CUCM和VCS或Expressway之间的安全RTP配置示例

目录

简介

本文档介绍如何在思科视频通信服务器(VCS)和思科统一通信管理器(CUCM)之间设置安全实时传输协议(RTP)。

先决条件

要求

Cisco 建议您了解以下主题：

- CUCM

- Cisco VCS或Cisco Expressway

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CUCM
- Cisco VCS或Cisco Expressway

  注意：本文使用Cisco Expressway产品进行说明（声明除外），但如果部署使用Cisco VCS，信息也适用。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

条件

- 在CUCM和Expressway之间路由的会话发起协议(SIP)呼叫
- 媒体加密是Expressway-C和CUCM之间的尽力/可选

描述

对于在CUCM和VCS/Expressway之间路由的SIP呼叫，配置尽力媒体加密时报告了一些困难。常见的错误配置会通过安全实时传输协议(SRTP)影响加密媒体的信令，这会在CUCM和Expressway之间的传输不安全时导致尽力加密呼叫失败。

如果传输不安全，则窃听者可以读取媒体加密信令。在这种情况下，会从会话描述协议(SDP)中删除媒体加密信令信息。 但是，可以将CUCM配置为通过不安全的连接发送（并期望接收）媒体加密信令。您可以通过两种方式之一解决此错误配置，具体取决于呼叫是路由到CUCM的中继端还是线路端。

中继端和线路端示例

中继端：CUCM上配置了通往Expressway的SIP中继。Expressway上配置了指向CUCM的对应邻居区域。如果您希望VCS注册（Expressway不是注册器，但VCS是）终端呼叫CUCM注册的终端，则需要中继。另一个示例是在部署中启用H.323互通。

线路端：线路端呼叫直接转到CUCM，而不是通过中继。如果所有注册和呼叫控制都由CUCM提供，则您的部署可能不需要通向Expressway的中继。例如，如果Expressway纯粹为移动和远程访问(MRA)部署，它会将线路侧呼叫从外部终端代理到CUCM。

缓解策略

如果CUCM和Expressway之间有SIP中继，则CUCM上的规范化脚本会相应地重写SDP，以便不会拒绝尽力加密呼叫。此脚本随CUCM的更高版本自动安装，但如果您拒绝了尽力而为的加密呼叫，思科建议您为CUCM版本下载并安装最新的vcs-interop脚本。

如果呼叫在线路端到CUCM，则如果媒体加密是可选的，则CUCM期望看到`x-cisco-srtp-fallback`头。如果CUCM未看到此报头，它会认为该呼叫是加密强制的。X8.2版本中为Expressway添加了对此报头的支持，因此思科建议MRA（协作边缘）使用X8.2或更高版本。

配置

线路端配置

[CUCM]< — 尽力而为 — >[Expressway-C]<—mandatory—>[Expressway-E]<—mandatory—>[终端]

要对从Expressway-C到CUCM的线路侧呼叫启用尽力加密，请执行以下操作：

- 使用支持的部署/解决方案（例如MRA）
- 在CUCM上使用混合模式安全
- 确保Expressway和CUCM相互信任(签署各方证书的证书颁发机构(CA)必须由另一方信任)
- 使用Expressway的X8.2版或更高版本
- 在CUCM上使用安全电话配置文件，设备安全模式设置为身份验证或加密 — 对于这些模式，传输类型为传输层安全(TLS)

中继端配置

- 使用支持的部署/解决方案
- 在CUCM上使用混合模式安全
- 确保Expressway和CUCM相互信任（签署各方证书的CA必须由另一方信任）
- 选择尽力而为作为加密模式，选择TLS作为从Expressway到CUCM的邻居区域上的传输（这些值在线路侧情况下自动预填充）
- 在SIP中继安全配置文件上选择TLS作为入站和出站传输
- 在从CUCM到Expressway的SIP中继上检查SRTP允许（请参阅Caution语句）
- 检查并应用CUCM和Expressway版本的正确规范化脚本（如果需要）

  警告：如果选中SRTP Allowed复选框，思科强烈建议您使用加密的TLS配置文件，以便在呼叫协商期间密钥和其他安全相关信息不会暴露。如果使用非安全配置文件，SRTP仍然有效。但是，密钥会以信令和跟踪方式暴露。在这种情况下，您必须确保CUCM和中继目标端之间网络的安全。

介质加密选项

无

不允许加密。需要加密的呼叫应会失败，因为它们不安全。CUCM和Expressway在本例中的信令一

致。

CUCM和Expressway都使m=RTP/AVP来描述SDP中的媒体。SDP的媒体部分中性（没有a=crypto...行）。

必需

介质加密是必需的。未加密的呼叫应始终失败；不允许回退。CUCM和Expressway在本例中的信令一致。

CUCM和Expressway都使m=RTP/SAVP来描述SDP中的媒体。SDP具有加密属性(a=……行，位于SDP的媒体部分)。

尽力

可以加密的呼叫将被加密。如果无法建立加密，则呼叫可能且应该回退到未加密的介质。在本例中，CUCM和Expressway不一致。

如果传输为传输控制协议(TCP)或用户数据报协议(UDP),Expressway始终拒绝加密。 如果需要媒体加密，必须保护CUCM和Expressway之间的传输。

SDP（如CUCM所写）：加密媒体描述m=RTP/SAVP,a=线路写入SDP。这是媒体加密的正确信令，但如果传输不安全，加密线路可读。

如果CUCM看到x-cisco-srtp-fallback，则允许呼叫回退到未加密的状态。如果此报头不存在，CUCM会假设呼叫需要加密（不允许回退）。

从X8.2开始，Expressway的工作方式与CUCM在线路端案例中的工作方式相同。

SDP（当Expressway在中继端写入时）：加密媒体描述m=RTP/AVP,a=线路写入SDP。

但是，a=crypto线路可能不存在有两个原因：

1. 当Expressway上进出SIP代理的传输跳数不安全时，代理将删除加密线路，以防止它们在不安全的跳数上暴露。
2. 应答方删除加密线路，以表明它不能或不会加密。

在CUCM上使用正确的SIP规范化脚本可缓解此问题。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

相关阅读

- 思科统一通信管理器安全指南，版本10.0(1)
- 《Cisco Unified Communications Manager和Cisco VCS解决方案指南(版本2.0)优化会议》
- 带Cisco Expressway（SIP中继）的Cisco Unified Communications Manager部署指南（适用于Cisco Expressway X8.2和Unified CM 8.6x和9.x）
- 带Cisco VCS（SIP中继）的Cisco Unified Communications Manager部署指南（适用于Cisco VCS X8.2和Unified CM 8.6.x和9.x）
- 通过Cisco VCS部署指南(适用于Cisco VCS X8.2和Cisco Unified CM 9.1(2)SU1或更高版本)实现的统一通信移动和远程访问
- 通过Cisco Expressway部署指南(适用于Cisco Expressway X8.2和Cisco Unified CM 9.1(2)SU1或更高版本)实现统一通信移动和远程访问
- 技术支持和文档 - Cisco Systems

相关RFC

- RFC 3261 SIP:会话初始协议
- RFC 4566 SDP:会话描述协议
- RFC 4568 SDP:安全说明