MSR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

一、 组网需求

在Router1和Router2之间建立一个IPSEC隧道，对Router1所在子网（1.1.1.1/32）和Router2所在的子网（2.2.2.2/32）之间的数据流进行保护

1.Router1和Router2之间采用IKE协商方式建立IPSEC SA；

2.Router1和Router2的隧道建立方式为RSA数据签名方式；

3.证书获取方式为手工导入；

4.IKE第一阶段协商模式采用野蛮模式。

设备清单：MSR路由器2台

二、 组网图

图一 手工导入证书建立IPSEC隧道配置组网图

三、 配置步骤

Router1配置：

```
[Router1]display  current-configuration
#
 version 5.20, Release 2313
#
 sysname Router1
#
acl number 3000
 rule 0 permit ip source 1.1.1.1 0 destination 2.2.2.2 0
#
pki entity h3c
  common-name h3c
#
pki domain h3c
  crl check disable
#
ike proposal 123
 authentication-method rsa-signature
#
ike peer 123
 exchange-mode aggressive
 remote-address 12.1.1.2
 certificate domain h3c
#
ipsec transform-set 123
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
 esp encryption-algorithm des
#
ipsec policy 123 1 isakmp
 security acl 3000
 ike-peer 123
 transform-set 123
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 12.1.1.1 255.255.255.0
 ipsec policy 123
#
```

```
 ip route-static 0.0.0.0 0.0.0.0 12.1.1.2
#
```

Router2配置:

```
[Router2]display  current-configuration
#
 version 5.20, Release 2318, Standard
#
 sysname Router2
#
acl number 3000
 rule 0 permit ip source 2.2.2.2 0 destination 1.1.1.1 0
#
pki entity h3c
  common-name h3c
#
pki domain h3c
  certificate request from ca
  certificate request entity h3c
  crl check disable
#
ike proposal 123
 authentication-method rsa-signature
#
ike peer 123
 exchange-mode aggressive
 remote-address 12.1.1.1
 certificate domain h3c
#
ipsec transform-set 123
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
 esp encryption-algorithm des
#
ipsec policy 123 1 isakmp
 security acl 3000
 ike-peer 123
 transform-set 123
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 12.1.1.2 255.255.255.0
 ipsec policy 123
#
ip route-static 0.0.0.0 0.0.0.0 12.1.1.1
#
```

证书导入步骤:

```
  //导入根证书
[Router1]pki import-certificate ca domain h3c pem filename 2003_server.cer
The trusted CA's finger print is:
    MD5  fingerprint:7EFC 890E 3E04 543F 940A E5FF C79A EAD9
    SHA1 fingerprint:AD8F 99DC CBBE 768E 69CE C10B 8C90 1A27 51BC FBA5

Is the finger print correct?(Y/N):y

%Jul 26 11:00:04:858 2010 Router1 PKI/6/PKI_CA_CERT_TRUSTED: Root CA certificate of the do
main h3c is trusted.
Import CA certificate successfully.
[Router1]
```

%Jul 26 11:00:04:867 2010 Router1 PKI/6/PKI_IMPORT_CA_CERT_SUCC: Imported CA certificates of the domain h3c successfully.

//导入服务器证书
[Router1]pki import-certificate local domain h3c p12 filename 2003_local.pfx
Please input challenge password:
Error:Failed to import the certificate.
There is one key pair on the local device and one in the file.
Please delete the local one.
本地存在密钥对，此处需要先删除本地密钥对：
[Router1]public-key local destroy rsa
Warning: Confirm to destroy these keys? [Y/N]:y
[Router1]pki import-certificate local domain h3c p12 filename 2003_local.pfx
Please input challenge password:　　//此处输入证书密钥
Import local certificate successfully.
Import key pair successfully.
[Router1]
%Jul 26 11:01:54:859 2010 Router1 PKI/6/PKI_IMPORT_LOCAL_CERT_SUCC: Imported local certif icate of the domain h3c successfully.

四、配置验证

[Router1]ping -a 1.1.1.1 2.2.2.2
  PING 2.2.2.2: 56 data bytes, press CTRL_C to break
    Request time out　　//先丢一个包
    Reply from 2.2.2.2: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 2.2.2.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 2.2.2.2: bytes=56 Sequence=3 ttl=255 time=1 ms
Reply from 2.2.2.2: bytes=56 Sequence=4 ttl=255 time=2 ms

display ike sa
    total phase-1 SAs: 1
    connection-id peer　　flag　　phase　doi

     9　　12.1.1.2　　RD|ST　　1　　IPSEC
10　　12.1.1.2　　RD|ST　　2　　IPSEC
五、　配置关键点
1. IKE对等体中，一定要关联认证域；
2. PKI域中要开启crl check disable，否则本地证书会导入失败；
3. 导入本地证书书，若本地已经存在密钥对，需要先删除。