排除故障SSL的VPN证书问题与CME

目录

简介

本文描述方法排除故障IP电话注册对通信管理器Express (CME)通过安全套接字协议层(SSL) VPN。

先决条件

要求

思科建议有安全证书、数据包捕获工具的您和通信管理器Express基本的了解。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 通信管理器Express版本8.6
- 思科7965 IP电话版本8.5.3

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

排除故障证书问题

有设置在一个IP电话在互联网和CME之间的SSL的两个方法VPN在公司网络里面。

- CME是在作为VPN头端的思科可适应安全工具(ASA)后。在此方案中， CME和ASA共享同一证书，并且IP电话协商与ASA的安全设置。

• CME直接地连接到互联网，并且作为VPN头端。它协商安全设置用直接IP电话。

在两种情况下，设立在一个IP电话在互联网和CME之间的SSL VPN包括相似的步骤：

1. CME生成或获取安全证书。
2. CME “推送”证书的哈希在Base64格式的到电话通过电话从CME下载通过TFTP的配置文件。
3. IP电话设法登陆与VPN头端并且通过传输层安全(TLS)协议接收证书。
4. IP电话解压缩从证书的哈希并且它与从CME下载前的哈希比较。如果哈希配比，则电话委托VPN头端并且继续进行进一步VPN协商。

验证

为了验证CME推送哈希到IP电话，请检查为安全电话生成的配置文件。为了简化此步骤，您在flash:能配置CME生成一个配置文件每个电话和存储它

```
R009-3945-1(config-telephony)#cnf-file perphone
R009-3945-1(config-telephony)#cnf-file location flash:
```

为了保证新的配置生成，推荐重建配置文件：

```
R009-3945-1(config-telephony)#no create cnf-files
CNF files deleted
R009-3945-1(config-telephony)#create cnf-file
Creating CNF files
```

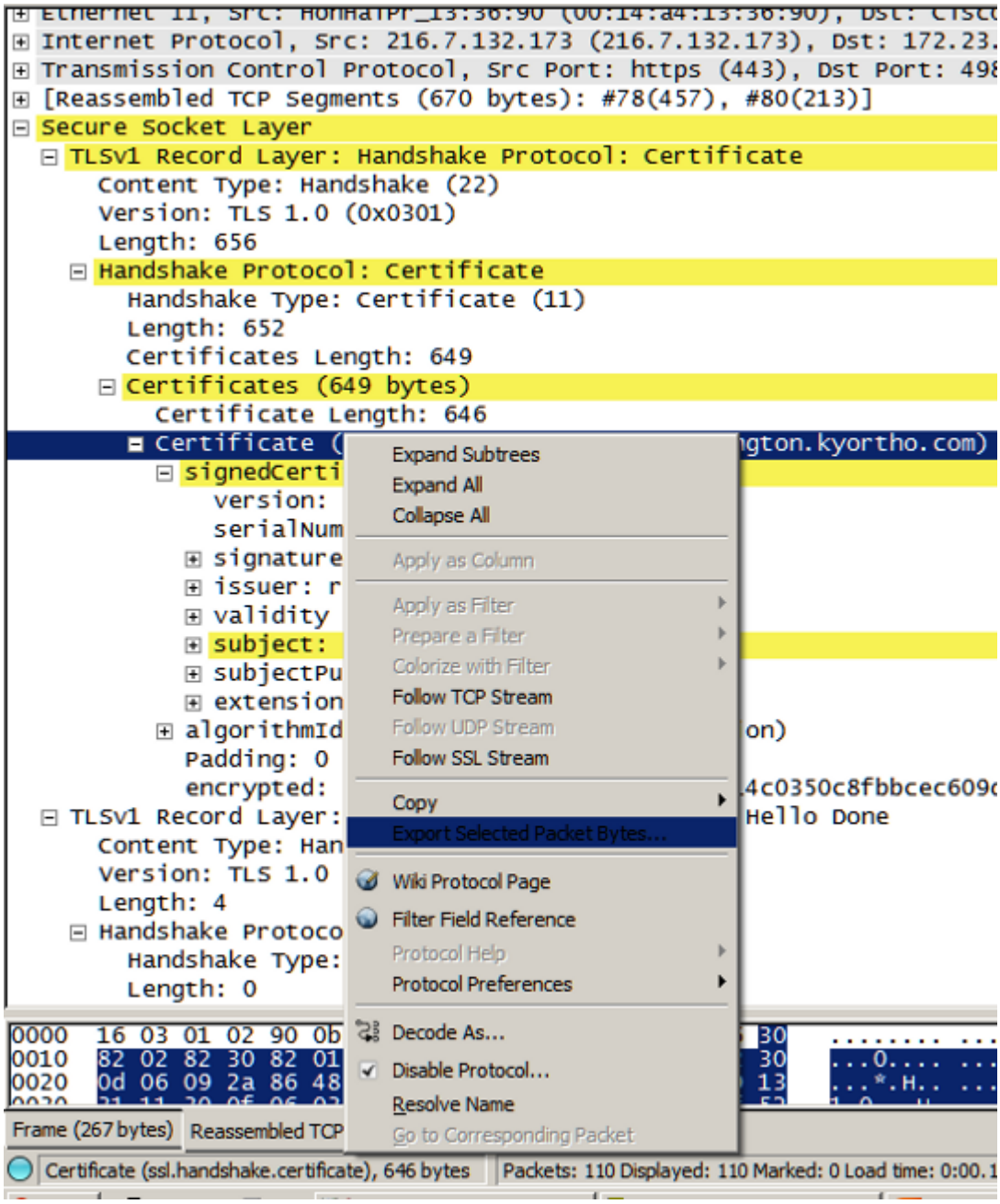
在闪存显示的对应的配置文件(有VPN组的ephone配置)后，您应该在文件目录的末端附近看到此：

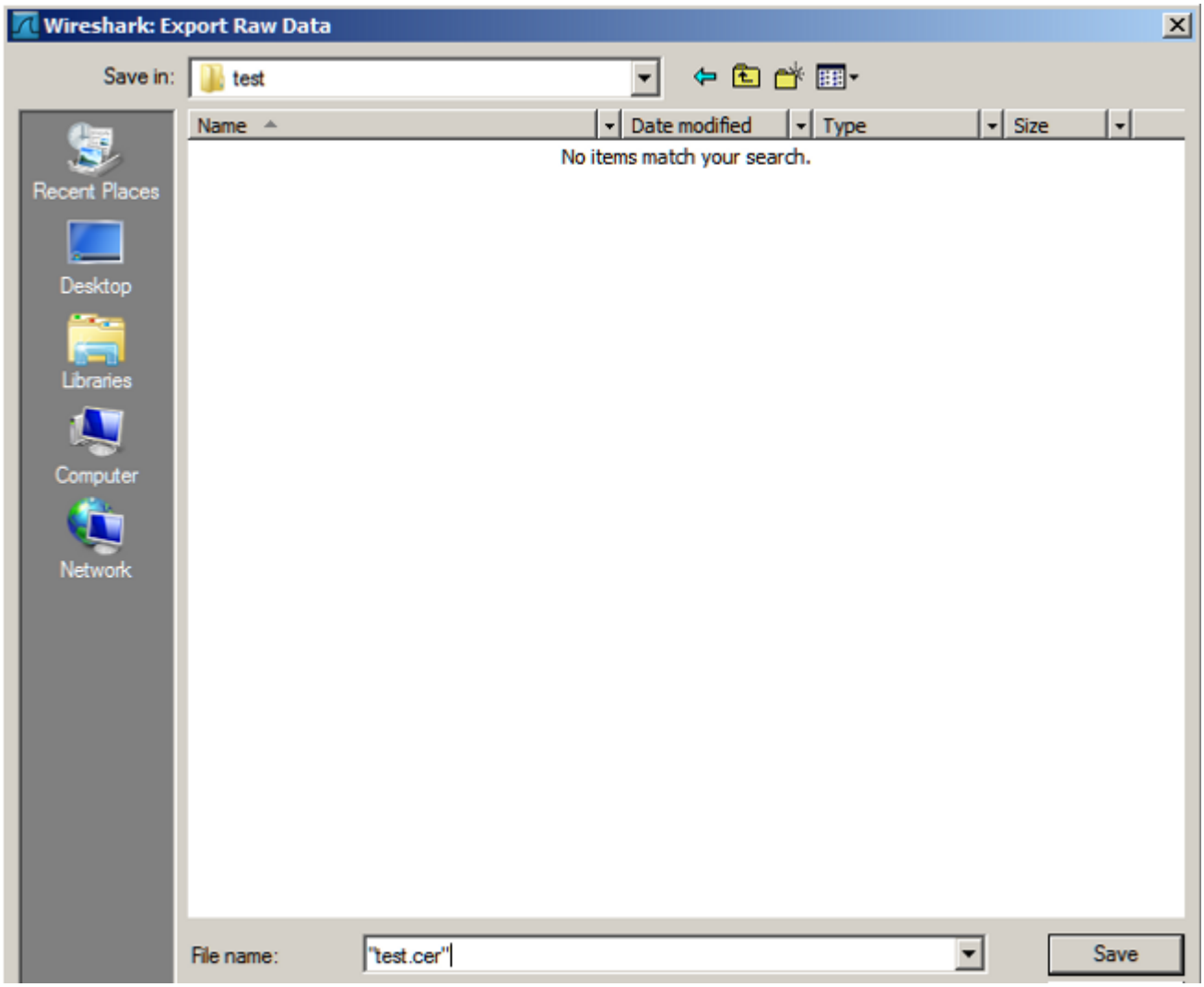
```
<vpnGroup>  <enableHostIDCheck>0</enableHostIDCheck>
<addresses>
<url1>https://10.201.160.201/SSLVPNphone</url1>
</addresses>
<credentials>
<hashAlg>0</hashAlg>
<certHash1>fZ2xQHMBcWj/fSoNs5IkPbA2Pt8=</certHash1>
</credentials>
</vpnGroup>
```

certHash1值是证书的哈希。在TLS设置期间时，当IP电话接收从VPN头端的证书，盼望证书的哈希同存储的Hash值一样。如果IP电话投掷“Bad证书”错误，可能是Hash值不配比。

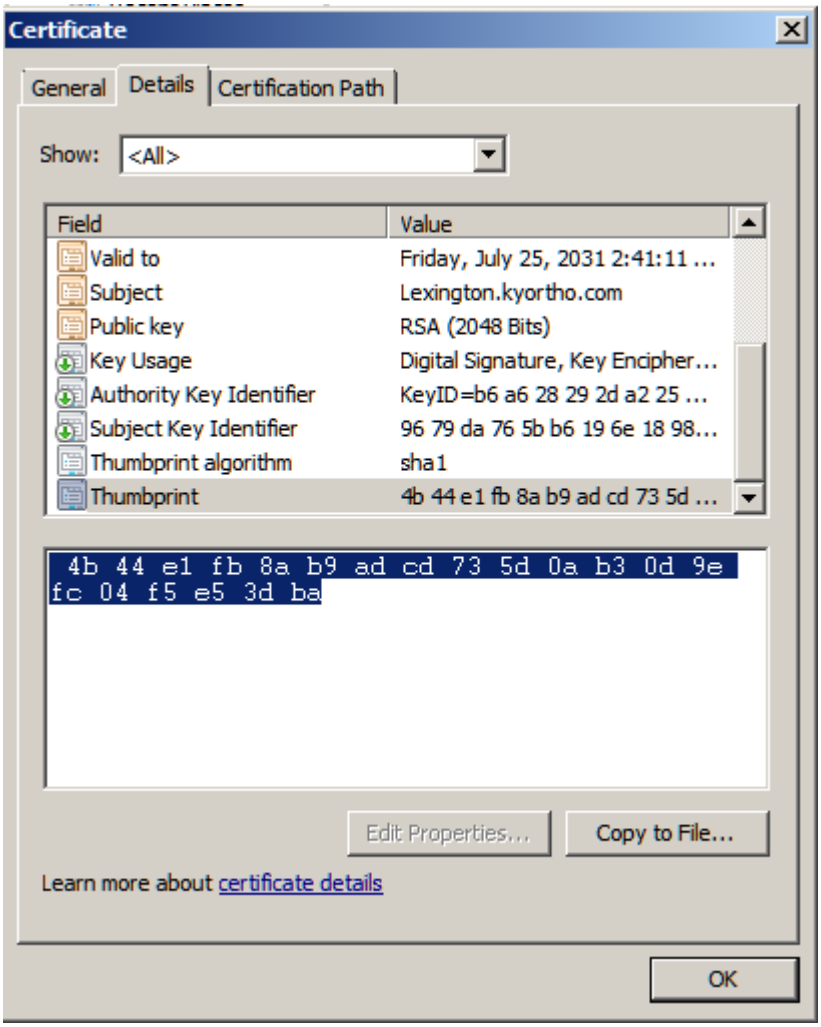
为了验证，请遵从这些步骤解压缩从数据包捕获的Hash值收集在IP电话和VPN头端之间：

1. 找出从包含证书的VPN数据转发设备的数据包到IP电话。它典型地在TLS服务器问候数据包。
2. 展开数据包内容并且找出报头：
   安全套接层> TLS V1记录层>握手协议：证书>证书>证书。
3. 用鼠标右键单击证书报头并且导出值到.CER文件


Ethernet II, Src: HonHaiPr_13:36:90 (00:14:a4:13:36:90), Dst: Cisco
Internet Protocol, Src: 216.7.132.173 (216.7.132.173), Dst: 172.23.
Transmission Control Protocol, Src Port: https (443), Dst Port: 498
[Reassembled TCP Segments (670 bytes): #78(457), #80(213)]
Secure Socket Layer
TLSv1 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 656
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 652
Certificates Length: 649
Certificates (649 bytes)
Certificate Length: 646
Certificate (
gton.kyortho.com)
signedCerti
version:
serialNum
signature
issuer: r
validity
subject:
subjectPu
extension
algorithmId
on)
Padding: 0
encrypted:
4c0350c8fbbcec609c
TLSv1 Record Layer:
Hello Done
Content Type: Han
Version: TLS 1.0
Length: 4
Handshake Protoco
Handshake Type:
Length: 0
Expand Subtrees
Expand All
Collapse All
Apply as Column
Apply as Filter
Prepare a Filter
Colorize with Filter
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Export Selected Packet Bytes...
Wiki Protocol Page
Filter Field Reference
Protocol Help
Protocol Preferences
Decode As...
Disable Protocol...
Resolve Name
Go to Corresponding Packet
0000 16 03 01 02 90 0b
0010 82 02 82 30 82 01
0020 0d 06 09 2a 86 48
Frame (267 bytes)
Reassembled TCP
Certificate (ssl.handshake.certificate), 646 bytes
Packets: 110 Displayed: 110 Marked: 0 Load time: 0:00.1
:



4. 打开.CER文件，去详细信息选项卡，选择Thumbprint，并且选择值。值是在六角形的格式的



哈希：

5. 其次，使用所有联机Hex-to-Base64转换工具，您转换哈希从十六进制到Base64。已转换值可以与在IP电话的配置文件的Hash值比较，如果他们不配比，然后含义IP电话接收的哈希是从不同的身份验证比VPN头端使用什么SSL。

相关信息

- 配置SCCP IP电话的SSL VPN客户端
- 技术支持和文档 - Cisco Systems

>