comwareV7 ipsec RSA证书认证典型配置

IPSec VPN　孔德飞　2021-12-21 发表

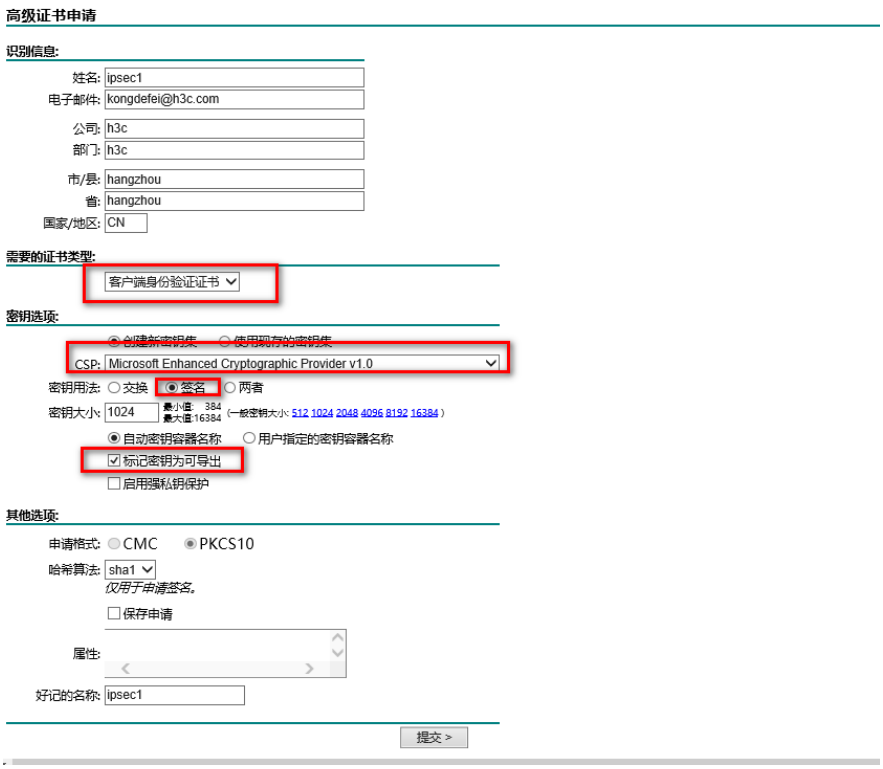
组网及说明

组网如图：

DeviceA与DeviceB以证书的方式建立IPSEC，刚兴趣流使用loopback0充当

配置步骤

前提是已经获得CA证书与服务器证书，现网中需要购买CA与服务器证书
本实验自行搭建CA服务器，然后申请CA证书有服务器证书
IPSEC证书申请的时候，标红的部分一定要和下面一致



DeviceA的主要配置：
（1）证书相关配置
创建PKI域

```
pki domain domain1
 public-key rsa signature name rsa1
 undo crl check enable
```

创建PKI实体

```
pki entity entity1
 common-name ipsec1
```

导入证书（前提是将CA证书与本地证书已经上传到设备上）

```
pki import domain domain1 der ca filename ca.cer
```

```
pki import domain domain1 p12 local filename ipsec1.pfx
```

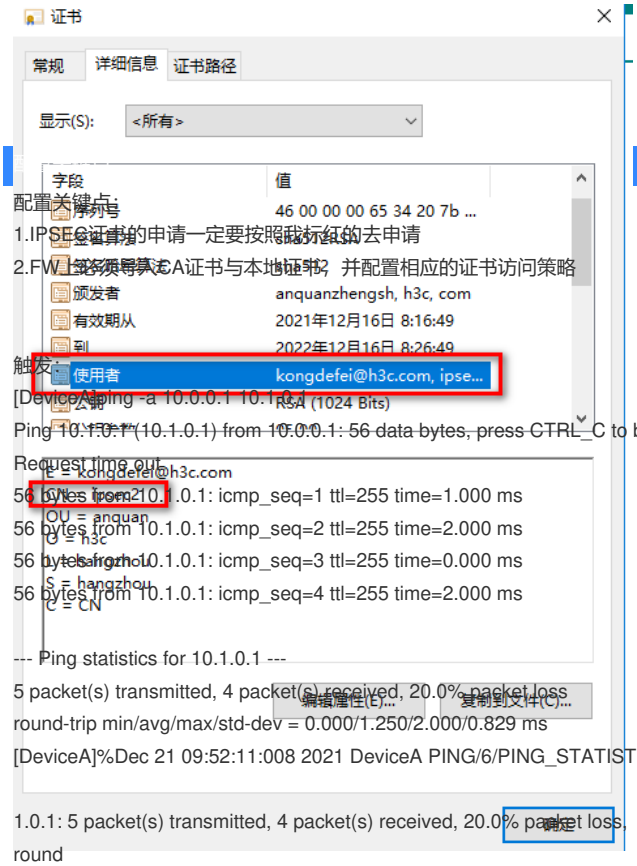
创建证书访问策略

```
pki certificate access-control-policy policy1
 rule 1 permit group1
```

创建证书访问规则，对端证书subject-name DN中需包含（ctn）规则中定义的字符串才被认为是有效的证书。本例使用的证书subject-name DN中包含字符“ipsec2”，因此在这里使用参数ctn ipsec2。

```
pki certificate attribute-group group1
 attribute 1 subject-name dn ctn ipsec2
```

PS:DN：distinguished name，唯一区别名，其实就是证书的使用者，本例子取其中的一个字段CN



配置关键点：

1.IPSEC证书的申请一定要按照我标红的去申请

2.FW上必须导入CA证书与本地证书，并配置相应的证书访问策略

触发：

[DeviceA]ping -a 10.0.0.1 10.1.0.1

Ping 10.1.0.1 (10.1.0.1) from 10.0.0.1: 56 data bytes, press CTRL_C to break

Request time out

56 bytes from 10.1.0.1: icmp_seq=1 ttl=255 time=1.000 ms

56 bytes from 10.1.0.1: icmp_seq=2 ttl=255 time=2.000 ms

56 bytes from 10.1.0.1: icmp_seq=3 ttl=255 time=0.000 ms

56 bytes from 10.1.0.1: icmp_seq=4 ttl=255 time=2.000 ms

--- Ping statistics for 10.1.0.1 ---

5 packet(s) transmitted, 4 packet(s) received, 20.0% packet loss

round-trip min/avg/max/std-dev = 0.000/1.250/2.000/0.829 ms

[DeviceA]%Dec 21 09:52:11:008 2021 DeviceA PING/6/PING_STATISTICS: -COntext=1; Ping statistics for 10.1.0.1: 5 packet(s) transmitted, 4 packet(s) received, 20.0% packet loss, round-trip min/avg/max/std-dev = 0.000/1.250/2.000/0.829 ms.

（2）ipsec主要配置

配置感兴趣流

[DeviceA]

interface LoopBack0

ip address 10.0.0.1 255.255.255.255

acl advanced 3000

rule 0 permit ip source 10.0.0.1 0 destination 10.1.0.1 0

ike的配置

[DeviceA]dis

ike profile profile1

certificate domain domain1

exchange-mode aggressive

local-identity dn

match remote certificate policy1

#

ike proposal 10

authentication-method rsa-signature

authentication-algorithm md5

ipsec的配置

ipsec transform-set tran1

esp encryption-algorithm des-cbc

esp authentication-algorithm sha1

#

ipsec policy map1 10 isakmp

transform-set tran1

security acl 3000

remote-address 1.1.1.3

ike-profile profile1

接口应用IPSEC策略

interface GigabitEthernet1/0/1

port link-mode route

combo enable copper

ip address 1.1.1.2 255.255.255.0

[DeviceA]dis ike sa

Connection-ID Remote Flag DOI

---

1 1.1.1.3 RD IPsec

Flags:

RD--READY RL--REPLACED FD-FADING RK-REKEY

[DeviceA]display ips

[DeviceA]display ipsec sa

Interface: GigabitEthernet1/0/1

IPsec policy: map1

Sequence number: 10

Mode: ISAKMP

Tunnel id: 0

Encapsulation mode: tunnel

Perfect Forward Secrecy:

Inside VPN:

Extended Sequence Numbers enable: N

Traffic Flow Confidentiality enable: N

Path MTU: 1444

Tunnel:

local address: 1.1.1.2

remote address: 1.1.1.3

Flow:

sour addr: 10.0.0.1/255.255.255.255 port: 0 protocol: ip

dest addr: 10.1.0.1/255.255.255.255 port: 0 protocol: ip

[Inbound ESP SAs]

SPI: 3569554732 (0xd4c3152c)

Connection ID: 4294967296
ipsec apply policy map1
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
静态路由的配置
SA duration (kilobytes/sec): 1843200/3600
ip route-static 0.0.0.0 0 1.1.1.3
SA remaining duration (kilobytes/sec): 1843199/3593
Max received sequence-number: 4
安全域与安全策略配置
Anti-replay check enable: Y
security-zone name Trust
Anti-replay window size: 64
import interface GigabitEthernet1/0/1
UDP encapsulation used for NAT traversal: N
Status: Active
security-policy ip
[Outbound ESP SAs]
rule 0 name 0
SPI: 3128190466 (0xba746602)
action pass
Connection ID: 4294967297
Transform set: ESP-ENCRYPT-DES-CBC ESP-AUTH-SHA1
deviceB的主要配置
SA duration (kilobytes/sec): 1843200/3600
(1) 证书相关配置
SA remaining duration (kilobytes/sec): 1843199/3593
创建PKI域
Max sent sequence-number: 4
pki domain domain1
UDP encapsulation used for NAT traversal: N
public-key rsa signature name rsa1
Status: Active
undo crl check enable
[DeviceA]

创建PKI实体
pki entity entity1