Ejemplo de Configuración de Secure RTP entre CUCM y VCS o Expressway

Contenido

Introducción

Este documento describe cómo configurar un protocolo de transporte en tiempo real (RTP) seguro entre Cisco Video Communication Server (VCS) y Cisco Unified Communication Manager (CUCM).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- CUCM
- Cisco VCS o Cisco Expressway

Componentes Utilizados

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

- CUCM
- Cisco VCS o Cisco Expressway

  Nota: En este artículo se utilizan los productos de Cisco Expressway con fines de explicación (excepto cuando se indique lo contrario), pero la información también se aplica si su implementación utiliza Cisco VCS.

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.

Antecedentes

Condiciones

- Llamadas de protocolo de inicio de sesión (SIP) enrutadas entre CUCM y Expressway
- El cifrado de medios es el mejor esfuerzo/opcional entre Expressway-C y CUCM

Descripción

Se han notificado dificultades para la configuración del cifrado de medios de mejor esfuerzo para las llamadas SIP que se enrutan entre CUCM y VCS/Expressway. Una configuración incorrecta común afecta a la señalización de los medios cifrados, mediante el protocolo de transporte en tiempo real seguro (SRTP), que provoca el error de las llamadas cifradas de mejor esfuerzo cuando el transporte entre CUCM y Expressway no es seguro.

Si el transporte no es seguro, la señalización de cifrado de medios podría ser leída por un observador. En este caso, la información de señalización de cifrado de medios se elimina del protocolo de descripción de sesión (SDP). Sin embargo, es posible configurar CUCM para enviar (y esperar recibir) señalización de cifrado de medios a través de una conexión no segura. Puede solucionar este error de configuración de una de dos maneras, dependiendo de si las llamadas se enrutan en línea troncal o en línea a CUCM.

Ejemplos del lado troncal y del lado de línea

Lado del tronco: Un troncal SIP se configura en CUCM hacia Expressway. Se configura una zona de vecino correspondiente en Expressway hacia CUCM. Necesitaría un enlace troncal si deseara que los terminales registrados en VCS (Expressway no es un registrador, pero VCS lo es) llamen

a los terminales registrados en CUCM. Otro ejemplo sería habilitar la interconexión H.323 en su implementación.

Lado de línea: Las llamadas del lado de la línea van directamente a CUCM, no a través de un tronco. Si CUCM proporciona todo el registro y el control de llamadas, es posible que su implementación no requiera un enlace troncal a Expressway. Por ejemplo, si Expressway se implementa exclusivamente para el acceso móvil y remoto (MRA), se proxies las llamadas de línea desde terminales externos a CUCM.

Estrategia de mitigación

Si hay un enlace troncal SIP entre CUCM y Expressway, un script de normalización en CUCM reescribe el SDP adecuadamente para que no se rechace la llamada de cifrado de mejor esfuerzo. Esta secuencia de comandos se instala automáticamente con las versiones posteriores de CUCM, pero si se rechazan las llamadas cifradas con el mejor esfuerzo, Cisco recomienda que descargue e instale la última secuencia de comandos vcs-interop para su versión de CUCM.

Si la llamada pasa del lado de la línea a CUCM, CUCM espera ver el encabezado `x-cisco-srtp-fallback` si el cifrado de medios es opcional. Si CUCM no ve este encabezado, considera que la llamada es obligatoria para el cifrado. El soporte para este encabezado se agregó a Expressway en la versión X8.2, por lo que Cisco recomienda X8.2 o posterior para MRA (Collaboration Edge).

Configurar

Configuración del lado de la línea

[CUCM]<—best-fort—>[Expressway-C]<—obligatorio—>[Expressway-E]<—obligatorio—>[Endpoint]

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

- Utilizar una implementación/solución admitida (por ejemplo, MRA)
- Usar seguridad de modo mixto en CUCM
- Asegúrese de que Expressway y CUCM confían entre sí (la autoridad certificadora (CA) que firma los certificados de cada parte debe ser de confianza para la otra parte)
- Utilice la versión X8.2 o posterior de Expressway
- Utilice perfiles de teléfono seguros en CUCM, con el modo de seguridad del dispositivo configurado como Autenticado o Cifrado. Para estos modos, el tipo de transporte es Seguridad de la capa de transporte (TLS).

Configuración del lado troncal

- Utilizar una implementación/solución admitida
- Usar seguridad de modo mixto en CUCM
- Asegúrese de que Expressway y CUCM confían entre sí (la otra parte debe confiar en la CA que firma los certificados de cada parte)

- Elija el mejor esfuerzo como el modo de cifrado y TLS como el transporte en la zona vecina de Expressway a CUCM (estos valores se rellenan automáticamente en el caso del lado de la línea)
- Seleccione TLS como transporte entrante y saliente en el perfil de seguridad del troncal SIP
- Verifique SRTP Allowed (consulte la instrucción Caution) en el troncal SIP de CUCM a Expressway
- Compruebe y aplique, si es necesario, el script de normalización correcto para las versiones de CUCM y Expressway

Precaución: Si marca la casilla de verificación SRTP Allowed (SRTP permitido), Cisco recomienda encarecidamente que utilice un perfil TLS cifrado para que las claves y otra información relacionada con la seguridad no se expongan durante las negociaciones de llamadas. Si utiliza un perfil no seguro, SRTP seguirá funcionando. Sin embargo, las claves se expondrán en la señalización y en los seguimientos. En ese caso, debe garantizar la seguridad de la red entre CUCM y el lado de destino del tronco.

Opciones de cifrado de medios

Ninguno

No se permite el cifrado. Las llamadas que requieren cifrado deben fallar porque no pueden ser seguras. CUCM y Expressway son consistentes en la señalización de este caso.

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

Obligatoria

Se requiere cifrado de medios. Las llamadas no cifradas siempre deben fallar; no se permite el repliegue. CUCM y Expressway son consistentes en la señalización de este caso.

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

Mejor esfuerzo

Las llamadas que se pueden cifrar están cifradas. Si no se puede establecer el cifrado, las llamadas pueden y deben volver a los medios sin cifrar. CUCM y Expressway son inconsistentes en este caso.

Expressway siempre rechaza el cifrado si el transporte es protocolo de control de transmisión (TCP) o protocolo de datagramas de usuario (UDP). Debe proteger el transporte entre CUCM y Expressway si desea el cifrado de medios.

SDP (como lo escribe CUCM): Los medios cifrados se describen como `m=RTP/SAVP` y `a=líneas crypto` se escriben en el SDP. Esta es la señalización correcta para el cifrado de medios, pero las

líneas criptográficas son legibles si el transporte no es seguro.

Si CUCM ve el encabezado `x-cisco-srtp-fallback`, permite que la llamada vuelva a estar descifrada. Si este encabezado no existe, CUCM asume que la llamada requiere cifrado (no permite el repliegue).

A partir de X8.2, Expressway hace el mejor esfuerzo del mismo modo que CUCM en el caso de línea.

SDP (como Expressway escribe el lado troncal): Los medios cifrados se describen como `m=RTP/AVP` y `a=líneas crypto` se escriben en el SDP.

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

1. Cuando un salto de transporte hacia o desde el proxy SIP en Expressway no es seguro, el proxy elimina las líneas criptográficas para evitar que se vean expuestas en el salto no seguro.
2. El contestador elimina las líneas criptográficas para indicar que no puede o no realizará el cifrado.

El uso del script de normalización SIP correcto en CUCM mitiga este problema.

Verificación

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

Troubleshoot

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

Información Relacionada

Lectura relacionada

- Guía de seguridad de Cisco Unified Communications Manager, versión 10.0(1)
- Guía de la Solución Optimized Conferencing para Cisco Unified Communications Manager y Cisco VCS (Versión 2.0)
- Guía de implementación de Cisco Unified Communications Manager con Cisco Expressway (línea troncal SIP) (para Cisco Expressway X8.2 y Unified CM 8.6x y 9.x)
- Guía de implementación de Cisco Unified Communications Manager con Cisco VCS (línea troncal SIP) (para Cisco VCS X8.2 y Unified CM 8.6.x y 9.x)
- Guía de implementación de Unified Communications Mobile and Remote Access a través de Cisco VCS (para Cisco VCS X8.2 y Cisco Unified CM 9.1(2)SU1 o posterior)
- Guía de implementación de Unified Communications Mobile and Remote Access a través de Cisco Expressway (para Cisco Expressway X8.2 y Cisco Unified CM 9.1(2)SU1 o posterior)

- Soporte Técnico y Documentación - Cisco Systems

RFC relacionados

- SIP RFC 3261: Protocolo de inicio de sesión
- RFC 4566 SDP: Protocolo de Descripción de Sesiones
- RFC 4568 SDP: Descripciones de seguridad