MSR证书下载失败故障排查

证书 朱玉广 2015-08-12 发表

数字证书是一个经CA（Certificate Authority，证书颁发机构）签名的、包含公开密钥及相关的用户身份信息的文件，它建立了用户身份信息与用户公钥的关联。CA对数字证书的签名保证了证书的合法性和权威性。数字证书的格式遵循ITU-T X.509国际标准，目前最常用的为X.509 V3标准。一个数字证书中包含多个字段，包括证书签发者的名称、主体的公钥信息、CA对证书的数字签名、证书的有效期等。

而对于MSR中比较常使用的，比如说做IPsec证书加密，主要用到的为两种：本地（local）证书和CA（Certificate Authority）证书。本地证书是CA签发给用户的数字证书；CA证书是CA自身的证书。若PKI系统中存在多个CA，则会形成一个CA层次结构，最上层的CA是根CA，它拥有一个CA“自签名”的证书。

对于证书的一般有两种获取方式，一种是通过路由器从服务器上自动下载，另外一种就是将证书导出，然后在路由器上做本地导入。比较常见的证书问题也主要有本地导入失败，路由器下载证书失败等。

1、南方某银行网点客户使用MSR2600设备做基于证书的IPsec，但是部分网点证书一直获取失败，排查过配置和系统时间，确认无异常，且有部分网点可以正常获取到证书。

收集debug信息，报错如下：

*Jul 23 01:54:07:030 2015 QZ-SQ-YDJR-A-001 PKI/7/PKI_Debug: SCEP send message:IP = 0xa0cc80b

*Jul 23 01:54:07:180 2015 QZ-SQ-YDJR-A-001 PKI/7/PKI_Debug: SCEP receive message: Server returned status code 500

*Jul 23 01:54:07:280 2015 QZ-SQ-YDJR-A-001 PKI/7/PKI_Debug: SCEP receive message: wrong MIME content type

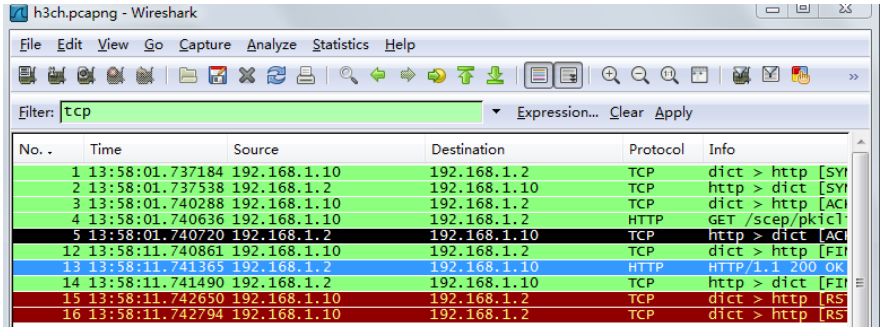
*Jul 23 01:54:07:381 2015 QZ-SQ-YDJR-A-001 PKI/7/PKI_Debug: Error while sending scep message

*Jul 23 01:54:07:481 2015 QZ-SQ-YDJR-A-001 PKI/7/PKI_Debug: SCEP certificate enroll: Failed to request certificate, error code is 95.

2、西北某银行客户网点使用MSR201X作为网点路由器，做基于证书的IPsec，从服务器侧看，证书已经发送给设备，但是设备依旧获取证书失败。

通过抓包来看，在设备发出证书请求之后，证书服务器回复了200 OK 消息，并将证书发了出来，但是设备侧依旧报错。

通过抓包可以看到信息如下：



1、南方某银行网点客户的证书问题，通过收集的debug信息来看，我司侧发出证书请求不久，就收到了CA服务器侧发送过来的500 Error报文。由此可以看出CA服务器内部存在异常。

2、西北某银行客户的证书问题，通过仔细观察抓包可以发现，MSR发出get请求后，过了10秒后才收到CA服务器的响应，而在10秒时，设备侧已经超时挂断，所以导致证书获取失败。

1、南方某银行网点客户的证书问题，经排查，确认是CA服务器突然出现异常，调整CA服务器之后，问题解决。

2、西北某银行客户的证书问题，为CA服务器响应过慢导致，也属于设备与CA服务器之间的兼容性问题，为了更好的兼容不同服务器，防止CA服务器响应过慢，导致设备挂断，设备侧从R2512P11版本开始，修改了接收接收时长，以兼容不同的CA服务器。升级版本，问题解决。当然此问题，也可以通过本地导入证书的方式解决。