CUCM和VCS或Expressway之間的安全RTP配置示例

目錄

簡介

本檔案介紹如何在思科視訊通訊伺服器(VCS)和思科整合通訊管理員(CUCM)之間設定安全即時傳輸通訊協定(RTP)。

必要條件

需求

思科建議您瞭解以下主題：

- CUCM

- Cisco VCS或Cisco Expressway

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- CUCM
- Cisco VCS或Cisco Expressway

  附註：本文使用Cisco Expressway產品進行解釋（宣告除外），但是如果您的部署使用Cisco VCS，該資訊也適用。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

狀況

- 在CUCM和Expressway之間路由的會話初始協定(SIP)呼叫
- 媒體加密是Expressway-C和CUCM之間盡最大努力/可選項

說明

在CUCM和VCS/Expressway之間路由的SIP呼叫的最佳努力媒體加密配置存在困難。常見的錯誤配置會影響通過安全即時傳輸協定(SRTP)的加密媒體信令，當CUCM和Expressway之間的傳輸不安全時，這會導致盡力加密呼叫失敗。

如果傳輸不安全，則竊聽者可以讀取媒體加密信令。在這種情況下，媒體加密訊號資訊會從作業階段說明通訊協定(SDP)中移除。 但是，可以將CUCM配置為通過不安全的連線傳送（並期望接收）媒體加密信令。根據呼叫是中繼端還是線路端路由到CUCM，您可以通過以下兩種方式之一解決此配置錯誤。

中繼端和線路端示例

中繼端：在CUCM上配置指向Expressway的SIP中繼。在Expressway上向CUCM配置相應的鄰居區域。如果您想讓VCS註冊（Expressway不是註冊器，但VCS是）的端點呼叫CUCM註冊的端點，則需要中繼。另一個示例是在部署中啟用H.323互通。

線路側：線路側呼叫直接轉到CUCM，而不是通過中繼。如果所有註冊和呼叫控制都由CUCM提供，則您的部署可能不需要到Expressway的中繼。例如，如果Expressway僅用於移動和遠端訪問(MRA)，它將代理從外部終端到CUCM的線路端呼叫。

緩解策略

如果CUCM和Expressway之間存在SIP中繼，則CUCM上的規範化指令碼會正確重寫SDP，以便不拒絕盡力加密呼叫。此指令碼隨較新版本的CUCM自動安裝，但是如果您拒絕盡力加密呼叫，思科建議您下載並安裝適用於您的CUCM版本的最新vcs-interop指令碼。

如果呼叫轉到線路端到CUCM，則如果媒體加密是可選的，CUCM期望看到`x-cisco-srtp-fallback`報頭。如果CUCM沒有看到此報頭，則會認為該呼叫是強制加密的。X8.2版中已向Expressway新增了對此標頭的支援，因此思科建議使用X8.2或更高版本進行MRA（合作邊緣）。

設定

線路端組態

[CUCM]< — 盡力而為 — >[Expressway-C]<—mandatory—>[Expressway-E]<—mandatory—>[Endpoint]

要對從Expressway-C到CUCM的線路端呼叫啟用盡力加密，請執行以下操作：

- 使用支援的部署/解決方案（例如MRA）
- 在CUCM上使用混合模式安全
- 確保Expressway和CUCM相互信任(簽署各方證書的證書頒發機構(CA)必須由另一方信任)
- 使用Expressway 8.2版或更高版本
- 在CUCM上使用安全電話配置檔案，將「裝置安全模式」設定為「已驗證」或「已加密」 — 對於這些模式，傳輸型別是「傳輸層安全(TLS)」

中繼端組態

- 使用支援的部署/解決方案
- 在CUCM上使用混合模式安全
- 確保Expressway和CUCM相互信任（簽署各方證書的CA必須是另一方信任的）
- 選擇盡力作為加密模式，選擇TLS作為從Expressway到CUCM的相鄰區域上的傳輸（這些值會自動預填充到行端案例中）
- 選擇TLS作為SIP中繼安全配置檔案上的入站和出站傳輸
- 檢查從CUCM到Expressway的SIP中繼上的SRTP Allowed（請參閱警告語句）
- 檢查CUCM和Expressway版本的正確規範化指令碼，並在必要時應用

  注意：如果選中SRTP Allowed覈取方塊，思科強烈建議使用加密的TLS配置檔案，以便在呼叫協商期間不會公開金鑰和其他安全相關資訊。如果您使用不安全的配置檔案，SRTP仍將運行。但是，金鑰將在信令和跟蹤中公開。在這種情況下，您必須確保CUCM和中繼目的端之間的網路安全。

媒體加密選項

無

不允許加密。需要加密的呼叫應會失敗，因為它們無法安全。CUCM和Expressway在此案例中的信

令保持一致。

CUCM和Expressway都使用m=RTP/AVP來描述SDP中的介質。在SDP的媒體部分中性(no=crypto...行)。

必填

需要介質加密。未加密的呼叫應始終失敗；不允許回退。CUCM和Expressway在此案例中的信令保持一致。

CUCM和Expressway都使用m=RTP/SAVP來描述SDP中的介質。SDP具有加密屬性(a=……行，在SDP的媒體部分中)。

盡最大努力

可對可加密的呼叫進行加密。如果無法建立加密，呼叫可能而且應該回退到未加密的介質。在此案例中，CUCM和Expressway不一致。

如果傳輸是傳輸控制通訊協定(TCP)或使用者資料包通訊協定(UDP),Expressway一律拒絕加密。 如果需要媒體加密，必須保護CUCM和Expressway之間的傳輸。

SDP（由CUCM寫入）：加密介質描述為m=RTP/SAVP,a=crypto行寫入到SDP。這是媒體加密的正確訊號，但是如果傳輸不安全，則加密線路是可讀的。

如果CUCM看到x-cisco-srtp-fallback報頭，則允許呼叫回退到未加密狀態。如果此報頭不存在，CUCM會假設該呼叫需要加密（不允許回退）。

從X8.2開始，Expressway會像線側案例中的CUCM一樣盡最大努力。

SDP（Expressway寫入中繼端）：加密介質描述為m=RTP/AVP,a=crypto行寫入到SDP。

但是，可能沒有a=crypto行有兩個原因：

1. 當Expressway上與SIP代理之間的傳輸躍點不安全時，代理會刪除加密行，以防止它們在不安全的躍點上暴露出來。
2. 應答方刪除加密行，以發出不能或不願進行加密的訊號。

在CUCM上使用正確的SIP規範化指令碼可以緩解此問題。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

相關閱讀

- 思科整合通訊管理員安全指南10.0(1)版
- Cisco Unified Communications Manager最佳化會議和Cisco VCS解決方案指南（版本2.0）
- Cisco Unified Communications Manager with Cisco Expressway（SIP中繼）部署指南（適用於Cisco Expressway X8.2和Unified CM 8.6x和9.x）
- Cisco Unified Communications Manager with Cisco VCS（SIP中繼）部署指南（適用於Cisco VCS X8.2和Unified CM 8.6.x和9.x）
- 通過Cisco VCS的統一通訊移動和遠端訪問部署指南(適用於Cisco VCS X8.2和Cisco Unified CM 9.1(2)SU1或更高版本)
- 通過Cisco Expressway進行統一通訊移動和遠端訪問部署指南(適用於Cisco Expressway X8.2和Cisco Unified CM 9.1(2)SU1或更高版本)
- 技術支援與文件 - Cisco Systems

相關RFC

- RFC 3261 SIP:作業階段啟始通訊協定
- RFC 4566 SDP:作業階段說明通訊協定
- RFC 4568 SDP:安全說明