Dépannez les questions de certificat pour le VPN SSL avec CME

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Dépannez les questions de certificat](#)
[Vérifiez](#)
[Informations connexes](#)

Introduction

Ce document décrit la méthodologie pour dépanner l'enregistrement de téléphone IP à la Communication Manager Express (CME) par l'intermédiaire de Secure Sockets Layer (SSL) VPN.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez une compréhension de base des Certificats de Sécurité, le paquet capturant l'outil, et la Communication Manager Express.

Composants utilisés

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

- Version 8.6 de Communication Manager Express
- Version 8.5.3 de téléphone IP de Cisco 7965

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Dépannez les questions de certificat

Il y a deux méthodes pour installer le VPN SSL entre un téléphone IP sur l'Internet et CME à l'intérieur du réseau d'entreprise.

- CME est derrière une appliance de sécurité adaptable Cisco (ASA) qui agit en tant que Headend VPN. Dans ce scénario, CME et l'ASA partagent le même certificat et le téléphone IP est en pourparlers la configuration de la sécurité avec l'ASA.
- CME est connecté à l'Internet directement, et agit en tant que Headend VPN. Il est en pourparlers la configuration de la sécurité avec le téléphone IP directement.

Dans les deux scénarios, l'établissement du VPN SSL entre un téléphone IP sur l'Internet et CME se compose des étapes semblables :

1. CME génère ou obtient un Security Certificate.
2. CME « pousse » les informations parasites du certificat dans le format Base64 au téléphone par l'intermédiaire du fichier de config que le téléphone télécharge de CME par l'intermédiaire du TFTP.
3. Les essais de téléphone IP à ouvrir une session avec le Headend VPN et reçoit le certificat par l'intermédiaire du protocole de Transport Layer Security (TLS).
4. Le téléphone IP extrait les informations parasites du certificat et les compare aux informations parasites qu'elles ont téléchargées de CME plus tôt. Si les informations parasites s'assortissent, alors le téléphone fait confiance au Headend VPN et se poursuit par davantage de négociation VPN.

Vérifiez

Afin de vérifier que CME a poussé les informations parasites au téléphone IP, vérifiez le fichier de configuration qu'il a généré pour le téléphone sécurisé. Afin de simplifier cette étape, vous pouvez configurer CME pour générer un fichier de configuration par téléphone et pour l'enregistrer dans l'éclair :

```
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 pour 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
```

Après que le fichier de configuration correspondant dans les affichages d'instantané (pour un ephone avec le VPN-groupe configuré), vous devrait voir ceci près de l'extrémité du contenu du fichier :

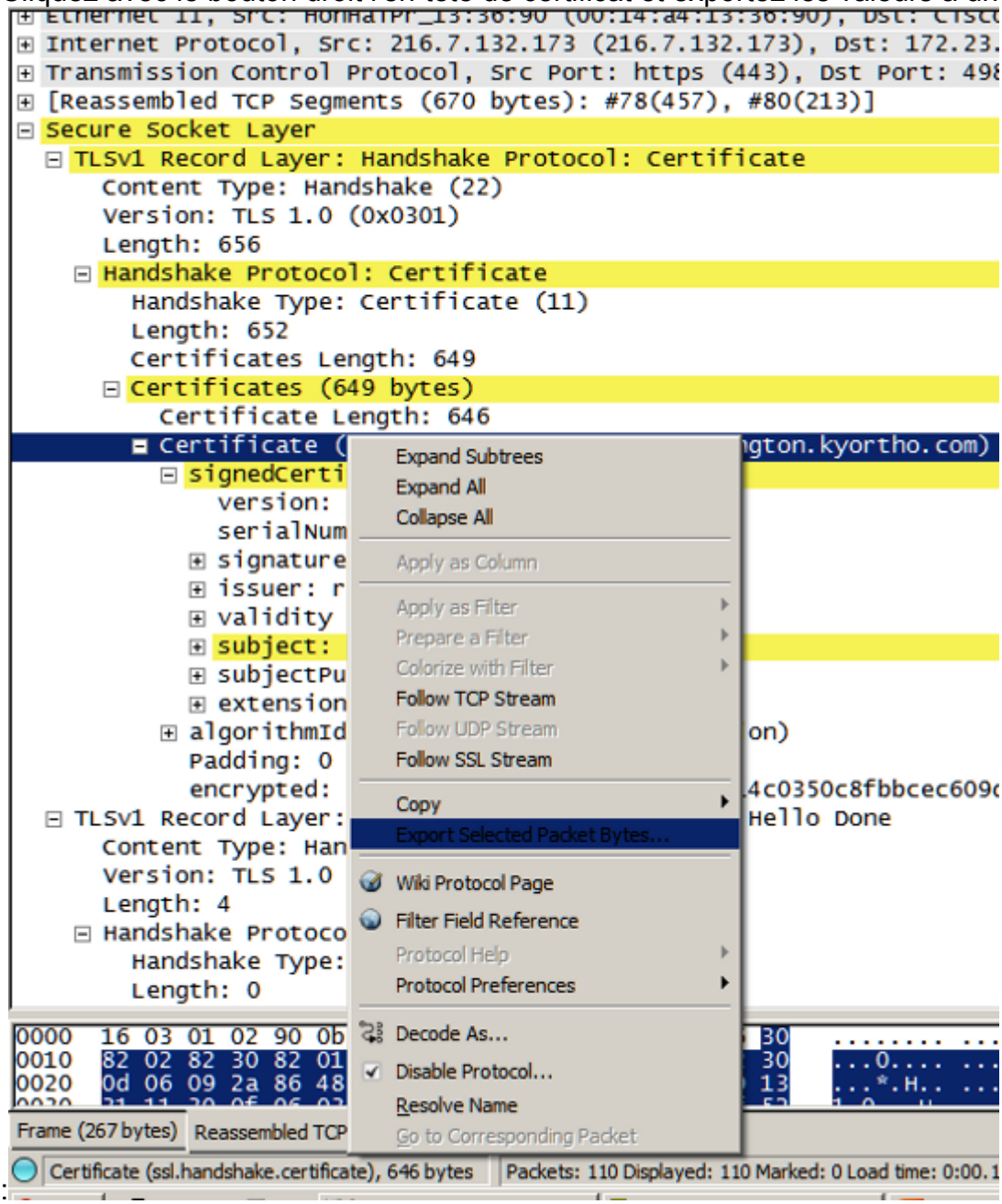
```
<vpnGroup>  <enableHostIDCheck>0</enableHostIDCheck>
<addresses>
<url1>https://10.201.160.201/SSLVPNphone</url1>
</addresses>
<credentials>
<hashAlg>0</hashAlg>
<certHash1>fZ2xQHMBcWj/fSoNs5IkPbA2Pt8=</certHash1>
</credentials>
</vpnGroup>
```

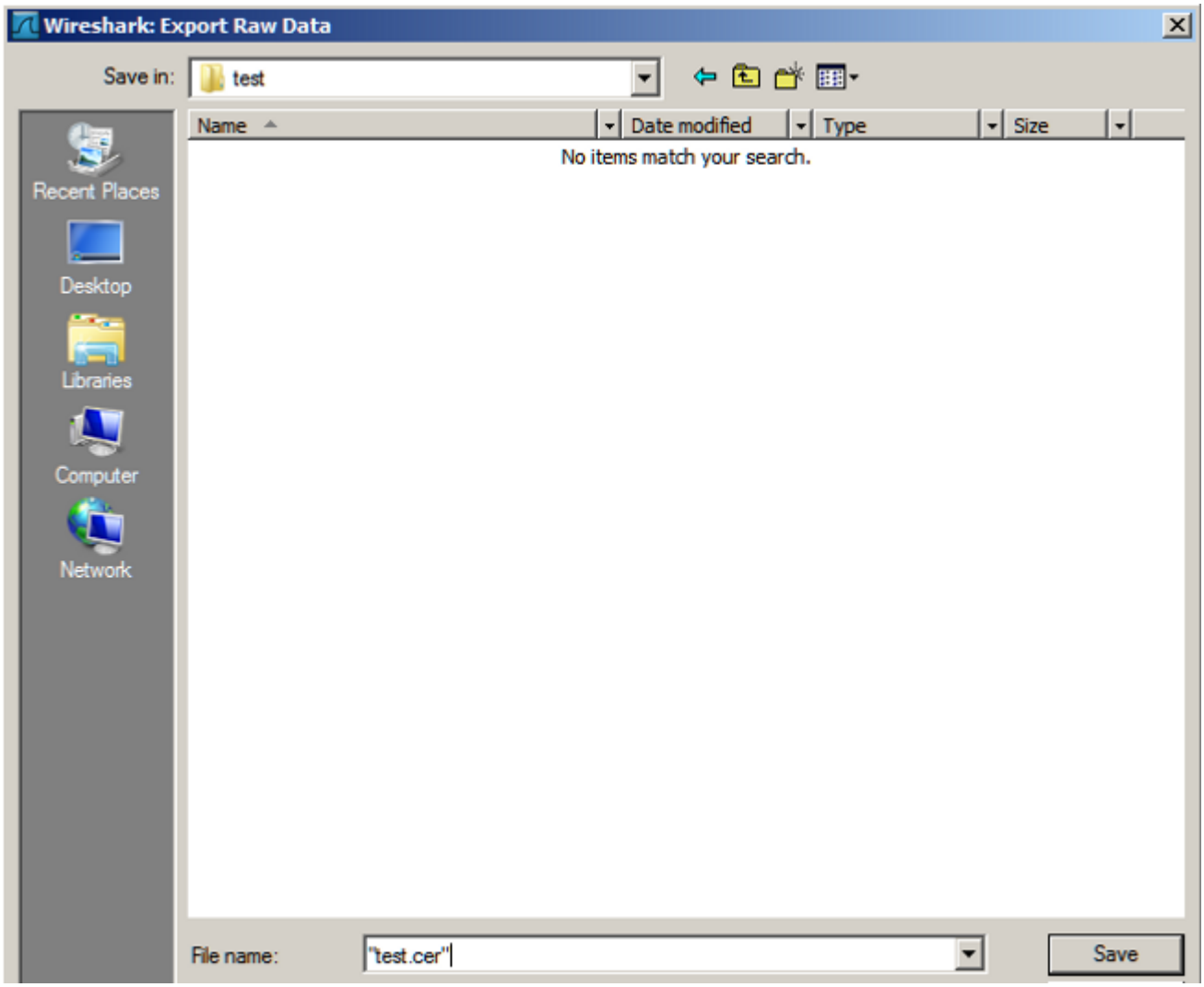
La valeur **certHash1** est les informations parasites du certificat. Quand le téléphone IP reçoit le certificat du Headend VPN pendant l'installation de TLS, elle s'attend à ce que les informations

parasites du certificat correspondent la valeur de hachage enregistrée. Si le téléphone IP jette une erreur de « mauvais certificat », il pourrait être que les valeurs de hachage ne s'assortissent pas.

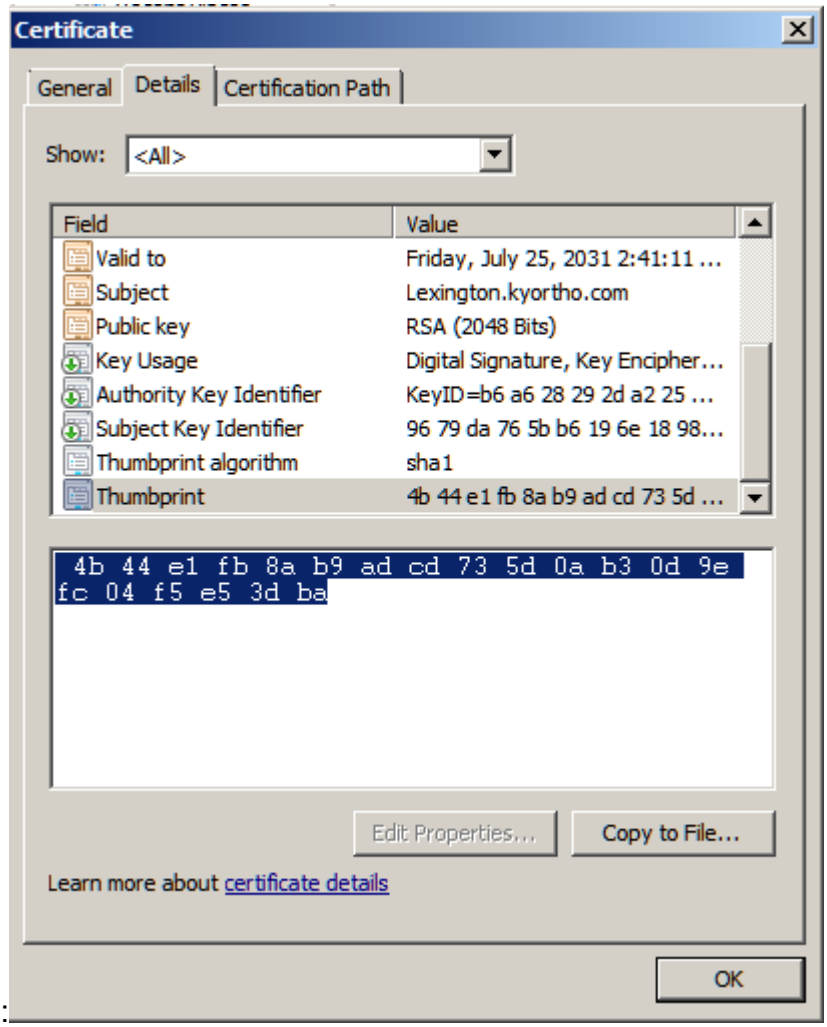
Afin de vérifier, suivez ces étapes pour extraire la valeur de hachage de la capture de paquet collectée entre le téléphone IP et le Headend VPN :

1. Localisez le paquet du périphérique de Headend VPN au téléphone IP qui contient le certificat. Il est typiquement dans le paquet de serveur de TLS bonjour.
2. Développez le contenu de paquet et localisez l'en-tête :
   Secure Socket Layer > couche > protocole handshake d'enregistrement du TLS V1 : Certificat > Certificats > certificat.
3. Cliquez avec le bouton droit l'en-tête de certificat et exportez les valeurs à un fichier .CER





4. Ouvrez le fichier .CER, allez aux détails l'onglet, choisissez Thumbprint, et choisissez les valeurs. Les valeurs sont les informations parasites dans le format hexadécimal



:

5. Ensuite, vous convertissez les informations parasites de l'hexa en Base64 utilisant n'importe quel outil en ligne de la conversion Hex-to-Base64. La valeur convertie peut être comparée à la valeur de hachage dans le fichier de configuration du téléphone IP s'ils ne s'assortissent pas, alors il signifie que les informations parasites reçues par le téléphone IP sont d'un certificat différent que ce qui est utilisé par le Headend VPN pour le SSL.

Informations connexes

- Configurer le client de VPN SSL pour des Téléphones IP de SCCP
- Support et documentation techniques - Cisco Systems

>