SecPath 1000F防火墙野蛮模式IPSec with CA 自动申请典型配置指南

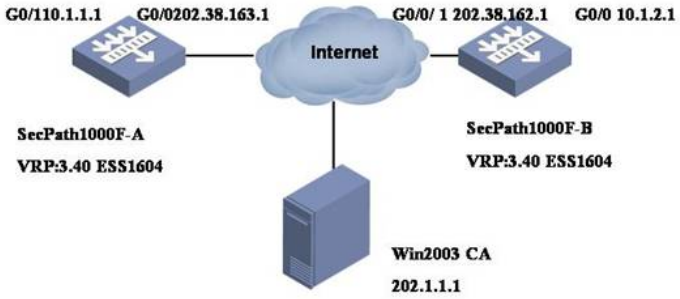
刘军 2006-11-03 发表

SecPath 1000F防火墙野蛮模式IPSec with CA自动申请典型配置指南

一、 组网需求

用户需要在野蛮模式下，自动申请证书建立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://1.1.1.20/certsrv/mscep/mscep.dll*由于是自动发起，URL必须配置成证书服务器的URL*

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

引入CA服务器证书

[Quidway] pki retrieval-certificate ca domain 1

```
[Quidway]pki retrieval-certificate ca domain 1
Retrieving CA/RA 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 FE6E 06BC 896C A6A4 7B38

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

Saving CA/RA certificates chain, please wait a moment......
%Dec 29 16:48:07:03 2004 Quidway PKI/5/Verify_CA_Root_Cert:CA root certificate
f the domain 1 is trusted......
CA certificates retrieval success.
%Dec 29 16:48:15:36 2004 Quidway PKI/5/Update_CA_Cert:Update CA certificates o
the Domain 1 successfully.
```

查看指纹和CA证书的指纹是否一致，输入“Y”后，路由器自动引入CA证书

动态申请实体证书

[Quidway] pki request-certificate domain 1

防火墙自动完成注册申请，获得证书。（这是CA服务器配置为自动发放证书时结果。如果CA服务器配置为管理员颁发模式，路由器需要等待一段时间后才能获得证书，不能手动获取已经颁发的证书。）

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://202.1.1.1/certsrv/mscep/mscep.dll

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

exchange-mode aggressive

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://202.1.1.1/certsrv/mscep/mscep.dll 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
exchange-mode aggressive
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

IIKE配置时要要用RSA签名。

配置IKE PEER时要采用申请的domain的证书 。

自动申请证书时，要指定证书服务器的地址。

在配置IKE PEER时，要指定为野蛮模式。