

### 组网及说明

无

### 问题描述

证书来源：**缺失证书**

状态：**错误：服务器缺少中间证书**

SecPath L1000-AK310(V7) 做入方向负载均衡，SSL证书导入失败。转换证书格式后成功导入证书，但是打开网页后用检测工具检测，显示服务器缺少中间证书，网页可以打开。

### 过程分析

1、由于设备类型和不同的服务器以及服务器的版本，需要用到不同的证书格式，转换证书格式并不会导致证书链缺失。

- .DER .CER，文件是二进制格式，只保存证书，不保存私钥。
- .PEM，一般是文本格式，可保存证书，可保存私钥。
- .CRT，可以是二进制格式，可以是文本格式，与 .DER 格式相同，不保存私钥。
- .PFX .P12，二进制格式，同时包含证书和私钥，一般有密码保护。
- .JKS，二进制格式，同时包含证书和私钥，一般有密码保护。

#转换工具可以去网上搜索。

2、导入的CA证书和Local证书需要合并，之后再发送服务器，可能是合成过程中部分证书链缺失。

证书安装流程如下：**(具体操作流程见附件)**

- (1) 设备上新建PKI域；
- (2) 在PKI域中安装CA证书和本地证书。
  - 对于不完整的证书链CA证书，需要分离出根CA。先安装根CA，最后安装子级CA。
  - 对于非证书链CA证书以及完整的证书链CA证书可以直接安装。
  - 对于无保护密码及私钥的本地证书，需要将key文件的密钥部分复制并粘贴至本地证书中安装。
  - 对于有保护密码及私钥的本地证书，安装本地证书时输入证书口令。
  - 对于有保护密码无私钥的本地证书，需要将key文件的密钥部分复制并粘贴至本地证书中，安装本地证书时需要输入证书口令。

3、重新合并证书后需要重新使能服务，并开启发送完整证书链功能。

(1) 修改完ssl-server-policy后所有引用ssl-server的虚服务都需要重新使能。**重新使能会导致业务中断，需要申请窗口时间。**

#

```
virtual-server XXXX type http
undo service enable
service enable
```

#

(2) 开启发送完整证书链功能

#

```
ssl server-policy policy1
certificate-chain-sending enable
```

#

**缺省情况下SSL协商时，SSL服务器端只发送本地证书，不发送证书链。**

### 解决方法

重新导入并合成证书，开启发送完整证书功能后重新使能虚服务，证书状态正常。

证书来源：**服务器返回的证书**

状态：**正常**

