SR6600路由器使用PKI认证建立IPSec隧道功能的配置

管祥杰 2008-12-11 发表

SR6600路由器

使用PKI认证建立IPSec隧道功能的配置

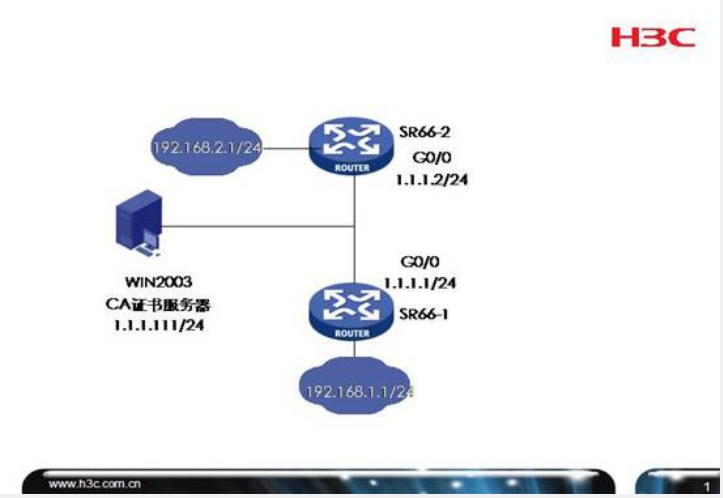
关键词：SR66;IPSec;IKE;PKI;RSA;Win2003;证书服务器

一、组网需求：

如下面的组网图，使用Win2003作为证书服务器，2台SR66路由器需要通过IKE建立IPSec隧道，IKE的认证方式使用PKI证书方式，证书服务器使用Win2003

设备清单：SR6600路由器2台，Win2003主机一台

二、组网图：



三、配置步骤：

设备和版本：SR6600

配置前的操作步骤
//SR66-1和SR66-2都执行如下操作，生成1024位的rsa本地密钥对（含公钥和私钥） [SR661]**public-key local create rsa** The range of public key size is (512 ~ 2048). NOTES: If the key modulus is greater than 512, It will take a few minutes. Press CTRL+C to abort. Input the bits of the modulus[default = 1024]: Generating Keys... ..++++++ .....++++++ ...++++++++ ..++++++++
SR66-1配置

```
#
//定义IKE提议，序号为1，优先度最高，使用rsa签名方式认证
ike proposal 1
 authentication-method rsa-signature
#
//pki实体sr661
pki entity sr661
  //实体的名字
  common-name sr661
  //所属组织部门，注意与CA保持一致
  organization-unit ts-sr66
  //所属组织，与CA保持一致
  organization h3c
  //城市，与CA保持一致
  locality bj
  //所属国家，与CA保持一致，CN表示中国
  country CN
#
//pki认证域h3c
pki domain h3c
  //CA的名字，可以从后面介绍中获得
  ca identifier win2003
  //证书获取URL，可以从后面介绍获得
  certificate request url http://1.1.1.111//certsrv/mscep/mscep.dll
  //证书获取方式为RA，注册委员会，使用Win2003时必须配置
  certificate request from ra
  //指定注册实体为sr661
  certificate request entity sr661
  //指定注册模式和密钥长度
  certificate request mode auto key-length 1024
  //输入CA证书的指纹，即CA证书的缩略图，可以从后面的介绍中获得
  root-certificate fingerprint sha1 c4cb24743e26d601f23b7618b4e749a1061d9eb0
  //CRL，即证书吊销列表的获取URL
  crl url http://1.1.1.111/certenroll/win2003.crl
#
//建立IKE Peer SR662
ike peer sr662
 remote-address 1.1.1.2
 local-address 1.1.1.1
 //指定证书域为h3c
 certificate domain h3c
#
//IPSec提议，即安全提议
ipsec proposal default
#
//IPSec策略
ipsec policy sr662 1 isakmp
 security acl 3000
 ike-peer sr662
 proposal default
#
//定义安全流量的ACL
acl number 3000
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 1.1.1.1 255.255.255.0
 //在出接口上绑定IPSec策略
 ipsec policy sr662
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 192.168.1.1 255.255.255.0
#
 //指定访问对方私网的静态路由
 ip route-static 192.168.2.0 255.255.255.0 1.1.1.2
#
```

SR66-2配置

```
#
//定义IKE提议，序号为1，优先度最高，使用rsa签名方式认证
ike proposal 1
 authentication-method rsa-signature
#
//pki实体sr662
pki entity sr662
  //实体的名字
  common-name sr662
  //所属组织部门，注意与CA保持一致
  organization-unit ts-sr66
  //所属组织，与CA保持一致
  organization h3c
  //城市，与CA保持一致
  locality bj
  //所属国家，与CA保持一致，CN表示中国
  country CN
#
//pki认证域h3c
pki domain h3c
  //CA的名字，可以从后面介绍中获得
  ca identifier win2003
  //证书获取URL，可以从后面介绍获得
  certificate request url http://1.1.1.111//certsrv/mscep/mscep.dll
  //证书获取方式为RA，注册委员会，使用Win2003时必须配置
  certificate request from ra
  //指定注册实体为sr662
  certificate request entity sr662
  //指定注册模式和密钥长度
  certificate request mode auto key-length 1024
  //输入CA证书的指纹，即CA证书的缩略图，可以从后面的介绍中获得
  root-certificate fingerprint sha1 c4cb24743e26d601f23b7618b4e749a1061d9eb0
  //CRL，即证书吊销列表的获取URL
  crl url http://1.1.1.111/certenroll/win2003.crl
#
//建立IKE Peer SR661
ike peer sr661
 remote-address 1.1.1.1
 local-address 1.1.1.2
 //指定证书域为h3c
 certificate domain h3c
#
//IPSec提议，即安全提议
ipsec proposal default
#
//IPSec策略
ipsec policy sr661 1 isakmp
 security acl 3000
 ike-peer sr661
 proposal default
#
//定义安全流量的ACL
acl number 3000
 rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
interface Ethernet0/0
 port link-mode route
 ip address 1.1.1.2 255.255.255.0
 //在出接口上绑定IPSec策略
 ipsec policy sr661
#
interface Ethernet0/1
 port link-mode route
 ip address 192.168.2.1 255.255.255.0
#
 //指定访问对方私网的静态路由
 ip route-static 192.168.1.0 255.255.255.0 1.1.1.1
#
```

手工获取证书的操作

```
//做完上述配置之后，可以通过一些命令来检查证书是否可以正确获取
//第一步，获取CA证书，可以根据提示判断是否正确获得
[SR66-2]pki retrieval-certificate ca domain h3c
Retrieving CA/RA certificates. Please wait a while.....
Saving CA/RA certificates chain, please wait a moment.....
%Dec 20 21:02:08:705 2006 2 PKI/4/Verify_CA_Root_Cert:CA root certificate of the domain h3c is trusted.
CA certificates retrieval success.
[SR662]
%Dec 20 21:02:08:754 2006 2 PKI/4/Update_CA_Cert:Update CA certificates of the Domain h3c successfully.
%Dec 20 21:02:08:755 2006 2 PKI/4/CA_Cert_Retrieval:Retrieval CA certificates of the domain h3c successfully.
//上述信息提示正确获得CA证书，即根证书，第二步，获取CA签名的本地证书
[SR66-2]pki request-certificate domain h3c
Certificate is being requested, please wait.....
[SR662]
Enrolling the local certificate,please wait a while.....
Certificate request Successfully!
Saving the local certificate to device.....
Done!
```

%Dec 20 21:02:29:02 2006 2 PKI/4/Local_Cert_Request:Request local certificate of the domain h3c successfully.
//上述信息提示本地证书获取成功，第三步，获取CRL，可以检查同一个CA签名的证书是否过期
[SR66-2]pki retrieval-crl domain h3c
Connecting to server for retrieving CRL. Please wait a while.....
CRL retrieval success!
[SR662]
%Dec 20 21:03:59:211 2006 SR662 PKI/4/Update_CRL:Update CRL of the domain h3c successfully.
%Dec 20 21:03:59:212 2006 SR662 PKI/4/Retrieval_CRL:Retrieval CRL of the domain h3c successfully.
[SR662]
//显示CA证书
[SR662]dis pki cert ca d h3c
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
613E1A31 00000000 0002
Signature Algorithm: sha1WithRSAEncryption
Issuer:
CN=win2003
Validity
Not Before: Dec 20 12:08:59 2006 GMT
Not After : Dec 20 12:18:59 2007 GMT
Subject:
C=CN
ST=bj
L=bj
O=h3c
OU=ts-sr66
CN=win2003
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00C2A4CE C5344632 263595CC 0680FA75
26E77572 D06E32F9 E717C20C 6D87A6C1
CF1F2C9A 46323DC6 0C72B06E 7B1D8C3E
0565EFF7 FEBEA570 F6DE66FF AD1EE75E
3E481A80 6A5FE282 CA41FD2B 92814482
6FB06093 E880F237 F984AA21 A53E52C8
7529C486 58965EB5 DFAEA99D 8A5B338D
FCAEAA1F AC1EA4B2 44F77393 E76EE67C
D1
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Key Usage: critical
Digital Signature, Non Repudiation
X509v3 Extended Key Usage:
1.3.6.1.4.1.311.20.2.1
1.3.6.1.4.1.311.20.2:
.,.E.n.r.o.l.l.m.e.n.t.A.g.e.n.t.O.f.f.l.i.n.e
X509v3 Subject Key Identifier:
4E5E380E DB22491E 3C5EE3DA FB26ED51 F7DD47F5
X509v3 Authority Key Identifier:
keyid:C818C4A6 0A5C766B E7C51760 2789A402 75181ABD

X509v3 CRL Distribution Points:
URI:http://ts-sr66/CertEnroll/win2003.crl
URI:file://\\ts-sr66\CertEnroll\win2003.crl

Authority Information Access:
CA Issuers - URI:http://ts-sr66/CertEnroll/ts-sr66_win2003.crt
CA Issuers - URI:file://\\ts-sr66\CertEnroll\ts-sr66_win2003.crt

Signature Algorithm: sha1WithRSAEncryption
6DA0B262 BACC97AA 614CEEED 83300939
E7C377F5 62F6B9E6 C21965DC D17FC116
7957E7E5 6FAE97A3 97BD1A65 27ADC066
92241702 7547DB45 74B5BC65 32CD45A6
FC1F2D69 EA8F8055 91E48C06 3FC63D58
18F1F130 37CDFF4B 6DCEC700 9DFAC050
DF4BF36D 2EA4D4F8 F09726AA 5C24D9D6
29708256 329BF4ED 69FA7948 E1C1058C
D45E06FD E05BFE20 C0C01CCB 3146110B
791B6573 68927EEA FBCA6283 6D2CA93A
7E32A9E8 E42B49AC 0ACAF60B 85FFBC00
FC2E427C 25EA55F0 DDE64A3F 06BF8001
2CC5FBC6 96ED277D 0AF4308B EE06C7DD
26364063 4D89FAF5 E26B681A 919D5F2D
F7E8D6F7 BBD9F64D CD3C864B FC538A99
DED85FA9 9910824A 084BA148 0A1BB899

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
613E1BA8 00000000 0003
Signature Algorithm: sha1WithRSAEncryption
Issuer:

```
        CN=win2003
      Validity
        Not Before: Dec 20 12:08:59 2006 GMT
        Not After : Dec 20 12:18:59 2007 GMT
      Subject:
        C=CN
        ST=bj
        L=bj
        O=h3c
        OU=ts-sr66
        CN=win2003
      Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (1024 bit)
          Modulus (1024 bit):
            00B8C294 112CDA38 27FE4564 3DDDE52C
            A428A819 0DF0DD94 7ECD7B74 F596294B
            1373BA5E 6A324BE4 98978E30 96036AC1
            2703324E B3D912FC E52DCDB1 24B05001
            C26B2E08 46FCD00F C4518415 C912AF39
            311BDE7F 7396AF31 AF9E0642 DB010702
            E36B954F 5BB881D7 328BEC88 0EA1AA82
            83900CBC E4E85A9B FE176046 136DF65D
            FF
          Exponent: 65537 (0x10001)
      X509v3 extensions:
        X509v3 Key Usage: critical
        Key Encipherment, Data Encipherment
        S/MIME Capabilities:
....80...+....  0'0
        X509v3 Extended Key Usage:
        1.3.6.1.4.1.311.20.2.1
        1.3.6.1.4.1.311.20.2:
          ...C.E.P.E.n.c.r.y.p.t.i.o.n
        X509v3 Subject Key Identifier:
        6A80370A A194479F 5C083027 A18CA358 BA43FD52
        X509v3 Authority Key Identifier:
        keyid:C818C4A6 0A5C766B E7C51760 2789A402 75181ABD

        X509v3 CRL Distribution Points:
        URI:http://ts-sr66/CertEnroll/win2003.crl
        URI:file://\\ts-sr66\CertEnroll\win2003.crl

        Authority Information Access:
        CA Issuers - URI:http://ts-sr66/CertEnroll/ts-sr66_win2003.crt
        CA Issuers - URI:file://\\ts-sr66\CertEnroll\ts-sr66_win2003.crt

    Signature Algorithm: sha1WithRSAEncryption
      B7E66039 EEFA866A 6C3D937E 0702775B
      49CF1C23 7D3ADD49 FC24AEBB DF525A91
      6898EA6B 0CDF345F 50847975 F73DE485
      3F055FB2 46AC212A 4D903852 5FA16E19
      626FCECE ED0BF5A3 56604253 BFA8F44E
      F7315A5F EE55E2A2 74A343CE A867BEE8
      2216AEFD 49AE27B7 81726DE5 F7D8CAC6
```