Configure el trunk de TLS del SORBO en el administrador de comunicaciones con un certificado firmado de CA.

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Antecedentes
Configurar
Paso 1. Utilice CA público o la configuración CA en el Servidor Windows 2003
Paso 2. Verifique el nombre de host y las configuraciones
Paso 3. Genere y descargue el pedido de firma de certificado (el CSR)
Paso 4. Firme el CSR con el Certificate Authority de Microsoft Windows 2003
Paso 5. Consiga el certificado raíz de CA
Paso 6. Certificado raíz de CA de la carga como confianza del CallManager
Paso 7. Cargue el certificado del CallManager CSR de la muestra de CA como certificado del CallManager.
Paso 8. Cree los perfiles de seguridad del trunk del SORBO
Paso 9. Cree los links troncales del SORBO
Paso 10. Cree a los patrones de ruta
Verificación
Troubleshooting
Recoja a la captura de paquetes en CUCM
Recoja las trazas CUCM
Discusiones relacionadas de la comunidad del soporte de Cisco

Introducción

Este documento describe un proceso gradual para configurar el trunk de Transport Layer Security del Session Initiation Protocol (SIP) (TLS) en el administrador de comunicaciones con un certificado firmado del Certificate Authority (CA).

Después de seguir este documento, los mensajes del SORBO entre dos clusteres serán cifrados usando TLS.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de:

- Administrador de las Comunicaciones unificadas de Cisco (CUCM)
- SORBO

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Versión 9.1(2) CUCM
- Versión 10.5(2) CUCM
- Microsoft Windows server 2003 como CA

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.

Antecedentes

Tal y como se muestra en de esta imagen, contacto SSL usando los Certificados.

Configurar

Paso 1. Utilice CA público o la configuración CA en el Servidor Windows 2003

Refiera al link: La configuración CA en Windows 2003 separa

Paso 2. Verifique el nombre de host y las configuraciones

Los Certificados se basan en los nombres. Asegúrese de que los nombres estén correctos antes de comenzar.

```
From SSH CLI
admin:show cert own CallManager
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
Subject Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
```

Para cambiar el nombre de host, refiera al link: Cambie el nombre de host en CUCM

Paso 3. Genere y descargue el pedido de firma de certificado (el CSR)

CUCM 9.1(2)

Para generar el CSR, navegan al Certificate Management (Administración de certificados) del > Security (Seguridad) **OS Admin > generan el CSR**

En el **campo de nombre del certificado,** seleccione la opción del **CallManager de la** lista desplegable.

Para descargar el CSR, navegue al **Certificate Management (Administración de certificados) > a la descarga CSR del > Security (Seguridad) OS Admin**

En el **campo de nombre del certificado**, seleccione la opción del **CallManager de la** lista

desplegable.

CUCM 10.5(2)

Para generar el CSR, navegue al **Certificate Management (Administración de certificados) del > Security (Seguridad) OS Admin > generan el CSR**

1. En el campo del **propósito del certificado,** seleccione el **CallManager de la** lista desplegable.

2. En el campo de la **longitud de clave,** seleccione **1024 de la** lista desplegable.
3. En el campo del **algoritmo de troceo,** seleccione el **SHA1 de la** lista desplegable.

Para descargar el CSR, navegue al **Certificate Management (Administración de certificados) > a la descarga CSR del > Security (Seguridad) OS Admin**

En el campo del **propósito del certificado,** seleccione la opción del **CallManager de la** lista desplegable.

> Nota: El CallManager CSR se genera con las 1024 claves del Rivest-Shamir-Addleman del bit (RSA).

Paso 4. Firme el CSR con el Certificate Authority de Microsoft Windows 2003

Esto es una información opcional para firmar el CSR con Microsoft Windows 2003 CA.

1. Abra las autoridades de certificación.

2. Haga clic con el botón derecho del ratón el icono de **CA** y navegue a **todas las tareas > someten la nueva petición**

3. Seleccione el CSR y haga clic la opción **abierta** (aplicable en ambos los CSR (CUCM 9.1(2) y CUCM 10.5(2))

4. Toda la visualización abierta CSR en la carpeta pendiente de las peticiones. Haga clic con el botón derecho del ratón cada CSR y navegue a **todas las tareas > problema** para publicar los Certificados. (Aplicable en ambos los CSR (CUCM 9.1(2) y CUCM 10.5(2))

5. Para descargar el certificado, elija la carpeta **publicada de los Certificados**.

Haga clic con el botón derecho del ratón el certificado y haga clic la opción **abierta**.

6. Visualizan a los detalles del certificado. Para descargar el certificado, seleccione la lengueta de los **detalles** y haga clic la **copia del** botón **para clasifiar…**

7. En la **ventana del Asistente de la exportación del certificado**, hacen clic el **base 64 codificaron X.509(.CER) el** botón de radio.

8. Nombran el archivo exactamente. Este ejemplo utiliza el formato de **CUCM1052.cer**.

Para CUCM 9.1(2), siga el mismo procedimiento.

Paso 5. Consiga el certificado raíz de CA

Abra la ventana de las **autoridades de certificación**.

Para descargar raíz CA

1. Haga clic con el botón derecho del ratón el icono de CA y haga clic la **opción Properties (Propiedades)**.

2. En la ficha general, haga clic el **certificado de la visión.**

3. En la ventana del **certificado**, haga clic la LENGUETA de los detalles.

4. Haga clic la **copia para clasifiar…**

Paso 6. Certificado raíz de CA de la carga como confianza del CallManager

Para cargar el certificado raíz de CA, login al **Certificate Management (Administración de certificados) del > Security (Seguridad) OS Admin > al certificado/a la Cadena de certificados de la carga**

Nota: Realice estos pasos en ambos el CUCMs (CUCM 9.1(2) y CUCM 10.5(2))

Paso 7. Cargue el certificado del CallManager CSR de la muestra de CA como certificado del CallManager.

Para cargar el CallManager CSR de la muestra de CA, inicie sesión al **Certificate Management (Administración de certificados) del > Security (Seguridad) OS Admin > al certificado/a la Cadena de certificados de la carga**

Nota: Realice estos pasos en ambos el CUCMs (CUCM 9.1(2) y CUCM 10.5(2))

Paso 8. Cree los perfiles de seguridad del trunk del SORBO

CUCM 9.1(2)

Para crear el perfil de seguridad del trunk del SORBO, navegue al **> Security (Seguridad) del sistema > al perfil de seguridad del trunk del SORBO**.

Copie la existencia perfil no seguro del trunk del SORBO y déle un nuevo nombre. En el ejemplo, el perfil no seguro del trunk del SORBO se ha retitulado con el perfil seguro TLS del trunk del SORBO.

En el asunto X.509 utilice el Common Name (CN) del CUCM 10.5(2) (certificado firmado de CA) tal y como se muestra en de esta imagen.

CUCM 10.5(2)

Navegue al **> Security (Seguridad) del sistema > al perfil de seguridad del trunk del SORBO.**

Copie la existencia perfil no seguro del trunk del SORBO y déle un nuevo nombre. En el ejemplo, el perfil no seguro del trunk del SORBO fue retitulado con el perfil seguro TLS del trunk del SORBO.

En el asunto X.509 utilice el CN del CUCM 9.1(2) (certificado firmado de CA) según lo resaltado:

Ambos los perfiles de seguridad del trunk del SORBO fijan un puerto entrante de 5061, en los cuales cada cluster escucha en el puerto TCP 5061 las nuevas llamadas entrantes de TLS del SORBO.

Paso 9. Cree los links troncales del SORBO

Después de que se creen los perfiles de seguridad, cree los links troncales del SORBO y realice los cambios para el parámetro de la configuración abajo en el trunk del SORBO.

CUCM 9.1(2)

1. En la ventana de la **configuración del tronco del** SORBO, marque el parámetro de la configuración **SRTP no prohibido el** checkbox.

Esto asegura el Real-Time Transport Protocol (RTP) que se utilizará para las llamadas sobre este trunk. Este cuadro debe ser marcado solamente cuando usted utiliza el SORBO TLS porque las claves para el protocolo Real-Time Transport seguro (SRTP) se intercambian en el cuerpo del mensaje del SORBO. La señalización del SORBO se debe asegurar por TLS, si no cualquier persona con la señalización NON-segura del SORBO podría desencriptar la secuencia correspondiente SRTP sobre el trunk.

2. En la **sección de información del SORBO de la** ventana de la **configuración del tronco del** SORBO, agregue **perfil de seguridad la dirección destino**, el **puerto destino**, y del **trunk del SORBO.**

CUCM 10.5(2)

1. En la ventana de la **configuración del tronco del** SORBO, marque el parámetro de la configuración **SRTP no prohibido el** checkbox.

Esto permite que el SRTP sea utilizado para las llamadas sobre este trunk. Este cuadro debe ser marcado solamente al usar el SORBO TLS, porque las claves para el SRTP se intercambian en el cuerpo del mensaje del SORBO. La señalización del SORBO se debe asegurar por TLS porque cualquier persona con una señalización NON-segura del SORBO podría desencriptar la secuencia segura correspondiente RTP sobre el trunk.

2. En la **sección de información del SORBO de la** ventana de la **configuración del tronco del** SORBO, agregue el **IP Address de destino**, el **puerto destino**, y el **perfil de seguridad**

Paso 10. Cree a los patrones de ruta

El método más simple es crear a un patrón de ruta en cada cluster, señalando directamente al trunk del SORBO. Los Grupos de Routes y las listas de la ruta podrían también ser utilizados.

Puntas CUCM 9.1(2) al **patrón de ruta** 9898 vía el trunk del SORBO de TLS al CUCM 10.5(2)

Las puntas CUCM 10.5(2) al **patrón de ruta** 1018 vía el trunk del SORBO de TLS al CUCM 9.1(2)

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

La llamada de TLS del SORBO se puede hacer el debug de con estos pasos.

Recoja a la captura de paquetes en CUCM

Para marcar la Conectividad entre el CUCM 9.1(2) y el CUCM 10.5(2), tomar a una captura de paquetes en los servidores y el reloj CUCM para el SORBO TLS trafique.

El tráfico de TLS del SORBO se transmite en el puerto TCP 5061, considerado como sorbo-TLS.

En el siguiente ejemplo hay una sesión CLI de SSH establecida al CUCM 9.1(2)

1. Captura de paquetes CLI en la pantalla

Este CLI imprime la salida en la pantalla para el tráfico de TLS del SORBO.

```
admin:utils network capture host ip 10.106.95.200
Executing command with options:
interface=eth0
ip=10.106.95.200
19:04:13.410944 IP CUCMA.42387 > 10.106.95.200.sip-tls: P 790302485:790303631(1146) ack
3661485150 win 182 <nop,nop,timestamp 2864697196 5629758>
19:04:13.450507 IP 10.106.95.200.sip-tls > CUCMA.42387: . ack 1146 win 249 <nop,nop,timestamp
6072188 2864697196>
19:04:13.465388 IP 10.106.95.200.sip-tls > CUCMA.42387: P 1:427(426) ack 1146 win 249
<nop,nop,timestamp 6072201 2864697196>
```

2. Capturas CLI a clasifiar

Este CLI hace a la captura de paquetes basada en el host y crea un archivo nombrado los paquetes.

```
admin:utils network capture eth0 file packets count 100000 size all host ip 10.106.95.200
```

Recomience el trunk del SORBO en CUCM 9.1(2) y haga la llamada de la extensión 1018 (CUCM 9.1(2)) a la extensión 9898 (CUCM 10.5(2))

Para descargar el archivo del CLI, funcione con este comando:

```
admin:file get activelog platform/cli/packets.cap
```

La captura se hace en el formato estándar .cap. Este ejemplo utiliza Wireshark para abrir el archivo packets.cap pero cualquier herramienta de la visualización de la captura de paquetes puede ser utilizada.

1. El Transmission Control Protocol (TCP) sincroniza (SYN) para establecer la comunicación TCP entre el CUCM 9.1(2)(Client) y el CUCM 10.5(2)(Server).
2. El CUCM 9.1(2) envía los saludos del cliente para comenzar la sesión de TLS.
3. El CUCM 10.5(2) envía los saludos del servidor, el certificado de servidor, y el pedido de certificado de comenzar el proceso de intercambio del certificado.

4. El certificado que el cliente CUCM 9.1(2) envía para completar el intercambio del certificado.
5. Los datos de aplicación que son señalización cifrada del SORBO, muestran que se ha establecido la sesión de TLS.

Fomente el control si los Certificados correctos están intercambiados. Después de los saludos del servidor, el servidor CUCM 10.5(2) envía su certificado al cliente CUCM 9.1(2).

El número de serie y la información sujeta que el servidor CUCM 10.5(2) tiene, se presenta al número de serie del cliente CUCM 9.1(2).The, tema, emisor, y las fechas de validez todas se comparan a la información sobre la página de la administración de certificados OS Admin.

El servidor CUCM 10.5(2) presenta su propio certificado para la verificación, ahora él marca el certificado del cliente CUCM 9.1(2). La verificación sucede en las ambas direcciones.

Si hay una discordancía entre los Certificados en la captura de paquetes y los Certificados en la página web OS Admin, después los Certificados correctos no están cargados.

Los Certificados correctos se deben cargar sobre la página CERT OS Admin.

Recoja las trazas CUCM

Las trazas CUCM pueden también ser útiles determinar qué mensajes se intercambian entre el CUCM 9.1(2) y los servidores CUCM 10.5(2) e independientemente de si establecen a la sesión SSL correctamente.

En el ejemplo, las trazas del CUCM 9.1(2) se han recogido.

Flujo de llamada:

Extensión 1018 > CUCM 9.1(2) > TRUNK de TLS del SORBO > CUCM 10.5(2) > extensión 9898

Análisis de dígitos ++

```
04530161.009 |19:59:21.185 |AppInfo |Digit analysis: match(pi="2", fqcn="1018",
cn="1018",plv="5", pss="", TodFilteredPss="", dd="9898",dac="0")
04530161.010 |19:59:21.185 |AppInfo |Digit analysis: analysis results
04530161.011 |19:59:21.185 |AppInfo ||PretransformCallingPartyNumber=1018
|CallingPartyNumber=1018
|DialingPartition=
|DialingPattern=9898
|FullyQualifiedCalledPartyNumber=9898
```

El SORBO TLS ++ se está utilizando en el puerto 5061 para esta llamada.

```
04530191.034 |19:59:21.189 |AppInfo |//SIP/SIPHandler/ccbId=0/scbId=0/SIP_PROCESS_ENQUEUE:
createConnMsg tls_security=3
04530204.002 |19:59:21.224 |AppInfo
|//SIP/Stack/Transport/0x0/sipConnectionManagerProcessConnCreated: gConnTab=0xb444c150,
addr=10.106.95.200, port=5061, connid=12, transport=TLS Over TCP
04530208.001 |19:59:21.224 |AppInfo |SIPTcp - wait_SdlSPISignal: Outgoing SIP TCP message to
10.106.95.200 on port 5061 index 12
[131,NET]
INVITE sip:9898@10.106.95.200:5061 SIP/2.0
Via: SIP/2.0/TLS 10.106.95.203:5061;branch=z9hG4bK144f49a43a
From: <sip:1018@10.106.95.203>;tag=34~4bd244e4-0988-4929-9df2-2824063695f5-19024196
To: <sip:9898@10.106.95.200>
Call-ID: 94fffc00-57415541-7-cb5f6a0a@10.106.95.203
User-Agent: Cisco-CUCM9.1
```

El mensaje SIPCertificateInd del Signal Distribution Layer ++ (SDL) proporciona los detalles sobre el tema CN y la información de conexión.

```
04530218.000 |19:59:21.323 |SdlSig   |SIPCertificateInd                    |wait
                  |SIPHandler(1,100,72,1)           |SIPTcp(1,100,64,1)
|1,100,17,11.3^*^*                       |[T:N-H:0,N:1,L:0,V:0,Z:0,D:0] connIdx= 12 --
remoteIP=10.106.95.200 --remotePort = 5061 --X509SubjectName
/C=IN/ST=cisco/L=cisco/O=cisco/OU=cisco/CN=CUCM10 --Cipher AES128-SHA --SubjectAltname =
04530219.000 |19:59:21.324 |SdlSig   |SIPCertificateInd
|restart0                       |SIPD(1,100,74,16)
|SIPHandler(1,100,72,1)           |1,100,17,11.3^*^*                       |[R:N-
H:0,N:0,L:0,V:0,Z:0,D:0] connIdx= 12 --remoteIP=10.106.95.200 --remotePort = 5061 --
X509SubjectName /C=IN/ST=cisco/L=cisco/O=cisco/OU=cisco/CN=CUCM10 --Cipher AES128-SHA --
SubjectAltname =
```