

Asegure el RTP entre CUCM y el VCS o el ejemplo de configuración de Expressway

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Condiciones](#)

[Descripción](#)

[Ejemplos del lado troncal y del lado de la línea](#)

[Estrategia de la mitigación](#)

[Configurar](#)

[Configuración del lado de la línea](#)

[Configuración del lado troncal](#)

[Opciones de encriptación de los media](#)

[Ninguno](#)

[Obligatorio](#)

[Mejor esfuerzo](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Lectura relacionada](#)

[RFC relacionados](#)

Introducción

Este documento describe cómo configurar un Real-Time Transport Protocol (RTP) seguro entre el video de Cisco Communication Server (Servidor de comunicación) (VCS) y el administrador unificado Cisco de la comunicación (CUCM).

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- CUCM
- VCS o Cisco Expressway de Cisco

Componentes Utilizados

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

- CUCM
- VCS o Cisco Expressway de Cisco

Note: Este artículo utiliza los Productos de Cisco Expressway con objeto de la explicación (a menos que donde expuesto), pero la información también se aplica si su despliegue utiliza el VCS de Cisco.

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

Condiciones

- Llamadas del Session Initiation Protocol (SIP) ruteadas entre CUCM y Expressway
- El cifrado de los media es mejor esfuerzo/opcional entre Expressway-C y CUCM

Descripción

Ha habido dificultades señaladas para la configuración del mejor cifrado de los media de esfuerzo para las llamadas del SORBO que se rutean entre CUCM y VCS/Expressway. Las configuraciones erróneas más comunes afectan a la señalización de los media cifrados, vía el protocolo Real-Time Transport seguro (SRTP), que causa el error de llamadas cifradas mejor esfuerzo cuando el transporte entre CUCM y Expressway no es seguro.

Si el transporte no es seguro, después la señalización del cifrado de los media se podría leer por un eavesdropper. En este caso, la información de señalización del cifrado de los media se elimina del protocolo session description (SDP). Sin embargo, es posible configurar CUCM para enviar (y esperar recibir) el cifrado de los media que señala sobre una conexión sin garantía. Usted puede trabajar alrededor de este misconfiguration en una de dos maneras, dependiente sobre si las llamadas son lado troncal o lado de la línea ruteado a CUCM.

Ejemplos del lado troncal y del lado de la línea

Lado troncal: Un trunk del SORBO se configura en CUCM hacia Expressway. Una zona vecina correspondiente se configura en Expressway hacia CUCM. Usted necesitaría un trunk si usted

quisiera que (Expressway no es secretario, pero el VCS es) los puntos finales VCS-registrados llamasen los puntos finales CUCM-registrados. Otro ejemplo sería habilitar H.323 que intertrabaja en su despliegue.

Lado de la línea: Las llamadas del lado de la línea van directamente a CUCM, no vía un trunk. Si todo el registro y Control de llamadas es proporcionado por CUCM, su despliegue no pudo requerir un trunk a Expressway. Por ejemplo, si Expressway se despliega puramente para el móvil y el Acceso Remoto (MRA), él proxys que el lado de la línea llama de los puntos finales externos a CUCM.

Estrategia de la mitigación

Si hay un trunk del SORBO entre CUCM y Expressway, un script de la normalización en el CUCM reescribe el SDP apropiadamente para no rechazar la llamada del cifrado de mejor esfuerzo. Este script está instalado automáticamente con versiones posteriores de CUCM, pero si usted hace las llamadas cifradas mejor esfuerzo rechazar, Cisco recomienda que usted descarga y instala el último script del VCS-Interop para su versión de CUCM.

Si la llamada va lado de la línea a CUCM, después CUCM espera ver la encabezado del x-Cisco-SRTP-*retraso* si el cifrado de los media es opcional. Si CUCM no ve esta encabezado, considera la llamada ser cifrado-MANDATORY. El soporte para esta encabezado fue agregado a Expressway en la versión X8.2, así que Cisco recomienda X8.2 o más adelante para MRA (borde de la Colaboración).

Configurar

Configuración del lado de la línea

```
[CUCM] <--mejor esfuerzo--> [Expressway-C] <--obligatorio--> [Expressway-E] <--obligatorio--> [Endpoint]
```

Para habilitar el cifrado de mejor esfuerzo de las llamadas del lado de la línea de Expressway-C a CUCM:

- Utilice un despliegue/una solución soportados (por ejemplo, MRA)
- Utilice la Seguridad mezclada del modo en CUCM
- Asegure esa confianza de Expressway y CUCM (el Certificate Authority (CA) que firme los Certificados de cada partido se debe confiar en por el otro partido)
- Utilice la versión X8.2 o más adelante de Expressway
- Utilice asegure los perfiles del teléfono en CUCM, con el conjunto del modo de la seguridad del dispositivo autenticado o cifrado - para estos modos el tipo del transporte es Transport Layer Security (TLS)

Configuración del lado troncal

- Utilice un despliegue/una solución soportados
- Utilice la Seguridad mezclada del modo en CUCM

- Asegure esa confianza de Expressway y CUCM (CA que firme los Certificados de cada partido se debe confiar en por el otro partido)
- Elija mejor esfuerzo como el modo de encriptación y TLS como el transporte en la zona vecina de Expressway a CUCM (estos valores prepopulated automáticamente en el caso del lado de la línea)
- Seleccione TLS como el transporte entrante y saliente en el perfil de seguridad del trunk del SORBO
- Marque el SRTP permitido (véase la declaración de la precaución) en el trunk del SORBO de CUCM a Expressway
- Marque para, y aplíquese en caso necesario, el script correcto de la normalización para sus versiones de CUCM y Expressway

Caution: Si usted marca la casilla de verificación permitida SRTP, Cisco recomienda fuertemente que usted utiliza un perfil cifrado de TLS de modo que las claves y la otra información relacionada con la seguridad no consiga expuestas durante las negociaciones de la llamada. Si usted utiliza un perfil NON-seguro, el SRTP todavía trabajará. Sin embargo, las claves serán expuestas en la señalización y las trazas. En ese caso, usted debe asegurar la Seguridad de la red entre CUCM y el lado de destino del trunk.

Opciones de encriptación de los media

Ninguno

El cifrado no se permite. Llama que requiere el cifrado debe fallar porque no pueden ser seguros. CUCM y Expressway son constantes en la señalización para este caso.

CUCM y Expressway ambos utilizan `m=RTP/AVP` para describir los media en el SDP. No hay atributos crypto (ningunas líneas del `a=crypto...` en las secciones de los media del SDP).

Obligatorio

Se requiere el cifrado de los media. Las llamadas Unencrypted deben fallar siempre; no se permite ningún retraso. CUCM y Expressway son constantes en la señalización para este caso.

CUCM y Expressway ambos utilizan `m=RTP/SAVP` para describir los media en el SDP. El SDP tiene atributos crypto (las líneas del `a=crypto...` en las secciones de los media del SDP).

Mejor esfuerzo

Llama se cifra que se puede cifrar. Si el cifrado no puede ser establecido, las llamadas pudieron y deben recurrir a los media unencrypted. CUCM y Expressway son contrarios en este caso.

Expressway rechaza siempre el cifrado si el transporte es Transmission Control Protocol (TCP) o User Datagram Protocol (UDP). Usted debe asegurar el transporte entre CUCM y Expressway si usted quiere el cifrado de los media.

SDP (como CUCM lo escribe): Se describe el media cifrado mientras que las líneas `m=RTP/SAVP` y del `a=crypto` se escriben en el SDP. Ésta es la señalización correcta para el cifrado de los media, pero las líneas `crypto` son legibles si el transporte no es seguro.

Si CUCM ve la encabezado del `x-Cisco-SRTP-retraso`, permite que la llamada recurra a unencrypted. Si esta encabezado está ausente, CUCM asume que la llamada requiere el cifrado (no permite el retraso).

A partir de X8.2, Expressway hace mejor esfuerzo la misma manera que CUCM hace en el caso del lado de la línea.

SDP (como Expressway escribe al lado troncal): Se describe el media cifrado mientras que las líneas `m=RTP/AVP` y del `a=crypto` se escriben en el SDP.

Sin embargo, hay dos razones que las líneas del `a=crypto` podrían estar ausentes:

1. Cuando un salto del transporte a o desde el proxy del SORBO en Expressway no es seguro, el proxy elimina las líneas `crypto` para prevenirlas de la exposición en el salto unsecure.
2. El partido de contestación elimina hacia fuera las líneas `crypto` para señalar que no puede ni hará el cifrado.

El uso del script correcto de la normalización del SORBO en CUCM atenúa este problema.

Verificación

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

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

Lectura relacionada

- [Guía de la Seguridad del administrador de las Comunicaciones unificadas de Cisco, versión 10.0\(1\)](#)
- [Conferencia optimizada para guía de la solución del VCS del administrador y de Cisco de las Comunicaciones unificadas de Cisco](#) (versión 2.0)
- [Administrador de las Comunicaciones unificadas de Cisco con el Guía de despliegue de Cisco Expressway \(trunk del SORBO\)](#) (para Cisco Expressway X8.2 y CM unificado 8.6x y 9.x)
- [Administrador de las Comunicaciones unificadas de Cisco con el Guía de despliegue del VCS de Cisco \(trunk del SORBO\)](#) (para el VCS X8.2 y CM unificado 8.6.x y 9.x de Cisco)
- [Móvil y Acceso Remoto de las Comunicaciones unificadas vía el Guía de despliegue del VCS](#)

- [de Cisco](#) (para el VCS X8.2 y CM unificado Cisco 9.1(2)SU1 de Cisco o más adelante)
- [Móvil y Acceso Remoto de las Comunicaciones unificadas vía el Guía de despliegue de Cisco Expressway](#) (para Cisco Expressway X8.2 y CM unificado Cisco 9.1(2)SU1 o más adelante)
- [Soporte Técnico y Documentación - Cisco Systems](#)

RFC relacionados

- SORBO DEL [RFC 3261](#): Session Initiation Protocol
- [RFC 4566](#) SDP: Protocolo de Descripción de Sesiones
- [RFC 4568](#) SDP: Descripciones de la Seguridad