Exemplo de configuração de RTP seguro entre CUCM e VCS ou Expressway

Contents

Introduction

Este documento descreve como configurar um RTP (Real-time Transport Protocol) seguro entre o Cisco Video Communication Server (VCS) e o Cisco Unified Communication Manager (CUCM).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- CUCM

- Cisco VCS ou Cisco Expressway

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- CUCM
- Cisco VCS ou Cisco Expressway

  Note: Este artigo usa os produtos Cisco Expressway para fins de explicação (exceto quando declarado), mas as informações também se aplicam se sua implantação usar o 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.

Informações de Apoio

Condições

- Chamadas do Session Initiation Protocol (SIP) roteadas entre o CUCM e o Expressway
- A criptografia de mídia é o melhor esforço/opcional entre o Expressway-C e o CUCM

Descrição

Foram relatadas dificuldades para a configuração da criptografia de mídia de melhor esforço para chamadas SIP que são roteadas entre CUCM e VCS/Expressway. Uma configuração incorreta comum afeta a sinalização de mídia criptografada, por meio do Secure Real-time Transport Protocol (SRTP), que causa falha de chamadas criptografadas de melhor esforço quando o transporte entre o CUCM e o Expressway não é seguro.

Se o transporte não for seguro, a sinalização de criptografia de mídia poderá ser lida por um espião. Nesse caso, as informações de sinalização de criptografia de mídia são removidas do Session Description Protocol (SDP). No entanto, é possível configurar o CUCM para enviar (e esperar receber) a sinalização de criptografia de mídia em uma conexão não segura. Você pode contornar esse erro de configuração de uma das duas maneiras, dependendo se as chamadas são roteadas do lado do tronco ou do lado da linha para o CUCM.

Exemplos de lado do tronco e lado da linha

Tronco: Um tronco SIP é configurado no CUCM em direção ao Expressway. Uma zona vizinha correspondente é configurada no Expressway em direção ao CUCM. Você precisaria de um tronco se quisesse endpoints registrados pelo VCS (o Expressway não é um registrador, mas o VCS é) para ligar para endpoints registrados pelo CUCM. Outro exemplo seria ativar o entrelaçamento H.323 em sua implantação.

Lado da linha: As chamadas do lado da linha vão diretamente para o CUCM, não através de um tronco. Se todo o registro e controle de chamada forem fornecidos pelo CUCM, sua implantação pode não exigir um tronco para o Expressway. Por exemplo, se o Expressway for implantado exclusivamente para acesso móvel e remoto (MRA), ele fará o proxy das chamadas de linha de endpoints externos para CUCM.

Estratégia de mitigação

Se houver um tronco SIP entre o CUCM e o Expressway, um script de normalização no CUCM regrava o SDP apropriadamente para que a chamada de criptografia de melhor esforço não seja rejeitada. Este script é automaticamente instalado com versões posteriores do CUCM, mas se você tiver chamadas criptografadas de melhor esforço rejeitadas, a Cisco recomenda que você faça download e instale o script vcs-interop mais recente para sua versão do CUCM.

Se a chamada for do lado da linha para CUCM, o CUCM espera ver o cabeçalho `x-cisco-srtp-fallback` se a criptografia de mídia for opcional. Se o CUCM não vir esse cabeçalho, ele considerará a chamada como sendo de criptografia obrigatória. O suporte para esse cabeçalho foi adicionado ao Expressway na versão X8.2, portanto a Cisco recomenda o X8.2 ou posterior para MRA (borda de colaboração).

Configurar

Configuração do lado da linha

[CUCM]<—best-effort—>[Expressway-C]<—obrigatório—>[Expressway-E]<—obrigatório—>[Endpoint]

Para habilitar a criptografia de melhor esforço de chamadas de linha do Expressway-C para o CUCM:

- Usar uma implantação / solução suportada (por exemplo, MRA)
- Usar segurança de modo misto no CUCM
- Certifique-se de que o Expressway e o CUCM confiam uns nos outros (a autoridade de certificação (CA) que assina os certificados de cada parte deve ser confiável pela outra parte)
- Usar a versão X8.2 ou posterior do Expressway
- Usar perfis de telefone seguros no CUCM, com o Device Security Mode definido como Authenticated ou Encrypted - para esses modos, o tipo de transporte é Transport Layer Security (TLS)

Configuração do lado do tronco

- Usar uma implantação / solução suportada
- Usar segurança de modo misto no CUCM
- Certifique-se de que o Expressway e o CUCM confiem um no outro (a CA que assina os certificados de cada parte deve ser confiável pela outra parte)
- Escolha o melhor esforço como o modo de criptografia e TLS como o transporte na zona

vizinha do Expressway para o CUCM (esses valores são automaticamente pré-preenchidos no caso do lado da linha)
- Selecione TLS como transporte de entrada e saída no perfil de segurança de tronco SIP
- Verifique o SRTP Permitido (consulte a instrução de cuidado) no tronco SIP do CUCM para o Expressway
- Verifique e aplique, se necessário, o script de normalização correto para suas versões do CUCM e Expressway

Caution: Se você marcar a caixa de seleção SRTP Permitido, a Cisco recomenda que você use um perfil TLS criptografado para que as chaves e outras informações relacionadas à segurança não sejam expostas durante as negociações de chamada. Se você usar um perfil não seguro, o SRTP ainda funcionará. No entanto, as chaves serão expostas na sinalização e nos rastreamentos. Nesse caso, você deve garantir a segurança da rede entre o CUCM e o lado de destino do tronco.

Opções de criptografia de mídia

Nenhum

A criptografia não é permitida. As chamadas que exigem criptografia devem falhar porque não podem ser seguras. O CUCM e o Expressway são consistentes na sinalização desse caso.

CUCM e Expressway usam `m=RTP/AVP` para descrever a mídia no SDP. Não há atributos de criptografia (sem `a=criptografia...` nas seções de mídia do SDP).

Obrigatório

A criptografia de mídia é obrigatória. As chamadas não criptografadas devem sempre falhar; não é permitido recuo. O CUCM e o Expressway são consistentes na sinalização desse caso.

CUCM e Expressway usam `m=RTP/SAVP` para descrever a mídia no SDP. O SDP tem atributos de criptografia (`a=crypto...` nas seções de mídia do SDP).

O melhor esforço

As chamadas que podem ser criptografadas são criptografadas. Se a criptografia não puder ser estabelecida, as chamadas podem e devem voltar para mídias não criptografadas. CUCM e Expressway são inconsistentes neste caso.

O Expressway sempre recusará a criptografia se o transporte for Transmission Control Protocol (TCP) ou User Datagram Protocol (UDP). Você deve proteger o transporte entre o CUCM e o Expressway se quiser criptografia de mídia.

SDP (como o CUCM escreve): A mídia criptografada é descrita como `m=RTP/SAVP` e `a=`linhas `criptografadas` são gravadas no SDP. Essa é a sinalização correta para criptografia de mídia, mas as linhas de criptografia podem ser lidas se o transporte não for seguro.

Se o CUCM vir o cabeçalho `x-cisco-srtp-fallback`, ele permitirá que a chamada volte para não criptografada. Se esse cabeçalho estiver ausente, o CUCM assumirá que a chamada requer criptografia (não permite fallback).

A partir do X8.2, o Expressway faz o melhor esforço da mesma forma que o CUCM faz no caso do lado da linha.

SDP (como o Expressway grava o lado do tronco): A mídia criptografada é descrita como `m=RTP/AVP` e `a=`linhas `criptografadas` são gravadas no SDP.

No entanto, há dois motivos para que as linhas de criptografia a=possam estar ausentes:

1. Quando um salto de transporte de ou para o proxy SIP no Expressway não é seguro, o proxy retira as linhas de criptografia para impedir que elas se exponham no salto não seguro.
2. A parte que responde retira as linhas de criptografia para sinalizar que não pode ou não fará criptografia.

O uso do script de normalização SIP correto no CUCM atenua esse problema.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

Leitura relacionada

- Guia de segurança do Cisco Unified Communications Manager, versão 10.0(1)
- Otimized Conferencing for Cisco Unified Communications Manager and Cisco VCS Solution Guide (Versão 2.0)
- Guia de implantação do Cisco Unified Communications Manager com Cisco Expressway (tronco SIP) (para Cisco Expressway X8.2 e Unified CM 8.6x e 9.x)
- Guia de implantação do Cisco Unified Communications Manager com Cisco VCS (tronco SIP) (para Cisco VCS X8.2 e Unified CM 8.6.x e 9.x)
- Unified Communications Mobile and Remote Access via Cisco VCS Deployment Guide (para Cisco VCS X8.2 e Cisco Unified CM 9.1(2)SU1 ou posterior)
- Unified Communications Mobile and Remote Access via Cisco Expressway Deployment Guide (para Cisco Expressway X8.2 e Cisco Unified CM 9.1(2)SU1 ou posterior)
- Suporte Técnico e Documentação - Cisco Systems

RFCs relacionados

- RFC 3261 SIP: Protocolo de Iniciação de Sessão
- RFC 4566 SDP: Protocolo de descrição de sessão
- RFC 4568 SDP: Descrições de segurança