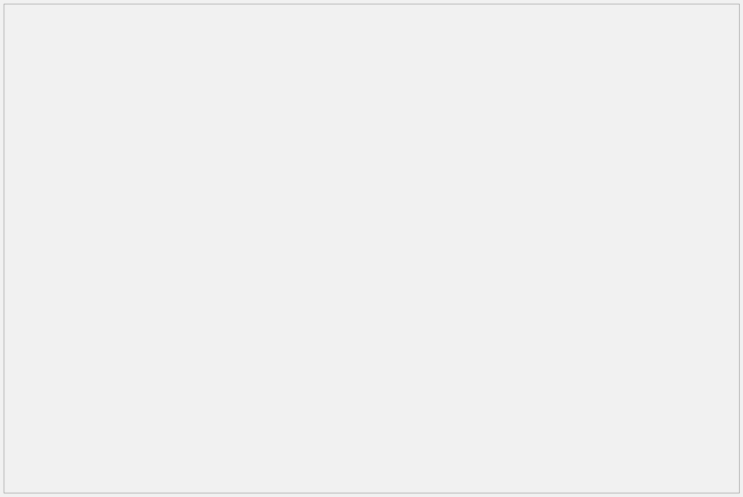
使用版本：E0006P05

Router1配置：

```
//配置环回接口模拟内网用户
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
//Router1的GigabitEthernet0/0口调用IPSEC策略
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 100.1.1.1 255.255.255.0
 ipsec apply policy 123
#
//配置静态路由，下一跳指向100.1.1.2
 ip route-static 2.2.2.2 32 100.1.1.2
#
//配置安全ACL
acl number 3000
 rule 0 permit ip source 1.1.1.1 0 destination 2.2.2.2 0
#
//配置PKI域h3c，CA服务器的URL地址为100.1.1.253
pki domain h3c
 ca identifier ts-msr
 certificate request url http://100.1.1.253/certsrv/mscep/mscep.dll
 certificate request from ra
 certificate request entity h3c
 public-key rsa general name 123
 undo crl check enable
#
//PKI实体为h3c
pki entity h3c
 common-name h3c
 country CN
```

```
#
//配置IPSEC提议，加密算法使用3des-cbc,认证方式为MD5
ipsec transform-set 123
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
//配置IPSEC安全策略，调用安全ACL，IPSEC提议和IKE Profile
ipsec policy 123 1 isakmp
 transform-set 123
 security acl 3000
 remote-address 100.1.1.2
 ike-profile 123
#
//配置IKE Profile 123，使用野蛮模式
ike profile 123
 certificate domain h3c
 exchange-mode aggressive
 local-identity fqdn Router1
 match remote identity fqdn R2
 proposal 123
#
//配置ike提议，指定使用数字证书认证方式
ike proposal 123
 authentication-method rsa-signature
 authentication-algorithm md5
#
Return
//证书申请过程：
//生成本地证书密钥对
[Router1]public-key local create rsa name 123
The local key pair already exists.
Confirm to replace it? [Y/N]:y
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
........++++++
.++++++
Create the key pair successfully.
//获取根证书
[Router1]pki retrieve-certificate domain h3c ca
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
Retrieved the certificates successfully.
//获取本地证书，password为本地密钥握手挑战码（BEDF2A91DED372FF）
[Router1]pki request-certificate domain h3c password 6054576C2575ED24
Start to request general certificate ...
Certificate requested successfully.

握手挑战码获取方式为:
登录：http://100.1.1.253/certsrv/mscep_admin
输入用户名和密码后会弹出如下界面：
```



图二

Router2配置:

```
#
//配置环回口模拟内用户
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
//接口GigabitEthernet0/0调用IPSEC策略
interface GigabitEthernet0/0
 port link-mode route
 ip address 100.1.1.2 255.255.255.0
 ipsec apply policy 123
#
//配置静态路由，下一条指向100.1.1.1
 ip route-static 1.1.1.1 32 100.1.1.1
#
//配置安全ACL
acl number 3000
 rule 0 permit ip source 2.2.2.2 0 destination 1.1.1.1 0
#
//配置PKI域h3c，CA服务器的URL为100.1.1.253
pki domain h3c
 ca identifier h3c
 certificate request url http://100.1.1.253/certsrv/mscep/mscep.dll
 certificate request from ra
 certificate request entity h3c
 public-key rsa general name 123
 undo crl check enable
#
//配置PKI实体h3c
pki entity h3c
 common-name h3c
 country CN
 organization-unit h3c
 organization H3C
#
//配置IPSEC提议，加密算法为3des-cbc,认证算法为MD5
ipsec transform-set 123
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
//配置IPSEC策略，调用安全ACL，IPSEC策略、IKE Profile
ipsec policy 123 1 isakmp
 transform-set 123
 security acl 3000
 remote-address 100.1.1.1
 ike-profile 123
#
```

```
//配置ike profile，使用野蛮模式
ike profile 123
 exchange-mode aggressive
 local-identity fqdn R2
 match remote identity fqdn Router1
 proposal 123
#
//配置Ike提议，指定使用证书认证方式
ike proposal 123
 authentication-method rsa-signature
 authentication-algorithm md5
#
证书申请过程：
[R2]public-key local create rsa name 123    //生成本地密钥对
The local key pair already exists.
Confirm to replace it? [Y/N]:y
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....++++++
.....++++++
Create the key pair successfully.
//获取根证书
[R2]pki retrieve-certificate domain h3c ca
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
Retrieved the certificates successfully.
//获取本地证书
[R2]pki request-certificate domain h3c password 6A8C9FACB2CA3DCF
Start to request general certificate ...
Certificate requested successfully.
[R2]%Jun 20 10:33:28:748 2013 R2 PKI/5/REQUEST_CERT_SUCCESS: Request
certificate of domain h3c successfully
四、验证配置
//查看根证书
[Router1]display pki certificate domain h3c ca
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number:
         56:c3:98:36:bf:9d:45:a9:43:61:78:94:72:3a:ad:a6
      Signature Algorithm: sha1WithRSAEncryption
      Issuer: CN=WIN-2VHX793UTF1-CA
      Validity
         Not Before: Dec 24 06:26:34 2012 GMT
         Not After : Dec 24 06:36:33 2017 GMT
      Subject: CN=WIN-2VHX793UTF1-CA
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
               00:b4:66:32:0d:55:39:6e:93:4d:4a:46:1b:29:e1:
               89:13:fe:58:d0:ac:50:2c:0c:af:7b:36:3e:bc:04:
               7f:a5:de:da:97:52:b4:d7:23:6f:0a:e7:7e:66:b4:
               fd:96:4a:68:3f:53:fe:46:bb:8c:0d:08:97:1d:00:
               84:14:1b:a4:08:cf:eb:39:8c:c0:f5:3b:a6:fb:fe:
               ab:10:47:36:cc:7b:75:e3:aa:3b:fb:38:cb:c0:bb:
               1a:20:21:9f:01:ce:59:0d:3f:a8:91:46:bd:3f:bc:
               ee:d3:23:7e:7b:8d:cd:ee:b4:79:d0:28:f0:58:3d:
               73:ad:b1:e1:ff:60:8e:16:4e:b6:58:c8:67:60:56:
```

```
                05:d6:b8:90:90:19:d4:41:cc:7a:12:81:16:4c:89:
                89:d3:52:e9:52:ff:10:39:15:a1:c2:8d:e2:69:45:
                a4:ba:e7:04:86:05:7c:c5:c0:f9:65:af:d0:e5:7c:
                76:41:13:62:73:28:92:db:46:09:ec:64:d5:55:38:
                0a:ba:3c:80:e6:0d:e9:4a:db:3f:f6:67:4b:be:40:
                cf:29:eb:50:e1:63:f1:7c:d3:18:72:ce:9e:4f:a2:
                f3:c4:a2:6e:da:67:02:d1:ff:1e:6e:7f:25:8f:f9:
                56:31:c8:10:6b:98:6a:6a:8a:8c:3a:6e:a0:0f:67:
                d3:f7
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage:
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                A2:F1:E9:DE:21:48:C8:AA:C6:89:D8:3E:D8:24:9E:E6:40:99:7B:E6
            1.3.6.1.4.1.311.21.1:
                ...
    Signature Algorithm: sha1WithRSAEncryption
        72:ed:88:12:01:73:be:75:1f:00:d5:39:a8:9a:6d:f8:ed:ec:
        f5:5e:a9:12:2d:1a:9d:1e:cc:09:6a:55:86:99:fe:96:97:e3:
        97:4b:11:ac:34:e2:70:25:27:7c:eb:05:3a:6c:9c:c5:7d:46:
        46:8f:00:05:29:40:e1:36:06:b0:e4:68:6d:74:fe:5f:60:7c:
        d1:73:8f:37:0e:11:72:cf:6c:af:ff:63:6c:94:cf:d1:cd:65:
        a1:f2:52:65:3e:b1:a4:38:68:eb:2a:06:cc:5d:35:4e:4f:1b:
        df:b6:03:ff:0e:cd:e3:3f:6a:b2:ab:d0:1e:4c:72:7c:e8:1c:
        9d:bc:fa:3a:05:b8:71:bf:15:6f:34:ba:b6:2f:14:a1:76:e8:
        2f:af:9c:1f:70:35:80:4b:44:3e:75:85:e8:8d:8e:4f:01:2e:
        7b:48:11:3e:20:74:54:0c:27:0d:80:73:dd:16:e9:5f:a7:1e:
        e3:93:39:f1:ec:46:4c:df:56:f2:4b:c7:45:71:4f:4e:3f:94:
        68:3c:cb:f0:d8:04:d7:16:3c:b2:bf:07:db:b0:5b:1f:33:c3:
        fc:53:5e:aa:04:27:9c:2f:4e:aa:3a:25:c0:f6:00:75:ee:2b:
        b0:7a:a8:e9:5f:c0:b7:90:d5:80:e4:16:9a:86:1a:57:9d:cb:
        08:ac:cb:50

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:70:75:6d:00:00:00:00:00:27
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=WIN-2VHX793UTF1-CA
        Validity
            Not Before: Jun 17 05:53:07 2013 GMT
            Not After : Jun 17 06:03:07 2014 GMT
        Subject: C=CN, O=H3C, CN=8048TEST-2008Server-RA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
.....  //证书有删减
//查看本地证书
[Router1]display pki certificate domain h3c local
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            61:5c:c1:1e:00:00:00:00:00:2a
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=WIN-2VHX793UTF1-CA
        Validity
            Not Before: Jun 20 02:03:18 2013 GMT
            Not After : Jun 20 02:13:18 2014 GMT
        Subject: unstructuredAddress=100.1.1.1, C=CN, CN=h3c
```

```
      Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
          Public-Key: (1024 bit)
          Modulus:
            00:bd:61:46:6c:1a:44:cc:97:27:a3:77:b1:cc:ec:
            22:29:e1:65:c3:4e:d4:4d:96:d0:ca:76:bd:4f:8f:
            52:69:33:9d:ea:5e:f3:4d:65:9a:bb:a4:4c:02:a2:
            0f:c4:b0:64:34:e1:79:ad:4b:2d:93:1a:f8:8d:c9:
            5a:92:3e:80:96:b4:8a:c4:f4:3c:fa:7f:f3:88:0d:
            24:0e:6e:b8:ef:53:d2:63:9d:31:f8:09:8e:1a:ae:
            4a:e1:60:63:36:8a:a0:0c:8b:46:fb:2b:53:67:87:
            29:20:b7:45:a0:19:00:a0:91:52:21:55:0d:51:41:
            17:f2:6c:92:56:fe:5f:66:b5
          Exponent: 65537 (0x10001)
      X509v3 extensions:
        X509v3 Key Usage:
          Digital Signature, Non Repudiation, Key Encipherment, Data Encipher
ment
        X509v3 Subject Alternative Name:
          IP Address:100.1.1.1
        X509v3 Subject Key Identifier:
          8F:F9:E7:57:94:F3:A6:FA:78:A9:2E:72:F7:BD:8E:E2:87:13:03:EB
        X509v3 Authority Key Identifier:
.....                                   //证书有删减
<Router1>ping -a 1.1.1.1 2.2.2.2
Ping 2.2.2.2 (2.2.2.2) from 1.1.1.1: 56 data bytes, press escape sequence to brea
k
Request time out                //第一个包丢掉
56 bytes from 2.2.2.2: icmp_seq=1 ttl=255 time=0.438 ms
56 bytes from 2.2.2.2: icmp_seq=2 ttl=255 time=0.238 ms
56 bytes from 2.2.2.2: icmp_seq=3 ttl=255 time=0.218 ms
56 bytes from 2.2.2.2: icmp_seq=4 ttl=255 time=0.252 ms

<Router1>display ike  sa
  Connection-ID   Remote              Flag        DOI
-----------------------------------------------------------------------------
  3             100.1.1.2           RD          IPSEC
Flags:
RD--READY RL--REPLACED FD-FADING
<Router1>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: 100.1.1.1
     remote address: 100.1.1.2
  Flow:
  sour addr: 1.1.1.1/255.255.255.255  port: 0  protocol: ip
  dest addr: 2.2.2.2/255.255.255.255  port: 0  protocol: ip

  [Inbound ESP SAs]
    SPI: 3563806421 (0xd46b5ed5)
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
```

SA remaining duration (kilobytes/sec): 1843199/3582
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: 3208384833 (0xbf3c1141)
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3582
Max sent sequence-number: 4
UDP encapsulation used for nat traversal: N
Status: active

五、 配置关键点：

1. 保证建立IPSEC隧道的两个路由器和CA服务器互通；

2. 获取本地证书前，要先通过配置生成本地密钥对；

3. 本地证书获取要使用握手挑战码，此挑战码是通过WEB访问CA服务器获取得到；

4. ipsec安全策略下（ipsec transform-set）默认是没有加密和认证方法的，这点需要注意。