Esempio di configurazione Secure RTP tra CUCM e VCS o Expressway

Sommario

Introduzione

Questo documento descrive come configurare un RTP (Real-time Transport Protocol) sicuro tra Cisco Video Communication Server (VCS) e Cisco Unified Communications Manager (CUCM).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CUCM

- Cisco VCS o Cisco Expressway

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CUCM
- Cisco VCS o Cisco Expressway

  Nota: In questo articolo vengono utilizzati i prodotti Cisco Expressway a scopo illustrativo, ad eccezione di quanto indicato, ma le informazioni sono valide anche se la distribuzione utilizza Cisco VCS.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Condizioni

- Chiamate SIP (Session Initiation Protocol) instradate tra CUCM ed Expressway
- Crittografia dei supporti (opzionale/ottimizzata) tra Expressway-C e CUCM

Descrizione

Sono state segnalate difficoltà per la configurazione della crittografia dei supporti più efficace per le chiamate SIP instradate tra CUCM e VCS/Expressway. Una configurazione errata comune influisce sulla segnalazione dei supporti crittografati, tramite il protocollo SRTP (Secure Real-time Transport Protocol), che causa il fallimento delle chiamate crittografate nel miglior modo possibile quando il trasporto tra CUCM ed Expressway non è sicuro.

Se il trasporto non è sicuro, la segnalazione di crittografia dei supporti può essere letta da un intercettatore. In questo caso, le informazioni di segnalazione della crittografia dei supporti vengono eliminate dal protocollo SDP (Session Description Protocol). Tuttavia, è possibile configurare CUCM per inviare (e ricevere) segnali di crittografia dei supporti su una connessione non protetta. Per ovviare a questo errore di configurazione, è possibile procedere in due modi, a seconda che le chiamate siano instradate sul lato trunk o sul lato linea a CUCM.

Esempi relativi al lato trunk e al lato linea

Lato trunk: Su CUCM è configurato un trunk SIP verso Expressway. Una zona adiacente corrispondente è configurata in Expressway verso CUCM. Se si desidera che gli endpoint con registrazione VCS siano chiamati (Expressway non è una funzione di registrazione, ma VCS lo è),

è necessario un trunk. Un altro esempio potrebbe essere l'abilitazione dell'interoperabilità H.323 nell'implementazione.

Lato linea: Le chiamate di linea vanno direttamente a CUCM, non tramite trunk. Se tutte le funzionalità di registrazione e controllo delle chiamate vengono fornite da CUCM, la distribuzione potrebbe non richiedere un trunk a Expressway. Ad esempio, se Expressway è distribuito esclusivamente per Mobile e Remote Access (MRA), inoltra le chiamate lato linea dagli endpoint esterni a CUCM.

Strategia di mitigazione

Se esiste un trunk SIP tra CUCM ed Expressway, uno script di normalizzazione sul CUCM riscrive correttamente il SDP in modo che la chiamata di crittografia ottimale non venga rifiutata. Questo script viene installato automaticamente con le versioni più recenti di CUCM, ma se le chiamate crittografate vengono rifiutate, Cisco consiglia di scaricare e installare lo script vcs-interop più recente per la propria versione di CUCM.

Se la chiamata viene effettuata su CUCM, quest'ultimo si aspetta di vedere l'intestazione `x-cisco-srtp-fallback` se la crittografia dei supporti è facoltativa. Se l'intestazione non viene visualizzata, la chiamata viene considerata obbligatoria per la crittografia. Il supporto per questa intestazione è stato aggiunto a Expressway nella versione X8.2, quindi Cisco consiglia X8.2 o versioni successive per MRA (collaboration edge).

Configurazione

Configurazione lato linea

[CUCM]<—massimo sforzo—>[Expressway-C]<—obbligatorio—>[Expressway-E]<—obbligatorio—>[Endpoint]

Per abilitare la crittografia ottimale delle chiamate di linea da Expressway-C a CUCM:

- Utilizzare una soluzione/installazione supportata (ad esempio, MRA)
- Usa protezione in modalità mista in CUCM
- Assicurarsi che Expressway e CUCM si considerino reciprocamente attendibili (l'autorità di certificazione (CA) che firma i certificati di ciascuna parte deve essere considerata attendibile dall'altra parte)
- Utilizza la versione X8.2 o successiva di Expressway
- Usa profili telefonici protetti in CUCM, con la modalità di sicurezza del dispositivo impostata su Autenticato o Crittografato - per queste modalità il tipo di trasporto è TLS (Transport Layer Security)

Configurazione lato trunk

- Utilizzare una soluzione/installazione supportata
- Usa protezione in modalità mista in CUCM
- Assicurarsi che Expressway e CUCM si considerino reciprocamente attendibili (la CA che

firma i certificati di ciascuna parte deve essere considerata attendibile dall'altra parte)
- Scegliere la modalità di crittografia migliore e TLS come trasporto nella zona adiacente da Expressway a CUCM (questi valori vengono prepopolati automaticamente nel case di linea)
- Selezionare TLS come trasporto in entrata e in uscita nel profilo di sicurezza trunk SIP
- Controllare se SRTP è consentito (vedere l'istruzione Caution) sul trunk SIP da CUCM a Expressway
- Cercare e applicare, se necessario, lo script di normalizzazione corretto per le versioni di CUCM ed Expressway

Attenzione: Se si seleziona la casella di controllo SRTP consentito, Cisco consiglia di utilizzare un profilo TLS crittografato in modo che le chiavi e altre informazioni relative alla sicurezza non vengano esposte durante le negoziazioni delle chiamate. Se si utilizza un profilo non sicuro, l'SRTP funzionerà comunque. Tuttavia, le chiavi verranno esposte nella segnalazione e nelle tracce. In tal caso, è necessario garantire la sicurezza della rete tra CUCM e il lato di destinazione del trunk.

Opzioni di crittografia dei supporti

Nessuna

Crittografia non consentita. Le chiamate che richiedono la crittografia devono avere esito negativo perché non possono essere protette. CUCM ed Expressway sono coerenti nella segnalazione per questo caso.

CUCM ed Expressway utilizzano entrambi `m=RTP/AVP` per descrivere i supporti nel SDP. Non ci sono attributi crypto (nessuna riga `a=crypto...` nelle sezioni media di SDP).

Obbligatorio

Crittografia dei supporti necessaria. Le chiamate non crittografate devono sempre avere esito negativo; fallback non consentito. CUCM ed Expressway sono coerenti nella segnalazione per questo caso.

CUCM ed Expressway utilizzano entrambi `m=RTP/SAVP` per descrivere i supporti nel SDP. L'SDP dispone di attributi di crittografia (`a=crypto...` righe nelle sezioni dei supporti dell'SDP).

Best-effort

Le chiamate che possono essere crittografate vengono crittografate. Se non è possibile stabilire la crittografia, le chiamate potrebbero e dovrebbero tornare a supporti non crittografati. In questo caso, CUCM ed Expressway non sono coerenti.

Expressway rifiuta sempre la crittografia se il trasporto è TCP (Transmission Control Protocol) o UDP (User Datagram Protocol). Se si desidera la crittografia dei supporti, è necessario proteggere il trasporto tra CUCM ed Expressway.

SDP (come scrive CUCM): I supporti crittografati sono descritti come `m=RTP/SAVP` e `a=crypto` le righe sono scritte nel SDP. Questa è la segnalazione corretta per la crittografia dei supporti, ma le linee crittografiche sono leggibili se il trasporto non è sicuro.

Se CUCM vede l'intestazione `x-cisco-srtp-fallback`, permette alla chiamata di tornare alla modalità non crittografata. Se l'intestazione è assente, CUCM presume che la chiamata richieda la crittografia (non consente il fallback).

A partire da X8.2, Expressway fa lo stesso sforzo di CUCM nel caso line-side.

SDP (mentre Expressway scrive sul lato trunk): I supporti crittografati sono descritti come `m=RTP/AVP` e `a=crypto` le righe vengono scritte nel SDP.

Tuttavia, ci sono due motivi per cui le righe a=crypto potrebbero essere assenti:

1. Quando un hop di trasporto da o verso il proxy SIP su Expressway non è sicuro, il proxy elimina le linee crittografiche in modo da evitare che vengano esposte sull'hop non sicuro.
2. La parte che risponde rimuove le linee crittografiche per segnalare che non può o non vuole eseguire la crittografia.

L'uso dello script di normalizzazione SIP corretto su CUCM riduce questo problema.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

Lettura correlata

- Guida alla sicurezza di Cisco Unified Communications Manager, versione 10.0(1)
- Guida alle soluzioni Optimized Conferencing per Cisco Unified Communications Manager e Cisco VCS (versione 2.0)
- Guida all'installazione di Cisco Unified Communications Manager con Cisco Expressway (SIP Trunk) (per Cisco Expressway X8.2 e Unified CM 8.6x e 9.x)
- Guida all'installazione di Cisco Unified Communications Manager con Cisco VCS (SIP Trunk) (per Cisco VCS X8.2 e Unified CM 8.6.x e 9.x)
- Unified Communications Mobile and Remote Access tramite Cisco VCS Deployment Guide (per Cisco VCS X8.2 e Cisco Unified CM 9.1(2)SU1 o versioni successive)
- Unified Communications Mobile and Remote Access tramite Cisco Expressway Deployment

Guide (per Cisco Expressway X8.2 e Cisco Unified CM 9.1(2)SU1 o versioni successive)
- Documentazione e supporto tecnico – Cisco Systems

RFC correlate

- RFC 3261 SIP: Session Initiation Protocol
- RFC 4566 SDP: Session Description Protocol
- RFC 4568 SDP: Descrizioni protezione