Problemas del certificado del Troubleshooting para SSL VPN con el CME

Contenido

Introducción

Este documento describe la metodología para resolver problemas el registro del teléfono del IP al administrador de comunicaciones expreso (CME) vía Secure Sockets Layer (SSL) VPN.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene una comprensión básica de los Certificados de la Seguridad, el paquete que captura la herramienta, y al administrador de comunicaciones expreso.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión expresa 8.6 del administrador de comunicaciones
- Versión 8.5.3 del teléfono del IP de Cisco 7965

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Resuelva problemas los problemas del certificado

Hay dos métodos para configurar SSL VPN entre un teléfono del IP en Internet y el CME dentro de la red corporativa.

- El CME está detrás de un dispositivo de seguridad adaptante de Cisco (ASA) que actúe como la cabecera VPN. En este escenario, el CME y el ASA comparten el mismo certificado y el teléfono del IP negocia la configuración de seguridad con el ASA.
- El CME está conectado con Internet directamente, y actúa como la cabecera VPN. Negocia la configuración de seguridad con el teléfono del IP directamente.

En ambos escenarios, el establecimiento de SSL VPN entre un teléfono del IP en Internet y el CME consiste en los pasos similares:

1. El CME genera u obtiene un Security Certificate.
2. El CME “avanza” el hash del certificado en el formato del base64 al teléfono vía el archivo de configuración que el teléfono descarga del CME vía el TFTP.
3. El teléfono del IP intenta iniciar sesión con la cabecera VPN y recibe el certificado vía el protocolo de Transport Layer Security (TLS).
4. El teléfono del IP extrae el hash del certificado y lo compara con el hash que descargó del CME anterior. Si el hash hace juego, después el teléfono confía en la cabecera VPN y procede con la negociación adicional VPN.

Verificación

Para verificar que el CME haya avanzado el hash al teléfono del IP, marque el archivo de configuración que generó para el teléfono seguro. Para simplificar este paso, usted puede configurar el CME para generar un archivo de configuración por el teléfono y para salvarlo en el flash:

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

Para asegurarse de que la nueva configuración esté generada, se recomienda para reconstruir los archivos de configuración:

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

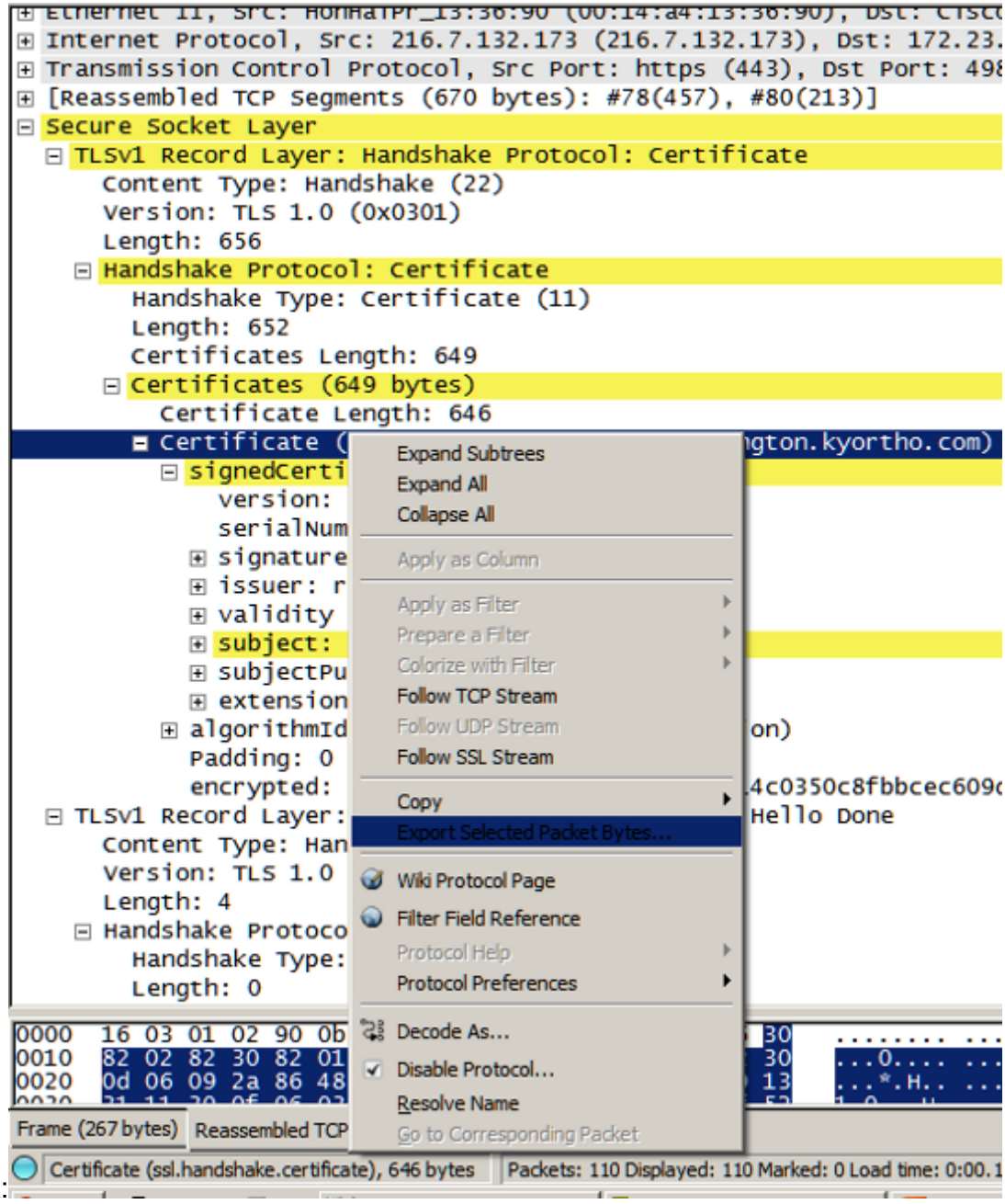
Después de que el archivo de configuración correspondiente en las visualizaciones del flash (para un ephone con el VPN-grupo configurado), usted deba considerar esto cerca del extremo del contenido del archivo:

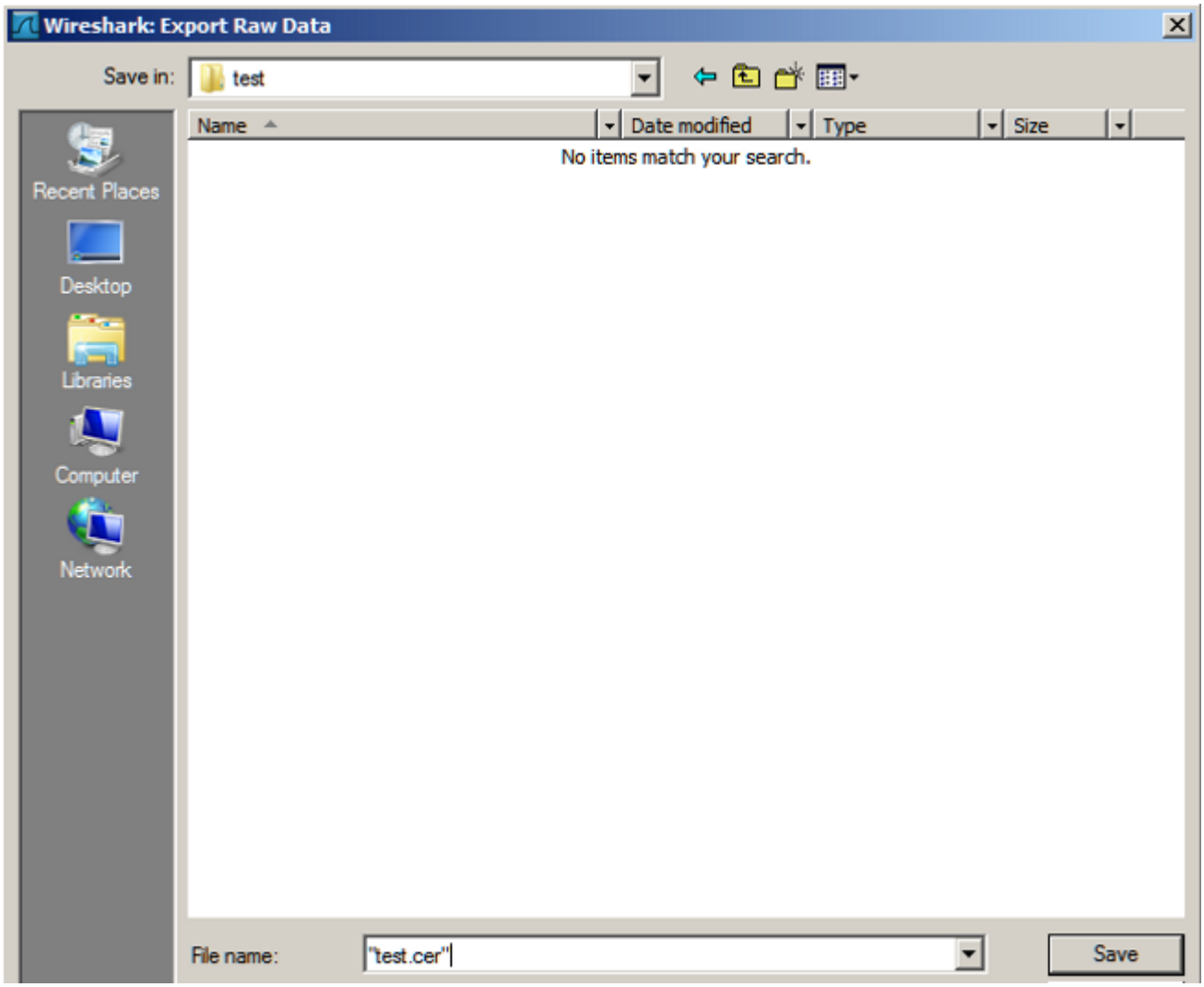
```
<vpnGroup>  <enableHostIDCheck>0</enableHostIDCheck>
<addresses>
<url1>https://10.201.160.201/SSLVPNphone</url1>
</addresses>
<credentials>
<hashAlg>0</hashAlg>
<certHash1>fZ2xQHMBcWj/fSoNs5IkPbA2Pt8=</certHash1>
</credentials>
</vpnGroup>
```

El valor **certHash1** es el hash del certificado. Cuando el teléfono del IP recibe el certificado de la cabecera VPN durante la configuración de TLS, espera que el hash del certificado sea lo mismo que el valor de troceo salvado. Si el teléfono del IP lanza un error del “mún certificado”, podría ser que los valores de troceo no hacen juego.

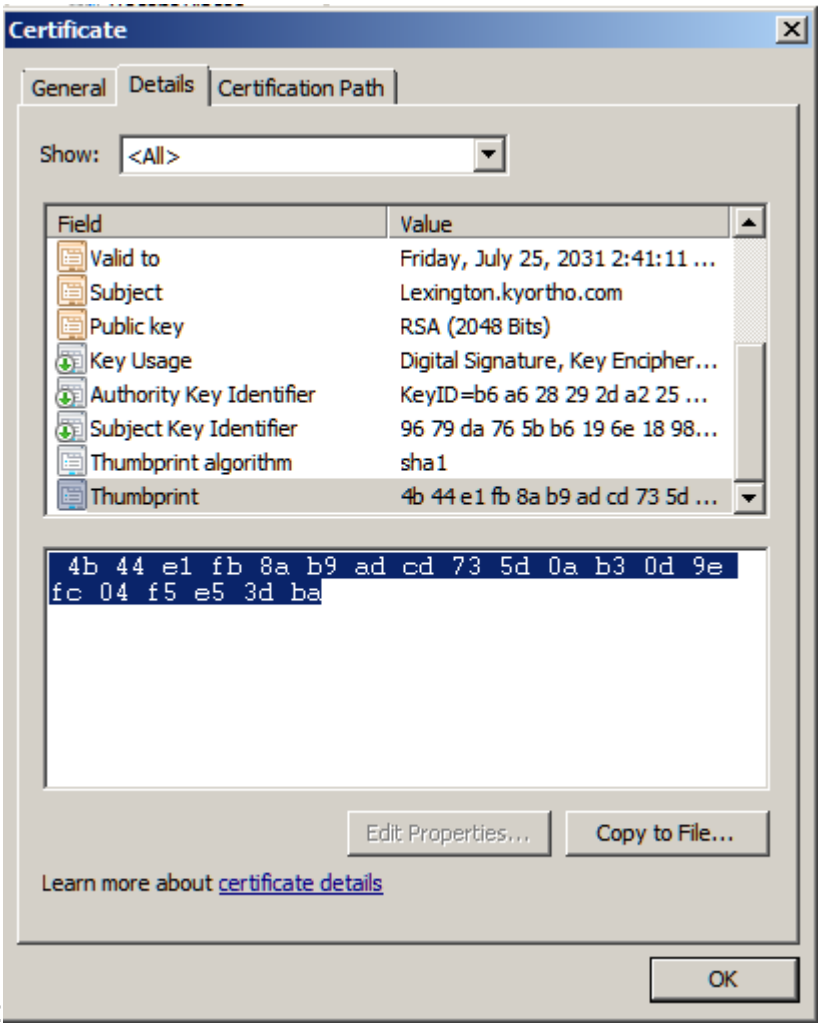
Para verificar, siga los siguientes pasos para extraer el valor de troceo de la captura de paquetes recogida entre el teléfono del IP y la cabecera VPN:

1. Localice el paquete del dispositivo de la cabecera VPN al teléfono del IP que contiene el certificado. Está típicamente en el paquete de los saludos del servidor de TLS.
2. Amplíe el contenido de paquetes y localice la encabezado:
   Secure Socket Layer > capa > protocolo de entrada en contacto del expediente de TLS V1: El certificado > certifica > certificado.
3. Haga clic con el botón derecho del ratón la encabezado del certificado y exporte los valores a un archivo .CER:





4. Abra el archivo .CER, vaya a la lengueta de los detalles, elija Thumbprint, y elija los valores. Los valores son el hash en el formato



hexadecimal:

5. Después, usted convierte el hash del maleficio al base64 usando cualquier herramienta en línea de la conversión Hex-to-Base64. El valor convertido se puede comparar al valor de troceo en el archivo de configuración del teléfono del IP si no hacen juego, después significa que el hash recibido por el teléfono del IP es de un diverso certificado que lo que es utilizada por la cabecera VPN para el SSL.

Información Relacionada

- Configurar al cliente VPN SSL para los Teléfonos IP del SCCP
- Soporte Técnico y Documentación - Cisco Systems

>