Dépannage des problèmes de certificat pour VPN SSL avec CME

Contenu

Introduction

Ce document décrit la méthodologie utilisée pour dépanner l'enregistrement des téléphones IP vers Communications Manager Express (CME) via VPN SSL (Secure Sockets Layer).

Conditions préalables

Conditions requises

Cisco recommande que vous ayez une compréhension de base des certificats de sécurité, de l'outil de capture de paquets et de Communications Manager Express.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Communications Manager Express version 8.6
- Téléphone IP Cisco 7965 version 8.5.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Dépannage des problèmes de certificat

Il existe deux méthodes pour configurer le VPN SSL entre un téléphone IP sur Internet et CME dans le réseau de l'entreprise.

- Le CME est derrière un dispositif de sécurité adaptatif (ASA) de Cisco qui fait office de tête de réseau VPN. Dans ce scénario, CME et l'ASA partagent le même certificat et le téléphone IP négocie la configuration de sécurité avec l'ASA.
- Le CME est directement connecté à Internet et fait office de tête de réseau VPN. Il négocie directement la configuration de sécurité avec le téléphone IP.

Dans les deux scénarios, l'établissement d'un VPN SSL entre un téléphone IP sur Internet et le CME se compose d'étapes similaires :

1. Le CME génère ou obtient un certificat de sécurité.
2. Le CME « pousse » le hachage du certificat au format Base64 vers le téléphone via le fichier de configuration que le téléphone télécharge à partir de CME via TFTP.
3. Le téléphone IP tente de se connecter avec la tête de réseau VPN et reçoit le certificat via le protocole TLS (Transport Layer Security).
4. Le téléphone IP extrait le hachage du certificat et le compare au hachage qu'il a téléchargé précédemment à partir de CME. Si le hachage correspond, le téléphone fait confiance à la tête de réseau VPN et poursuit la négociation VPN.

Vérification

Afin de vérifier que le CME a poussé le hachage sur le téléphone IP, vérifiez le fichier de configuration qu'il a généré pour le téléphone sécurisé. Afin de simplifier cette étape, vous pouvez configurer le CME pour générer un fichier de configuration par téléphone et le stocker dans la mémoire Flash :

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

Afin de s'assurer que la nouvelle configuration est générée, il est recommandé de recréer les fichiers de configuration :

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

Une fois le fichier de configuration correspondant affiché dans la mémoire Flash (pour un ephone avec groupe VPN configuré), vous devriez voir ceci près de la fin du contenu du fichier :

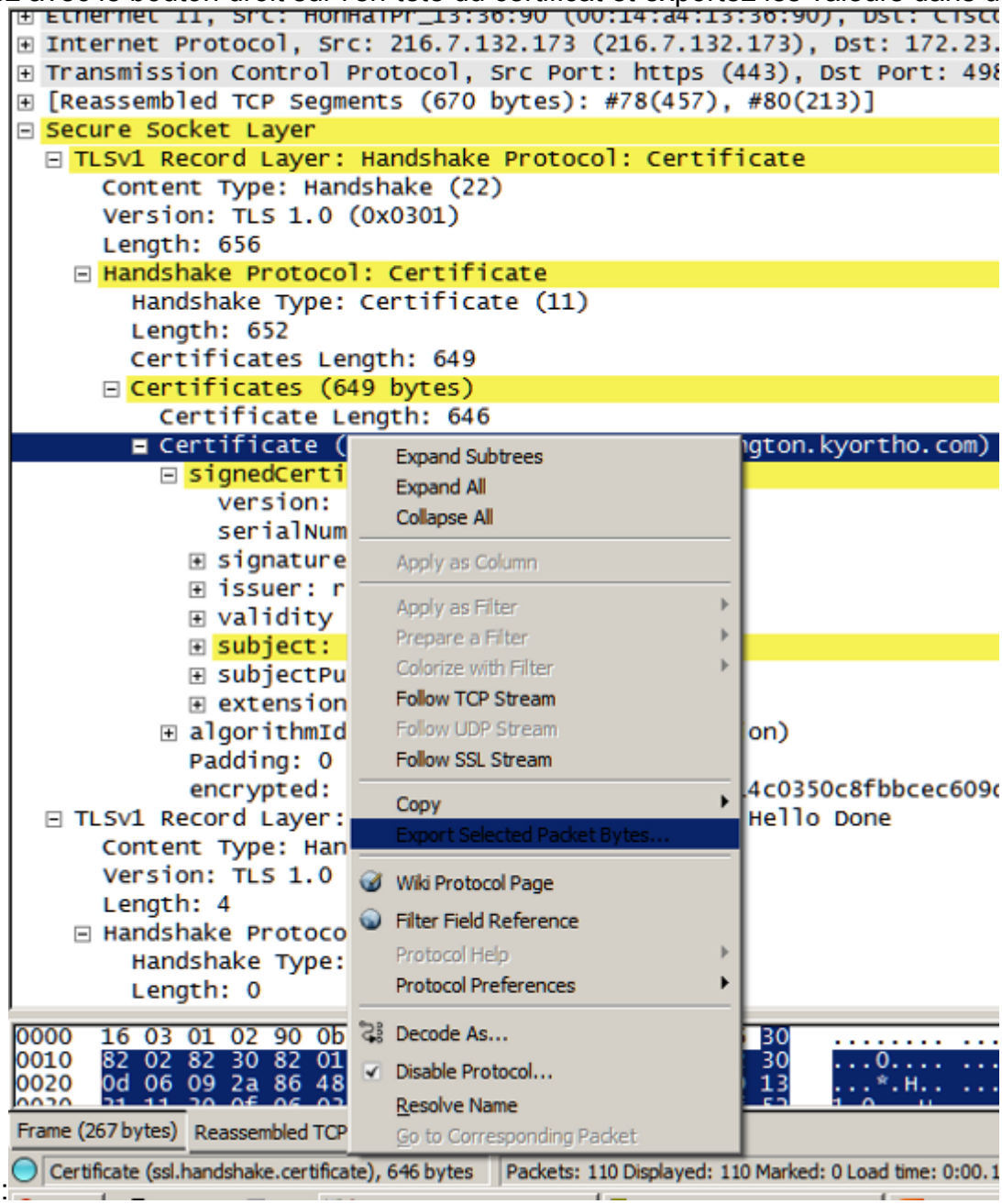
```
<vpnGroup>  <enableHostIDCheck>0</enableHostIDCheck>
<addresses>
<url1>https://10.201.160.201/SSLVPNphone</url1>
</addresses>
<credentials>
<hashAlg>0</hashAlg>
<certHash1>fZ2xQHMBcWj/fSoNs5IkPbA2Pt8=</certHash1>
</credentials>
</vpnGroup>
```

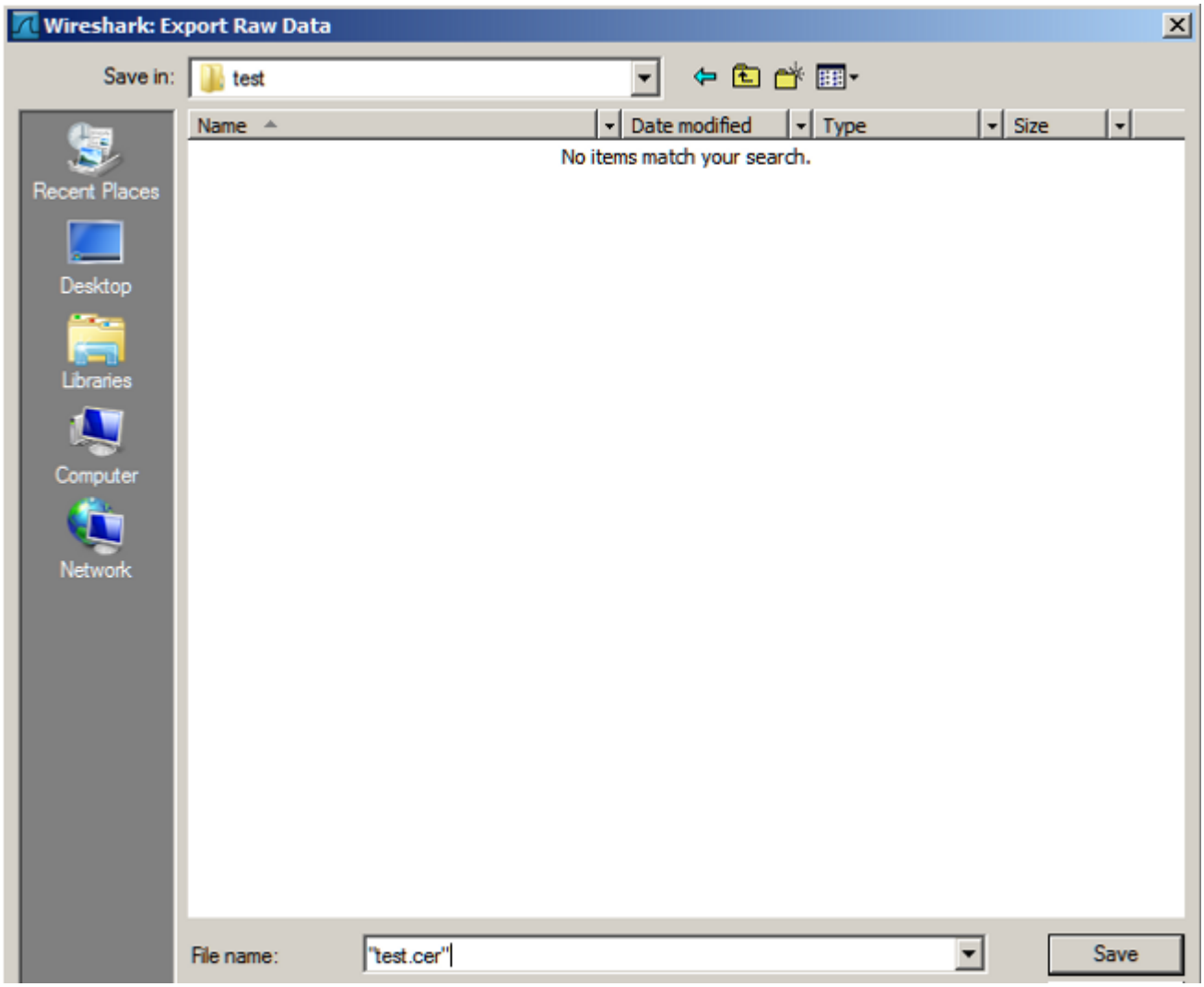
La valeur **certHash1** est le hachage du certificat. Lorsque le téléphone IP reçoit le certificat de VPN Headend lors de la configuration de TLS, il s'attend à ce que le hachage du certificat soit

identique à la valeur de hachage stockée. Si le téléphone IP émet une erreur « Mauvais certificat », il se peut que les valeurs de hachage ne correspondent pas.

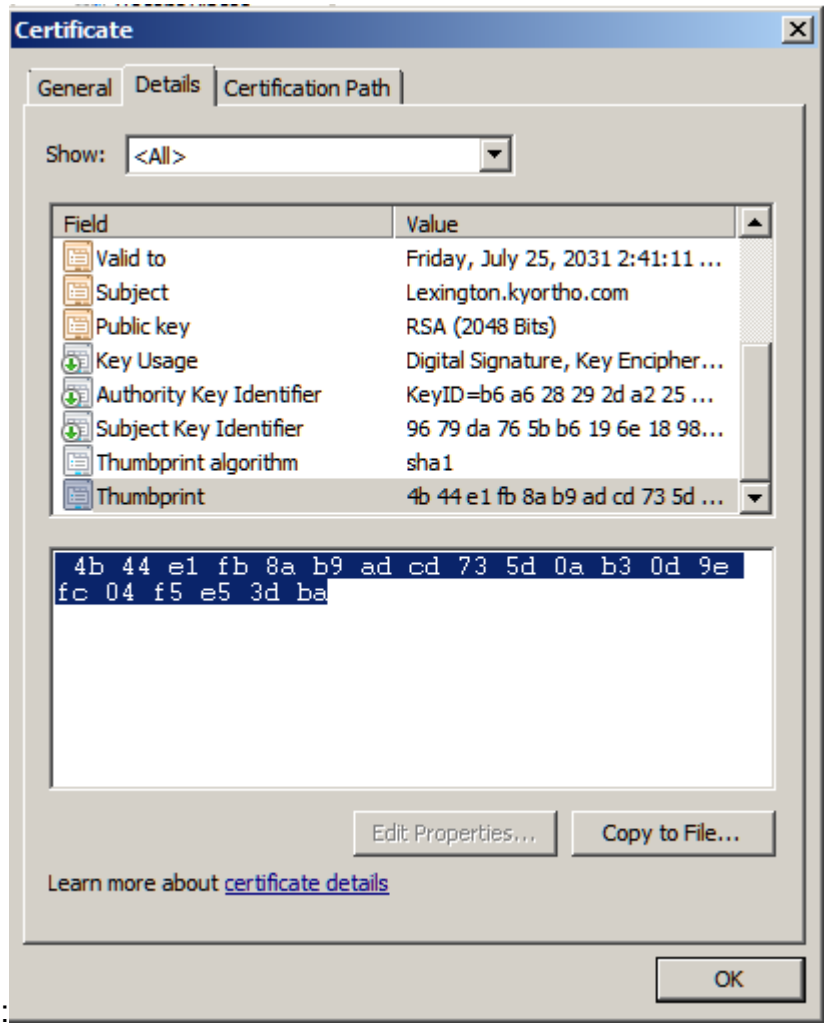
Afin de vérifier, suivez ces étapes pour extraire la valeur de hachage de la capture de paquets collectée entre le téléphone IP et la tête de réseau VPN :

1. Localisez le paquet du périphérique de tête de réseau VPN vers le téléphone IP qui contient le certificat. Il se trouve généralement dans le paquet Hello du serveur TLS.
2. Développez le contenu du paquet et localisez l'en-tête :
   Secure Socket Layer > TLS V1 Record Layer > Handshake Protocol : Certificat > Certificats > Certificat.
3. Cliquez avec le bouton droit sur l'en-tête du certificat et exportez les valeurs dans un fichier .CER :





4. Ouvrez le fichier .CER, accédez à l'onglet Détails, choisissez Empreinte numérique et choisissez les valeurs. Les valeurs sont le hachage au format hexadécimal



:

5. Ensuite, vous convertissez le hachage hexadécimal en Base64 à l'aide de n'importe quel outil de conversion hexadécimal vers Base64 en ligne. La valeur convertie peut être comparée à la valeur de hachage dans le fichier de configuration du téléphone IP si elle ne correspond pas, alors cela signifie que le hachage reçu par le téléphone IP provient d'un certificat différent de celui utilisé par la tête de réseau VPN pour SSL.

Informations connexes

- Configuration du client VPN SSL pour les téléphones IP SCCP
- Support et documentation techniques - Cisco Systems

>