Fixe o RTP entre CUCM e VC ou exemplo de configuração da via expressa

Índice

Introdução

Este documento descreve como estabelecer um Real-Time Transport Protocol (RTP) seguro entre o servidor de comunicação da vídeo Cisco (VC) e o gerente unificado Cisco de uma comunicação (CUCM).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- CUCM
- Cisco VC ou via expressa de Cisco

Componentes Utilizados

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

- CUCM
- Cisco VC ou via expressa de Cisco

  Nota: Este artigo usa o Produtos da via expressa de Cisco para fins da explicação (a não ser que onde indicado), mas a informação igualmente aplica-se se seu desenvolvimento usa Cisco VC.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Condições

- Atendimentos do Session Initiation Protocol (SIP) distribuídos entre CUCM e via expressa
- A criptografia de mídias é melhor esforço/opcional entre a via expressa-C e o CUCM

Descrição

Houve umas dificuldades relatadas para a configuração da melhor criptografia de mídias do esforço para os atendimentos do SORVO que são distribuídos entre CUCM e VCS/Expressway. Uma falta de configuração comum afeta a sinalização de media cifrados, através do protocolo de transporte em tempo real seguro (SRTP), que causa a falha de atendimentos cifrados melhor esforço quando o transporte entre CUCM e via expressa não é seguro.

Se o transporte não é seguro, a seguir a sinalização da criptografia de mídias poderia ser lida por um eavesdropper. Neste caso, a informação de sinalização da criptografia de mídias é descascada do protocolo session description (SDP). Contudo, é possível configurar CUCM para enviar (e para esperar receber) a criptografia de mídias que sinaliza sobre uma conexão inseguro. Você pode trabalhar em torno deste misconfiguration em uma de duas maneiras, dependente de se os atendimentos são Lado de truncamento ou linha lateral distribuída a CUCM.

Exemplos do Lado de truncamento e da linha lateral

Lado de truncamento: Um tronco do SORVO é configurado em CUCM para a via expressa. Uma zona vizinha correspondente é configurada na via expressa para CUCM. Você precisaria um tronco se você quis (a via expressa não é um escrivão, mas os VC são) valores-limite VC-

registrados chamar valores-limite CUCM-registrados. Um outro exemplo seria permitir H.323 que colabora em seu desenvolvimento.

Linha lateral: Os atendimentos da linha lateral vão diretamente a CUCM, não através de um tronco. Se todo o registro e Controle de chamadas são fornecidos por CUCM, seu desenvolvimento não pôde exigir um tronco à via expressa. Por exemplo, se a via expressa está distribuída puramente para o móbil e o Acesso remoto (MRA), ele proxys que a linha lateral chama dos valores-limite externos a CUCM.

Estratégia da mitigação

Se há um tronco do SORVO entre CUCM e via expressa, um script da normalização no CUCM reescreve o SDP apropriadamente de modo que o atendimento da criptografia do melhor esforço não seja rejeitado. Este script é instalado automaticamente com liberações mais atrasadas de CUCM, mas se você tem atendimentos cifrados melhor esforço rejeitados, Cisco recomenda que você transfere e instala o script o mais atrasado de VC-Interop para sua versão de CUCM.

Se o atendimento vai linha lateral a CUCM, a seguir CUCM espera ver o encabeçamento da x-Cisco-SRTP-`reserva` se a criptografia de mídias é opcional. Se CUCM não vê este encabeçamento, considera o atendimento ser criptografia-MANDATORY. O apoio para este encabeçamento foi adicionado à via expressa na versão X8.2, assim que Cisco recomenda X8.2 ou mais tarde para MRA (borda da Colaboração).

Configurar

Configuração da linha lateral

[CUCM] <--melhor esforço--> [Expressway-C] <--obrigatório--> [Expressway-E] <--obrigatório--> [Endpoint]

A fim permitir a criptografia do melhor esforço de atendimentos da linha lateral da via expressa-C a CUCM:

- Use um desenvolvimento/solução apoiados (por exemplo, MRA)
- Use Segurança misturada do modo em CUCM
- Assegure essa via expressa e confiança CUCM (o Certificate Authority (CA) que assina os Certificados de cada partido deve ser confiado pelo outro partido)
- Use a versão X8.2 ou mais tarde da via expressa
- Use fixa perfis do telefone em CUCM, com o grupo do modo da segurança do dispositivo autenticado ou cifrado - para estes modos o tipo do transporte é o Transport Layer Security (TLS)

Configuração do Lado de truncamento

- Use um desenvolvimento/solução apoiados
- Use Segurança misturada do modo em CUCM
- Assegure essa via expressa e confiança CUCM (CA que assina os Certificados de cada

partido deve ser confiado pelo outro partido)
- Escolha o melhor esforço como o modo de criptografia e o TLS como o transporte na zona vizinha da via expressa a CUCM (estes valores prepopulated automaticamente no exemplo da linha lateral)
- Selecione o TLS como o transporte de entrada e de partida no perfil de segurança do tronco do SORVO
- Verifique o SRTP permitido (veja a indicação do cuidado) no tronco do SORVO de CUCM à via expressa
- Verifique, e aplique caso necessário, o script correto da normalização para suas versões de CUCM e via expressa

Cuidado: Se você verifica a caixa de verificação permitida SRTP, Cisco recomenda fortemente que você usa um perfil cifrado TLS de modo que as chaves e a outra informação relacionado à segurança não obtenham expostas durante negociações de chamada. Se você usa um perfil NON-seguro, o SRTP ainda trabalhará. Contudo, as chaves serão expostas na sinalização e nos traços. Nesse caso, você deve assegurar a Segurança da rede entre CUCM e o lado de destino do tronco.

Opções da criptografia de mídias

Nenhum

A criptografia não é permitida. Chama que exige a criptografia deve falhar porque não podem ser seguros. CUCM e a via expressa são consistentes na sinalização para este caso.

CUCM e a via expressa ambos usam `m=RTP/AVP` a fim descrever os media no SDP. Não há nenhum atributo cripto (nenhumas linhas do `a=crypto… nas` seções dos media do SDP).

Obrigatório

A criptografia de mídias é exigida. Os atendimentos Unencrypted devem sempre falhar; nenhuma reserva é permitida. CUCM e a via expressa são consistentes na sinalização para este caso.

CUCM e a via expressa ambos usam `m=RTP/SAVP` a fim descrever os media no SDP. O SDP tem atributos criptos (linhas do `a=crypto… nas` seções dos media do SDP).

O melhor esforço

Chama que pode ser cifrado é cifrado. Se a criptografia não pode ser estabelecida, os atendimentos puderam e devem cair de volta aos media unencrypted. CUCM e a via expressa são incompatíveis neste caso.

A via expressa recusa sempre a criptografia se o transporte é Transmission Control Protocol (TCP) ou User Datagram Protocol (UDP). Você deve fixar o transporte entre CUCM e via expressa se você quer a criptografia de mídias.

SDP (como CUCM o escreve): O media cifrado é descrito enquanto as linhas `m=RTP/SAVP` e da`=crypto` são escritas no SDP. Esta é a sinalização correta para a criptografia de mídias, mas as linhas criptos são legíveis se o transporte não é seguro.

Se CUCM vê o encabeçamento da x-Cisco-SRTP-`reserva`, permite que o atendimento caia de volta a unencrypted. Se este encabeçamento é ausente, CUCM supõe que o atendimento exige a criptografia (não permite a reserva).

Até à data de X8.2, a via expressa faz o melhor esforço a mesma maneira que CUCM faz no exemplo da linha lateral.

SDP (como a via expressa escreve o Lado de truncamento): O media cifrado é descrito enquanto as linhas `m=RTP/AVP` e da`=crypto` são escritas no SDP.

Contudo, há dois raciocina que as linhas do a=crypto poderiam ser ausentes:

1. Quando um salto do transporte a ou do proxy do SORVO na via expressa não é seguro, o proxy descasca as linhas criptos a fim impedi-las da exposição no salto inseguro.
2. O partido de resposta descasca para fora as linhas criptos a fim sinalizar que não pode nem não fará a criptografia.

O uso do script correto da normalização do SORVO em CUCM abranda esta edição.

Verificar

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

Troubleshooting

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

Informações Relacionadas

Leitura relacionada

- Guia da Segurança do gerente das comunicações unificadas de Cisco, liberação 10.0(1)
- Conferências aperfeiçoadas para comunicações unificadas gerente de Cisco e o guia da solução de Cisco VC (liberação 2.0)
- Gerente das comunicações unificadas de Cisco com o guia de distribuição da via expressa de Cisco (tronco do SORVO) (para a via expressa X8.2 e CM unificado 8.6x e 9.x de Cisco)
- Gerente das comunicações unificadas de Cisco com o guia de distribuição de Cisco VC (tronco do SORVO) (para Cisco VC X8.2 e CM unificado 8.6.x e 9.x)
- Móbil e Acesso remoto das comunicações unificadas através do guia de distribuição de Cisco VC (para Cisco VC X8.2 e CM unificado Cisco 9.1(2)SU1 ou mais tarde)

- Móbil e Acesso remoto das comunicações unificadas através do guia de distribuição da via expressa de Cisco (para a via expressa X8.2 e CM unificado Cisco 9.1(2)SU1 de Cisco ou mais tarde)
- Suporte Técnico e Documentação - Cisco Systems

RFC relacionados

- SORVO DO RFC 3261: Protocolo de iniciação de sessão
- RFC 4566 SDP: Protocolo session description
- RFC 4568 SDP: Descrições da Segurança