在CUCM和VCS或者Expressway配置示例之间的安全RTP

目录

简介

本文描述如何设置在Cisco视频通信服务器(VCS)和Cisco Unified Communications管理器(CUCM)之间的一安全实时传输协议(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：此条款为说明的目的使用Cisco Expressway产品(除了其中陈述)，但是信息也应用，如果您的部署使用Cisco VCS。

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

- 会话初始化协议(SIP)呼叫路由在CUCM和Expressway之间
- 梅迪亚加密是最佳效果/可选在ExpresswayC和CUCM之间

说明

有为最佳效果媒体加密的配置报告的困难路由在CUCM和VCS/Expressway之间的SIP呼叫的。一普通的误配置通过安全实时传输协议(SRTP)影响已加密媒体信令，导致尽最大努力加密的呼叫的失败，当在CUCM和Expressway之间的传输不安全时。

如果传输不安全，则媒体加密信令可能由窃听者读。在这种情况下，媒体加密信令信息从会话描述协议(SDP)剥离。然而，配置CUCM发送(和期望接收)是可能的发信号在一无担保的连接的媒体加密。您在两种方式之一中能在此误配置附近工作，从属呼叫是否是路由的中继线侧或线路端对CUCM。

中继线侧和线路端示例

中继线侧：SIP中继在往Expressway的CUCM配置。一个对应的邻接区域在往CUCM的Expressway配置。您会需要中继，如果希望VCS注册的(Expressway不是管理员，但是VCS是)终端呼叫CUCM注册的终端。另一示例是启用相互作用在您的部署的H.323。

线路端：线路侧呼叫去直接地CUCM，不通过中继。如果CUCM提供所有注册和呼叫控制，您的部署也许不要求中继到Expressway。例如，如果Expressway为莫比尔和远程访问(MRA)纯粹地部署，它线路端从外部终端呼叫到CUCM的代理。

缓解策略

如果有在CUCM和Expressway之间的一SIP中继，在CUCM的一份标准化脚本重写SDP适当地，以便最佳效果加密呼叫没有拒绝。此脚本用CUCM最新版本自动地安装，但是，如果安排尽最大努力加密的呼叫拒绝，思科建议您下载并且安装CUCM您的版本的最新的VCS Interop脚本。

如果呼叫去线路端CUCM，则CUCM期望发现x思科SRTP `fallback`报头，如果媒体加密可选。如果CUCM看不到此报头，认为呼叫加密MANDATORY。此报头的支持被添加了到在版本X8.2的Expressway，因此思科推荐X8.2或以后为MRA (协作边缘)。

配置

线路侧配置

[CUCM] <--尽最大努力--> [Expressway-C] <--必须--> [Expressway-E] <--必须--> [Endpoint]

为了启用线路端呼叫的最佳效果加密从ExpresswayC的到CUCM ：

- 请使用一支持的部署/解决方案(例如， MRA)
- 请使用在CUCM的混合模式的安全
- 保证Expressway和CUCM互相委托(签署每个当事人的证书的Certificate Authority (CA)必须由另一个当事人委托)
- 请使用版本X8.2或以上Expressway
- 请使用在CUCM的安全电话配置文件，当设备安全性模式设置验证或加密-这些模式的传输类型是传输层安全(TLS)

中继线侧配置

- 请使用一支持的部署/解决方案
- 请使用在CUCM的混合模式的安全
- 保证Expressway和CUCM互相委托(签署每个当事人的证书的CA必须由另一个当事人委托)
- 选择尽力作为加密模式和TLS作为在邻接区域的传输从Expressway到CUCM (这些值在线路侧案件自动地被事前填充)
- 选择TLS，在SIP中继安全配置文件的入站和出站传输
- 检查在从CUCM的SIP中继允许的(请参阅小心语句) SRTP到Expressway
- 检查，并且如果需要，申请，正确标准化脚本CUCM您的版本和Expressway

  警告：如果检查允许的SRTP复选框，思科强烈建议您使用一已加密TLS配置文件，以便密钥和其他涉及安全的信息没获得显示在呼叫协商中。如果使用一不安全的配置文件， SRTP将运作。然而，密钥在信令和跟踪将显示。在那种情况下，您必须保证网络的安全在CUCM和中继的目的地端的之间。

梅迪亚加密选项

无

加密没有允许。要求加密的呼叫应该发生故障，因为他们不可以安全。CUCM和Expressway是一致

在此案件的信令。

CUCM和Expressway两个使用m=RTP/AVP为了描述在SDP的媒体。没有crypto属性(在SDP的媒体部分的没有a=crypto…线路)。

必须

梅迪亚加密要求。未加密呼叫应该总是发生故障;fallback没有允许。CUCM和Expressway是一致在此案件的信令。

CUCM和Expressway两个使用m=RTP/SAVP为了描述在SDP的媒体。SDP有crypto属性(在SDP的媒体部分的a=crypto…线路)。

尽力

可以加密的呼叫加密。如果加密不可能设立，呼叫也许并且应该下跌回到未加密媒体。CUCM和Expressway在这种情况下不一致。

如果传输是传输控制协议(TCP)或用户数据报协议(UDP)， Expressway总是拒绝加密。如果想要媒体加密，您必须获取在CUCM和Expressway之间的传输。

SDP (作为CUCM写入它) ：当m=RTP/SAVP和a=crypto线路写入到SDP，已加密媒体描述。这是媒体加密的正确信号，但是crypto线路是可读的，如果传输不安全。

如果CUCM看到x思科SRTP fallback报头，允许呼叫落回到未加密。如果此报头是缺少的，CUCM假设呼叫要求加密(不允许fallback)。

自X8.2， Expressway执行尽力和一样CUCM在线路侧案件执行的方式。

SDP (作为Expressway写中继线侧) ：当m=RTP/AVP和a=crypto线路写入到SDP，已加密媒体描述。

然而，有两原因a=crypto线路可能是缺少的：

1. 当到/从SIP代理的传输跳Expressway的不安全时，代理剥离crypto线路为了防止他们在不安全的跳的风险。
2. 回答的当事人剥离crypto线路为了表明不能或不执行加密。

使用在CUCM的正确SIP标准化脚本缓和此问题。

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

相关读

- Cisco Unified Communications Manager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)的优化会议
- Cisco Unified Communications Manager用思科Expressway (SIP中继)部署指南(思科Expressway X8.2和Unified CM 8.6x和9.x)
- Cisco Unified Communications Manager用Cisco VCS (SIP中继)部署指南(Cisco VCS X8.2和Unified CM 8.6.x和9.x)
- 统一通信移动和远程访问通过Cisco VCS部署指南(Cisco VCS X8.2和Cisco Unified CM 9.1(2)SU1或以上)
- 统一通信莫比尔和远程访问通过思科Expressway部署指南(思科Expressway X8.2和Cisco Unified CM 9.1(2)SU1或以上)
- 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