S3500-EA系列交换机PKI实体向CA申请证书功能的配置（方式一）

岳斌 2008-09-03 发表

S3500-EA系列交换机PKI实体向CA申请证书功能的配置（方式一）

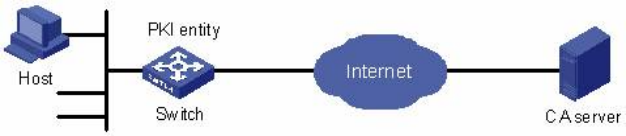
一、 组网需求：

在作为PKI实体的设备Switch上进行相关配置，实现以下需求：

（1）设备向CA服务器申请本地证书

（2）获取CRL为证书验证做准备

二、 组网图：



三、 配置步骤：

（1）CA服务器端的配置

1、创建CA服务器myca

在本例中，CA服务器上首先需要进行基本属性Nickname和Subject DN的配置。其它属性选择默认值。其中，Nickname为可信任的CA名称，Subject DN为CA的DN属性，包括CN、OU、O和C。

2、 配置扩展属性

基本属性配置完毕之后，还需要在生成的CA服务器管理页面上对“Jurisdiction Configuration”进行配置，主要内容包括：根据需要选择合适的扩展选项；启动自动颁发证书功能；添加可以自动颁发证书的地址范围。

3、配置CRL发布

CA服务器的基本配置完成之后，需要进行CRL的相关配置。

本例中选择CRL的发布方式为HTTP，自动生成CRL发布点的URL为http://4.4.4.133:447/myca.crl。

以上配置完成之后，还需要保证设备的系统时钟与CA的时钟同步才可以正常使用设备来申请证书和获取CRL。

（2）设备Switch上的配置

1、配置实体命名空间

配置实体名称为aaa，通用名为Switch。

<Switch> system-view

[Switch] pki entity aaa

[Switch-pki-entity-aaa] common-name Switch

[Switch-pki-entity-aaa] quit

2、配置PKI域参数

创建并进入PKI域torsa。

[Switch] pki domain torsa

配置可信任的CA名称为myca。

[Switch-pki-domain-torsa] ca identifier myca

配置注册服务器URL，格式为http://host:port/Issuing Jurisdiction ID。其中的Issuing Jurisdiction ID为CA服务器上生成的16进制字符串。

[Switch-pki-domain-torsa] certificate request url http://4.4.4.133:446/c95e970f632d27be5e8cbf80e971d9c4a9a93337

配置证书申请的注册受理机构为CA。

[Switch-pki-domain-torsa] certificate request from ca

指定实体名称为aaa。

[Switch-pki-domain-torsa] certificate request entity aaa

配置CRL发布点位置。

[Switch-pki-domain-torsa] crl url http://4.4.4.133:447/myca.crl

[Switch-pki-domain-torsa] quit

3、用RSA算法生成本地密钥对

[Switch] public-key local create rsa

The range of public key size is (512 ~ 2048).

NOTES: If the key modulus is greater than 512,

It may take a few minutes.

Press CTRL+C to abort.

Input the bits in the modulus [default = 1024]:

```
Generating keys...
........++++++
.....++++++++
.....++++++++
.
```

4、证书申请

获取CA证书并下载至本地。

```
[Switch] pki retrieval-certificate ca domain torsa
Retrieving CA/RA certificates. Please wait a while.....
The trusted CA's finger print is:
    MD5  fingerprint:EDE9 0394 A273 B61A F1B3 0072 A0B1 F9AB
    SHA1 fingerprint: 77F9 A077 2FB8 088C 550B A33C 2410 D354 23B2 73A8

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

Saving CA/RA certificates chain, please wait a moment.....
CA certificates retrieval success.
```

获取CRL并下载至本地。

```
[Switch] pki retrieval-crl domain torsa
Connecting to server for retrieving CRL. Please wait a while.....
CRL retrieval success!
```

手工申请本地证书。

```
[Switch] pki request-certificate domain torsa challenge-word
Certificate is being requested, please wait.....
Enrolling the local certificate,please wait a while.....
Certificate request Successfully!
Saving the local certificate to device.....
Done!
```

5、验证配置结果

通过以下显示命令可以查看获取的本地证书信息。

```
<Switch> display pki certificate local domain torsa
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            9A96A48F 9A509FD7 05FFF4DF 104AD094
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:
            C=cn
            O=org
            OU=test
            CN=myca
        Validity
            Not Before: Jan  8 09:26:53 2007 GMT
            Not After : Jan  8 09:26:53 2008 GMT
        Subject:
            CN=Switch
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00D67D50 41046F6A 43610335 CA6C4B11
                    F8F89138 E4E905BD 43953BA2 623A54C0
                    EA3CB6E0 B04649CE C9CDDD38 34015970
                    981E96D9 FF4F7B73 A5155649 E583AC61
                    D3A5C849 CBDE350D 2A1926B7 0AE5EF5E
                    D1D8B08A DBF16205 7C2A4011 05F11094
                    73EB0549 A65D9E74 0F2953F2 D4F0042F
                    19103439 3D4F9359 88FB59F3 8D4B2F6C
                    2B
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 CRL Distribution Points:
```

URI:http://4.4.4.133:447/myca.crl

Signature Algorithm: sha1WithRSAEncryption
836213A4 F2F74C1A 50F4100D B764D6CE
B30C0133 C4363F2F 73454D51 E9F95962
EDE9E590 E7458FA6 765A0D3F C4047BC2
9C391FF0 7383C4DF 9A0CCFA9 231428AF
987B029C C857AD96 E4C92441 9382E798
8FCC1E4A 3E598D81 96476875 E2F86C33
75B51661 B6556C5E 8F546E97 5197734B
C8C29AC7 E427C8E4 B9AAF5AA 80A75B3C

关于获取的CA证书及CRL文件的详细信息可以通过相应的显示命令来查看，此处略。具体内容请参考命令display pki certificate ca domain和display pki crl domain。

四、 配置关键点：

（1）当采用RSA Keon软件时，不需要安装SCEP插件。此时，配置PKI domain时，需要使用certificate request from ca命令指定实体从CA注册申请证书。

（2）若本地证书已存在，为保证密钥对与现存证书的一致性，不应执行创建密钥对命令，必须在删除本地证书后再执行public-key local create rsa命令生成新的密钥对。

（3）如果本地证书已存在，则不允许再执行证书申请操作，以避免因相关配置的修改使得证书与注册信息不匹配。若想重新申请，请先使用pki delete-certificate命令删除存储于本地的CA证书与本地证书，然后再执行pki request-certificate domain命令。

（4）当无法通过SCEP协议向CA在线申请证书时，可以使用可选参数pkcs10打印出本地的证书申请信息。用户保存证书申请信息，并将其通过带外方式发送给CA进行证书申请。

（5）证书申请之前必须保证实体时钟与CA的时钟同步，否则申请证书的有效期会出现异常。