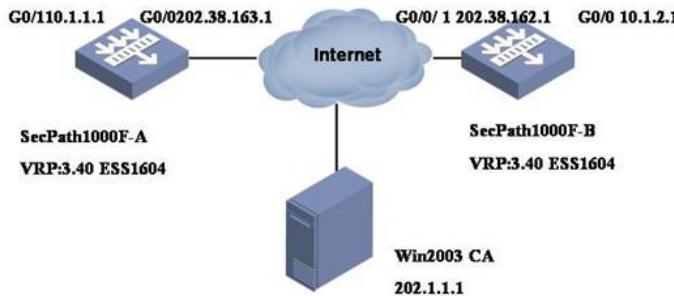


SecPath 1000F防火墙主模式IPSec
with CA手工申请典型配置指南

一、 组网需求

用户需要在主模式下，手动申请证书建立IPSec。

二、 组网图



如图所示，SecPath1000F-A要与SecPath1000F-B建立基于证书的VPN。

软件版本如下：

SecPath1000F-A： VRP 3.40 ESS 1604；

SecPath1000F-B： VRP 3.40 ESS 1604；

三、 典型配置

1. 基本配置命令

定义PKI Domain

```
pki domain 8042.com //Domain名称
```

```
ca identifier h3c //ca服务器的名称
```

```
certificate request url http://3.1.1.1 //由于是手动发起，URL可任意配置
```

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

```
certificate request entity 1kf-2
```

```
crl check disable
```

PKI实体配置

```
pki entity 8042.com //PKI实体配置，此处名称应该与PKI Domain中的实体名称一样
```

```
common-name SecPath 1kf-2
```

```
locality ShangDi
```

```
state Beijing
```

```
country CN
```

```
fqdn 1kf-2.8042.com
```

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 8042.com pkcs10
```

```
[Quidway]pki request-certificate do 1 pkcs10
-----BEGIN CERTIFICATE REQUEST-----
MIIBCzCBtgIBADBRMqswCQYDVQQGEwJDTjE0MA4GA1UEBxMHYmVpamluZzEUMBIG
A1UEChMlaHvhd2VpLTNjb20xCzAJBgNVBAgTAnRjMQ0wCwYDVQDBwQzMDAwMFww
DQYJKoZIhvcNAQEBBQADSwAwSAJBAMz2VmyM1HY0EY1iNCwskWh6VgfTIDN1kad2
T9Hjt94caY21ACnFDoX7UHtQmhyCmDmmefGxTBV4S2ogL1YrAXUCAwEAAsAAMA0G
CSqGSib3DQEBBUA0EAZw4vIWjZkdH9GCpsn15Lr+heIHpwMJJay6i91SEUggT
ZalsGwVTegJEYBwt6F7kCD63dxoh8eUdUPJJZEBYw==
-----END CERTIFICATE REQUEST-----
```

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”

```
[Quidway]pki request-certificate do 1 pkcs10
-----BEGIN CERTIFICATE REQUEST-----
MIIBCzCBtgIBADBRM0swC0YDVQGGEwD1jEQMA4GA1UEBxMHYmVpamluzzEUMBIG
A1UEChMLaHvh2VpLTNjb20xCzAJBgNVBAAsTAnRjMQ0wCwYDVQQDEwQzMDAwMFww
DQYJKoZIhvcNAQEBOQADSvAwSAjBAMz2VmhyM1HY0EYLiNCwskWh6VgftIDN1kad2
T9HjT94caY21AcnfPoX7UhtQmhyCmDmnefGxTBY4S2ogLlYrAXUCAwEAAsAAMA0G
CSqGS1b3DQEBAUAA0EAZw4vIwjZkdDH9GCpsm15Lr+heIHWMJJay6I91SEUggT
ZalsGwVTejYEYBwt6F7kCD63dXxoh8oUdUPJJZEBYw==
-----END CERTIFICATE REQUEST-----
```

选择“高级证书申请”

地址: Http://1.1.1.20/certsrv/ Microsoft 证书服务 -- win2003 主页

欢迎

使用此网站为您的 Web 浏览器,电子邮件客户端或其他程序申请一个证书。通过使用证书,您可以向通过 Web 通信的人确认您的身份,签署并加密邮件,并且,根据您申请的证书的类型,执行其他安全任务。

您也可以使用此网站下载证书颁发机构(CA)证书,证书链,或证书吊销列表(CRL),或查看挂起的申请的状态。

有关证书服务的详细信息,请参阅[证书服务文档](#)。

选择一个任务:

- [申请一个证书](#)
- [查看挂起的证书申请的状态](#)
- [下载一个 CA 证书,证书链或 CRL](#)

选择使用PKCS#10文件提交证书申请

Microsoft 证书服务 -- win2003 主页

申请一个证书

选择一个证书类型:

- [Web 浏览器证书](#)
- [电子邮件保护证书](#)

或者, 提交一个 [高级证书申请](#)。

将路由器中本地证书请求信息粘贴到表格中,点击提交

Microsoft 证书服务 -- win2003 主页

高级证书申请

CA 的策略决定了您可以申请的证书类别。单击下列选项之一来:

- [创建并向此 CA 提交一个申请。](#)
- [使用 base64 编码的 CMC 或 PKCS #10 文件提交一个证书申请,或使用 base64 编码的 PKCS #7 文件续订证书申请。](#)

完成证书申请后,可以看到如下信息。

Microsoft 证书服务 -- win2003 主页

提交一个证书申请或续订申请

要提交一个保存的申请到 CA,在“保存的申请”框中粘贴一个由外部源(如 Web 服务器)生成的 base-64 编码的 CMC 或 PKCS #10 证书申请或 PKCS #7 续订申请。

保存的申请:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBCzCBtgIBADBRM0swC0YDVQGGEwD1jEQMA4G
A1UEChMLaHvh2VpLTNjb20xCzAJBgNVBAAsTAnRj
DQYJKoZIhvcNAQEBOQADSvAwSAjBAMz2VmhyM1HY0
T9HjT94caY21AcnfPoX7UhtQmhyCmDmnefGxTBY4
CSqGS1b3DQEBAUAA0EAZw4vIwjZkdDH9GCpsm15
|
```

[浏览要插入的文件。](#)

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

Microsoft 证书服务 -- win2003 主页

证书挂起

您的证书申请已经收到。但是,您必须等待管理员颁发您申请的证书。

您的申请 Id 为 3。

请在一天或两天内返回此网站以检索您的证书。

注意: 您必须用此 Web 浏览器在 10 天内返回以检索您的证书

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

Microsoft 证书服务 — win2003

主页

欢迎

使用此网站为您的 Web 浏览器、电子邮件客户端或其他程序申请一个证书。通过使用证书，您可以向通过 Web 通信的人确认您的身份，签署并加密邮件，并且，根据您申请的证书的类型，执行其他安全任务。

您也可以使用此网站下载证书颁发机构(CA)证书、证书链，或证书吊销列表(CRL)，或查看挂起的申请的状态。

有关证书服务的详细信息，请参阅[证书服务文档](#)。

选择一个任务：

[申请一个证书](#)
[查看挂起的证书申请的状态](#)
[下载一个 CA 证书、证书链或 CRL](#)

在引入CA证书时，需要确定该证书的“指纹”是否正确

```
<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
```

正确引入实体证书后，会有相应提示信息

最终配置

```
防火墙 SecPath1000F-A的最终配置
SecPath1000F-A>dis cu
#
sysname SecPath1000F-A
#
firewall packet-filter enable
firewall packet-filter default permit
#
undo connection-limit enable
connection-limit default deny
connection-limit default amount upper-limit 50 lower-limit 20
#
firewall statistic system enable
#
pki entity 1kf-2
common-name SecPath 1kf-2
locality ShangDi
state Beijing
country CN
fqdn 1kf-2.8042.com
#
pki domain 8042.com
ca identifier h3c
certificate request url http://3.3.3.1
certificate request from ra
certificate request entity 1kf-2
crl check disable
#
radius scheme system
#
domain system
#
#
ike proposal 2
authentication-method rsa-signature
encryption-algorithm 3des-cbc
dh group5
#
ike peer peer
remote-address 202.38.162.1
```

```
certificate domain 8042.com
#
ipsec proposal pro
transform ah-esp
esp authentication-algorithm md5
#
ipsec policy pol 1 isakmp
security acl 3000
ike-peer peer
proposal pro
#
acl number 3000
rule 1 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.2
55
#
interface Aux0
async mode flow
#
interface GigabitEthernet0/0
ip address 202.38.163.1 255.255.255.0
ipsec policy pol
#
interface GigabitEthernet0/1
ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0
ip address 192.168.1.2 255.255.255.0
#
interface GigabitEthernet1/1
#
interface Encrypt2/0
#
interface NULL0
#
firewall zone local
set priority 100
#
firewall zone trust
add interface GigabitEthernet0/0
add interface GigabitEthernet0/1
add interface GigabitEthernet1/0
add interface GigabitEthernet1/1
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 0.0.0.0 0.0.0.0 202.38.163.2 preference 60
```

```
#  
firewall defend syn-flood zone local  
#  
user-interface con 0  
user-interface aux 0  
user-interface vty 0 4  
#  
return  
防火墙 SecPath1000F-B的最终配置  
SecPath1000F-B>dis cu  
#  
sysname SecPath1000F-B  
#  
firewall packet-filter enable  
firewall packet-filter default permit  
#  
connection-limit disable  
connection-limit default deny  
connection-limit default amount upper-limit 50 lower-limit 20  
#  
firewall statistic system enable  
#  
pki entity 1kf-2  
common-name SecPath 1kf-2  
locality ShangDi  
state Beijing  
country CN  
fqdn 1kf-2.8042.com  
#  
pki domain 8042.com  
ca identifier h3c  
certificate request url http://3.3.3.1/  
certificate request from ra  
certificate request entity 1kf-2  
crl check disable  
#  
radius scheme system  
#  
domain system  
#  
#  
ike proposal 2  
authentication-method rsa-signature  
encryption-algorithm 3des-cbc  
dh group5  
#  
ike peer peer  
remote-address 202.38.163.1  
certificate domain 8042.com  
#  
ipsec proposal pro  
transform ah-esp  
esp authentication-algorithm md5  
#  
ipsec policy pol 1 isakmp  
security acl 3000  
ike-peer peer  
proposal pro  
#  
acl number 3000  
rule 1 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.2  
55  
#  
interface Aux0
```

```
async mode flow
#
interface Ethernet1/0
#
interface GigabitEthernet0/0
ip address 202.38.162.1 255.255.255.0
ipsec policy pol
#
interface GigabitEthernet0/1
ip address 10.1.2.1 255.255.255.0
#
interface Encrypt2/0
#
interface NULL0
#
firewall zone local
set priority 100
#
firewall zone trust
add interface GigabitEthernet0/0
add interface GigabitEthernet0/1
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 0.0.0.0 0.0.0.0 202.38.162.2 preference 60
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
return
```

四、配置关键点

1IKE配置时要用RSA签名
2配置IKE PEER时要采用申请的domain的证书