SecPath防火墙IPsec WITH CA的典型配置

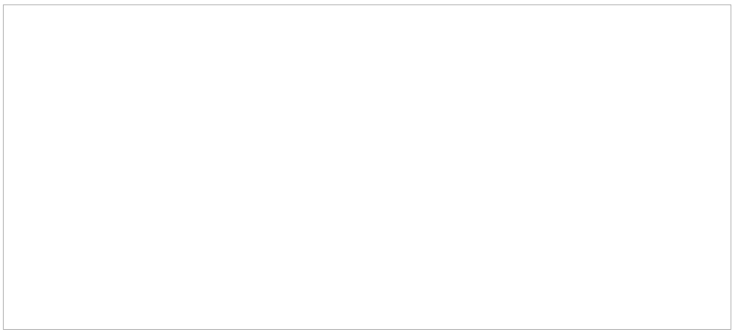
刘军 2006-09-08 发表

SecPath防火墙IPsec with CA 典型配置指南

一、 组网需求

防火墙建立IPSEC VPN有两种验证方法，一种是预共享密钥，一种是证书认证，在一些安全性要求较高的一些场合，如政府、军队、公安在建立VPN时一般都推荐使用证书方式验证，下面讲述的手动方式申请证书及建立VPN的过程。

二、 组网图



如图所示，SecPath1000F要与SecPath500F-B建立基于证书的VPN，中间的SecPath500F只起数据转发的作用。

软件版本如下：

SecPath1000F： VRP 3.40 ESS 1604;

SecPath500F： VRP 3.40 ESS 1604;

SecPath500F-B： VRP 3.40 ESS 1604。

三、 典型配置

1.基本配置命令

定义PKI Domain

pki domain 1 *//Domain名称*

ca identifier win2003 *//ca服务器的名称，可在//win2003命令行中输入certutil查看名称，也可进入"证书服务"查看*

certificate request url http://5.5.5.5 *//由于是静态配置，此处URL地址可随意配置*

certificate request from ra *//Windows2003仅支持RA模式*

certificate request entity 3000

crl check disable

PKI实体配置

pki entity 3000 *//PKI实体配置，此处名称应该与PKI Domain中的实体名称一样*

common-name 3000

organization-unit tc

organization H3C

locality beijing

country cn

通过RSA生成公、私密钥对

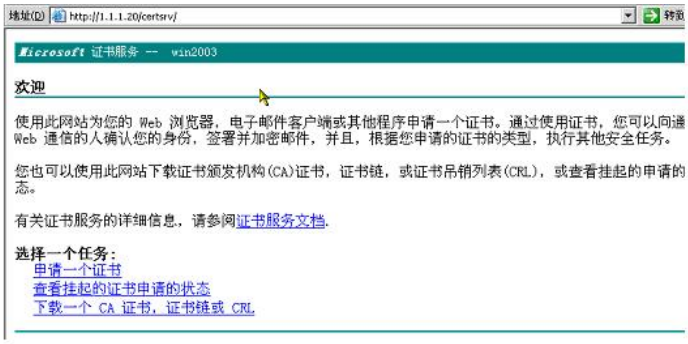
[Quidway]rsa local-key-pair create

打印出本地证书请求信息，通过带外方式向RA申请证书

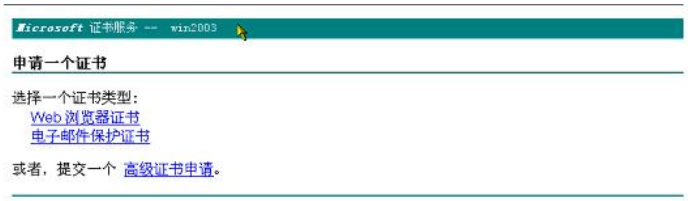
[Quidway]pki request-certificate domain 1 pkcs10

向win2003server申请证书（证书服务器的安装及使用请参照附件《证书服务器配置指南》

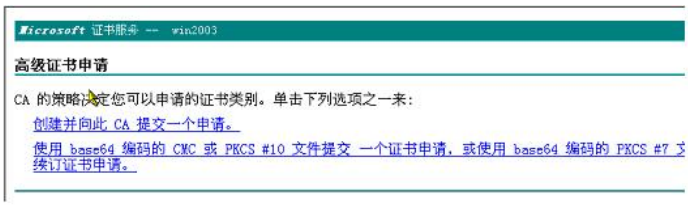
打开证书服务器申请主页，选择"申请一个证书"



选择“高级证书申请”



选择使用PKCS#10文件提交证书申请



将路由器中本地证书请求信息粘贴到表格中，点击提交

完成证书申请后，可以看到如下信息。

当证书服务器管理员颁发证书后，回到主页点击“查看挂起…”获取实体证书，点击“下载一个CA…”获取CA证书

将CA和实体证书通过FTP上载到路由器的FLASH中，用import-certificate引入证书

```
<Quidway>dir
Directory of flash:/

   0   -rw-   8853504  Dec 06 2004 12:00:03   main.bin
   1   -rw-       428  Dec 28 2004 10:31:33   hostkey
   2   -rw-       572  Dec 28 2004 10:31:43   serverkey
   3   -rw-       851  Dec 28 2004 13:57:19   3000.cer
   4   -rw-       870  Dec 28 2004 13:57:33   certnew.cer
   5   -rw-      1309  Dec 21 2004 10:44:17   ipsecpki.cfg

31877 KB total (23196 KB free)

<Quidway>sys
System View: return to User View with Ctrl+Z.
[Quidway]pki import-certificate ca domain 1 der filename certnew.cer
```

在引入CA证书时，需要确定该证书的“指纹”是否正确

```
Importing certificates. Please wait a while......

The trusted CA's finger print is:
    MD5  fingerprint:CACB 65CB E1AE A40B A35A 90C7 368C 3E58
    SHA1 fingerprint:5C76 2CCA A432 DCF5 B079 FE6B 06BC 896C A6A4 7B38

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

%Dec 28 16:55:08:805 2004 Quidway PKI/5/Verify_CA_Root_Cert:CA root certi
of the domain 1 is trusted......
Import CA certificate successfully.
%Dec 28 16:55:16:640 2004 Quidway PKI/5/Update_CA_Cert:Update CA certifics
 the Domain 1 successfully.
[Quidway]
%Dec 28 16:55:16:770 2004 Quidway PKI/5/Import_CA_Cert:Import CA certifics
 the domain 1 successfully.
```

正确引入实体证书后，会有相应提示信息

```
[Quidway]pki import-certificate local domain  1 der filename 3000.cer
Importing certificates. Please wait a while......
%Dec 28 16:57:20:818 2004 Quidway PKI/5/Verify_Cert:Verify certificate CN=
U=tc,O=huawei-3com,L=beijing,C=CN of the domain 1 successfully.....
Import local certificate successfully.
%Dec 28 16:57:25:173 2004 Quidway PKI/5/Import_Local_Cert:Import local cer
te of the domain 1 successfully.
```

最终配置

路由器SecPath500-B的最终配置

```
500F-B>dis cu
#
 sysname 500F-B
#
 ike local-name 500f
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
 firewall statistic system enable
#
pki entity 2000
  common-name 2000
  organization-unit tc
  organization h3c
  locality beijing
  country CN
#
pki domain 1
  ca identifier ts-sec
  certificate request url http://5.5.5.1
  certificate request from ra
  certificate request entity 2000
  crl check disable
#
radius scheme system
#
domain system
#
ike proposal 1
 authentication-method rsa-signature
#
ike peer 1000f
 exchange-mode aggressive
 id-type name
 remote-name 1000f
 nat traversal
 certificate domain 1
```

```
#
ike peer 100f
#
ipsec proposal p1
#
ipsec policy test 1 isakmp
 security acl 3000
 ike-peer 1000f
 proposal p1
#
acl number 3000
 rule 0 permit ip source 2.2.2.0 0.0.0.255 destination 3.3.3.0 0.0.0.255
#
interface Aux0
 async mode flow
#
interface GigabitEthernet0/0
 loopback
 ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet0/1
#
interface GigabitEthernet1/0
 ip address 1.1.1.1 255.255.255.0
 ipsec policy test
#
interface GigabitEthernet1/1
#
interface Encrypt2/0
#
interface NULL0
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface GigabitEthernet0/0
 add interface GigabitEthernet1/0
 set priority 85
#
firewall zone untrust
 set priority 5
#
firewall zone DMZ
 set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local DMZ
#
firewall interzone trust untrust
#
firewall interzone trust DMZ
#
firewall interzone DMZ untrust
#
 ip route-static 3.3.3.0 255.255.255.0 1.1.1.2 preference 60
 ip route-static 4.4.4.0 255.255.255.0 1.1.1.2 preference 60
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
```

```
 authentication-mode none
 user privilege level 3
#
return
<500f>
```
防火墙 SecPath1000F的最终配置
```
<1000f>dis cu
#
 sysname 1000f
#
 ike local-name 1000f
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
 firewall statistic system enable
#
 qos carl 1 dscp 16
 qos carl 2 dscp 16
 qos carl 3 mac 0000-1111-2222
 qos carl 4 precedence 0
 qos carl 5 precedence 2
#
 firewall blacklist enable
 firewall blacklist 10.1.1.123
#
pki entity 3000
  common-name 3000
  organization-unit tc
  organization h3c
  locality beijing
  country cn
#
pki domain 1
  ca identifier ts-sec
  certificate request url http://5.5.5.5
  certificate request from ra
  certificate request entity 3000
  crl check disable
#
radius scheme system
#
domain system
#
local-user aaa
 password simple aaaaaa
 service-type telnet
 level 3
local-user ftp
 password simple ftp
 service-type ftp
#
ike proposal 1
 authentication-method rsa-signature
#
ike peer 500f
 exchange-mode aggressive
 id-type name
 remote-name 500f
 remote-address 1.1.1.1
 nat traversal
 certificate domain 1
#
ike peer test
```

```
#
ipsec proposal p1
#
ipsec policy test 1 isakmp
 security acl 3000
 ike-peer 500f
 proposal p1
#
acl number 3000
 rule 0 permit ip source 3.3.3.0 0.0.0.255 destination 2.2.2.0 0.0.0.255
#
interface Aux0
 async mode flow
#
interface GigabitEthernet0/0
 ip address 3.3.3.1 255.255.255.0
 qos gts acl 3000 cir 150000 cbs 75000 ebs 0 queue-length 50
#
interface GigabitEthernet0/1
 ip address 4.4.4.2 255.255.255.0
 ipsec policy test
#
interface GigabitEthernet1/0
 shutdown
 ip address 55.1.1.1 255.255.255.0
 qos gts any cir 50000000 cbs 75000000 ebs 0 queue-length 50
#
interface GigabitEthernet1/1
#
interface Encrypt2/0
#
interface NULL0
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface GigabitEthernet0/0
 add interface GigabitEthernet0/1
 add interface GigabitEthernet1/0
 set priority 85
#
firewall zone untrust
 set priority 5
#
firewall zone DMZ
 set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local DMZ
#
firewall interzone trust untrust
#
firewall interzone trust DMZ
#
firewall interzone DMZ untrust
#
 FTP server enable
#
 ip route-static 1.1.1.0 255.255.255.0 4.4.4.1 preference 60
 ip route-static 2.2.2.0 255.255.255.0 4.4.4.1 preference 60
```

```
#
user-interface con 0
user-interface aux 0
user-interface vty 0
 undo shell
user-interface vty 1 4
#
return
<1000f>
```

防火墙SecPath500F的最终配置

```
<mid-500>dis cu
#
 sysname mid-500
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
 firewall statistic system enable
#
radius scheme system
#
domain system
#
acl number 2000
 rule 0 permit source 4.4.4.0 0.0.0.255
#
interface Aux0
 async mode flow
#
interface GigabitEthernet0/0
 ip address 1.1.1.2 255.255.255.0
#
interface GigabitEthernet0/1
#
interface GigabitEthernet1/0
 ip address 4.4.4.1 255.255.255.0
#
interface GigabitEthernet1/1
#
interface Encrypt2/0
#
interface NULL0
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface GigabitEthernet0/0
 add interface GigabitEthernet1/0
 set priority 85
#
firewall zone untrust
 set priority 5
#
firewall zone DMZ
 set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local DMZ
#
firewall interzone trust untrust
```

#
firewall interzone trust DMZ
#
firewall interzone DMZ untrust
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
 authentication-mode none
 user privilege level 3
#
return

四、配置关键点

IKE配置时要要用RSA签名

ike proposal 1
 authentication-method rsa-signature

配置IKE PEER时要采用申请的domain的证书

certificate domain 1