

Configuration de l'interfonctionnement SRTP-RTP sur CUBE

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Assistance pour services supplémentaires](#)

[Configurations](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit un processus étape par étape sur la façon de configurer l'interfonctionnement SRTP-RTP sur CUBE.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Border Element (CUBE)
- Protocole d'ouverture de session (SIP)
- TLS (Transport Layer Security)
- Protocole RTP (Real-time Transport Protocol)
- Secure Media : protocole SRTP (Secure Real-time Transport Protocol)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Unified Border Element (CUBE)
- Cisco IOS XE - versions 17.6 et ultérieures
- Cisco C8200-1N-4T

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La fonctionnalité Cisco Unified Border Element (CUBE) Support for SRTP-RTP Interworking connecte les domaines d'entreprise SRTP aux liaisons SIP du fournisseur de SIP RTP.

L'interfonctionnement SRTP-RTP connecte les réseaux d'entreprise RTP avec SRTP sur un réseau externe entre les entreprises. Cela permet des communications interentreprises sécurisées et flexibles, sans tunnels IPsec statiques ni déploiement SRTP au sein de l'entreprise.

Les points clés de l'interopérabilité SRTP-RTP sur CUBE sont les suivants :

1. Chiffrement et déchiffrement : CUBE peut chiffrer et déchiffrer des flux de données vers et depuis des réseaux SRTP et RTP.
2. Prise en charge TLS : la sécurité de la couche transport (TLS) peut être activée ou désactivée entre le serveur SCCP et le client SCCP. Par défaut, TLS est activé pour protéger les clés SRTP.
3. Services supplémentaires : dans Cisco IOS version 15.2(1), la fonctionnalité a été étendue pour prendre en charge des services supplémentaires sur CUBE.
4. Transcodage : l'interconnexion SRTP-RTP est disponible avec des transcodeurs normaux et universels, appelés à l'aide de la messagerie SCCP.
5. Gestion de secours : si l'un des terminaux d'appel ne prend pas en charge le protocole SRTP, l'appel peut revenir à RTP-RTP ou échouer, selon la configuration. Ce fallback se produit uniquement si la commande `srtp fallback` est configurée sur le terminal de numérotation `dial-peer` correspondant.
6. Déploiement : l'interconnexion SRTP à RTP peut être déployée sur les interfaces UNI (User to Network Interfaces) et NNI (Network to Network Interfaces).

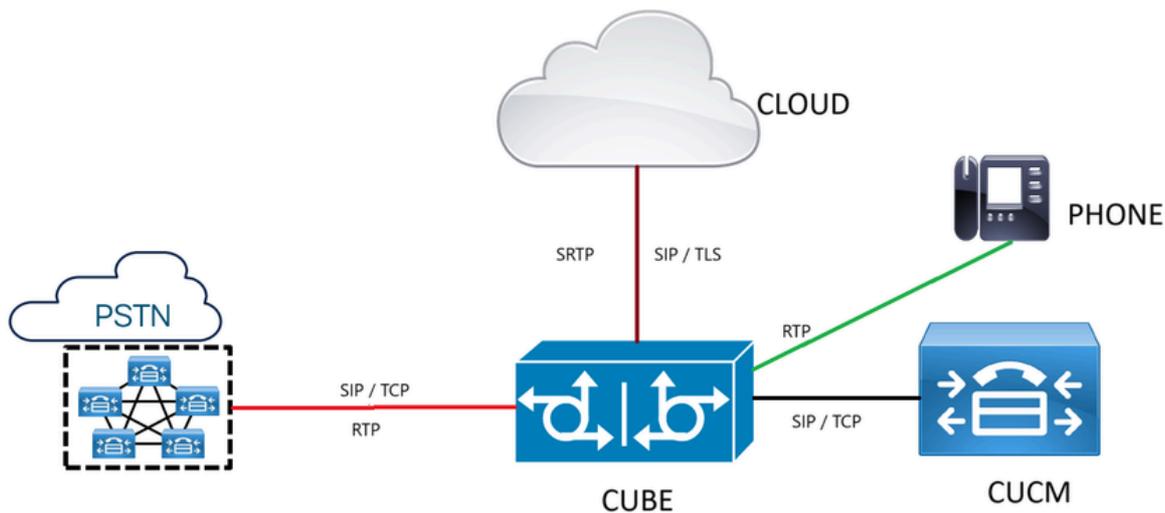


Remarque :

- Les ressources DSP sont requises pour les plates-formes exécutées sur les versions de Cisco IOS.
- Les plates-formes exécutées sur les versions Cisco IOS XE ne nécessitent pas de ressources DSP.

Configurer

Diagramme du réseau



Assistance pour services supplémentaires

Les services supplémentaires pris en charge sont :

- Modification du codec Midcall avec configuration du codec de classe vocale
- Mise en attente et reprise d'un appel sur invitation
- Musique d'attente (MoH) appelée à partir de Cisco Unified Communications Manager (Cisco UCM), où le tronçon d'appel change entre SRTP et RTP pour une source de musique d'attente
- Renvoi et transfert d'appels sur invitation
- Transfert d'appel basé sur un message REFER, avec consommation locale ou transmission du message REFER sur le CUBE
- Transfert d'appel basé sur un message 302, avec consommation locale ou transfert du message 302 sur le CUBE
- commutation de fax T.38
- Basculement fax Pass-Through

Pour les transferts d'appels impliquant des messages REFER et 302 (messages qui sont consommés localement sur CUBE), la renégociation de média de bout en bout est initiée à partir de CUBE uniquement lorsque vous configurez la commande `additional-service media-renegotiate` en mode de configuration `voice service voip`.

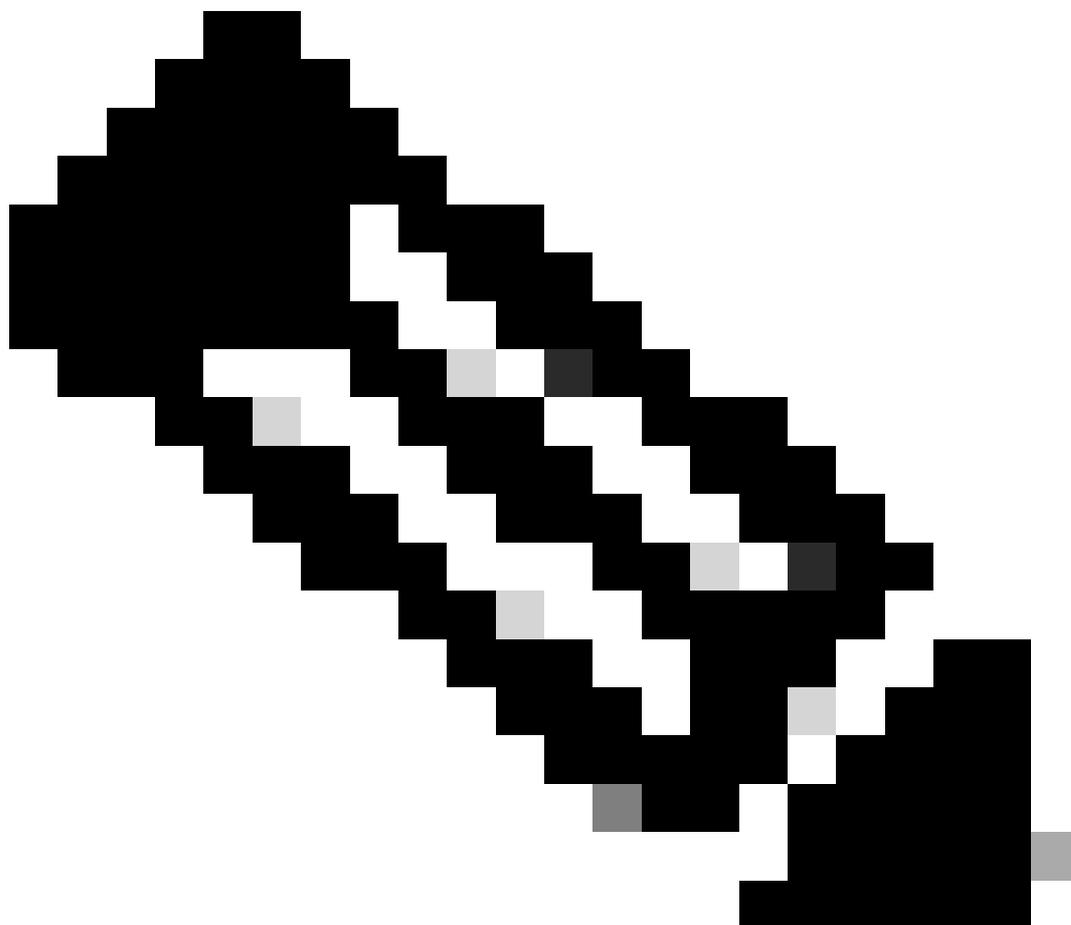
Tout flux d'appels dans lequel il y a une commutation de RTP à SRTP sur le même tronçon d'appel SIP nécessite la commande `additional-service media-renegotiate` activée en mode de configuration globale ou `voip` du service vocal pour s'assurer qu'il y a un audio bidirectionnel.

Exemples de flux d'appels :

- RTP - Transfert SRTP côté CUCM
- attente musicale non sécurisée exécutée pendant la mise en attente ou la reprise d'un appel sécurisé ;

Lorsque des services supplémentaires sont appelés à partir des points d'extrémité, l'appel peut

basculer entre SRTP et RTP pendant la durée de l'appel. Par conséquent, Cisco vous recommande de configurer de telles liaisons SIP pour la reprise SRTP.



Remarque : à partir de la version 16.5.1b de Cisco IOS XE Everest, ces suites de chiffrement sont activées par défaut sur la branche SRTP :

- AEAD_AES_256_GCM
- AEAD_AES_128_GCM
- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32

Configurations

Étape 1. Activez SRTP et configurez Dial-Peer pour le tronçon SRTP : il s'agit du tronçon où SRTP est requis.

```
dial-peer voice <tag> voip
```

```
description Homologue de numérotation SRTP entrant
destination-pattern <pattern>
session protocol sipv2
session target ipv4 :<SRTP-Peer-IP-Address>
voice-class codec 1
srtp
dtmf-relay rtp-net
signalisation ip qos dscp cs3
!
```

Étape 2. Configurer le terminal de numérotation dial-peer pour la branche RTP : il s'agit de la branche où RTP est requis.

```
dial-peer voice <tag> voip
description Dial-Peer RTP sortant
destination-pattern <pattern>
session protocol sipv2
session target ipv4 :<RTP-Peer-IP-Address>
voice-class codec 1
dtmf-relay rtp-net
signalisation ip qos dscp cs3
!
```

Étape 3. Configurer l'authentification cryptographique

Étapes de configuration de CUBE pour la prise en charge d'une connexion SRTP à l'aide de la suite de chiffrement AES_CM_128_HMAC_SHA1_80

- Configuration du niveau dial-peer

```
dial-peer voice <tag> voip
    voice-class sip srtp-auth sha1-80
!
```

- Configuration de niveau global

voix sur IP

sip

srtp-auth sha1-80

!

- Configuration au niveau de la classe vocale

voice class srtp-crypto 3000

crypto 1 AES_CM_128_HMAC_SHA1_80

crypto 2 AES_CM_128_HMAC_SHA1_32

!

Étape 4. Enable SRTP Fallback : vous pouvez configurer SRTP avec l'option de secours afin qu'un appel puisse revenir à RTP si SRTP n'est pas pris en charge par l'autre extrémité de l'appel. L'activation de la reprise SRTP est requise pour la prise en charge de services supplémentaires non sécurisés tels que la musique d'attente, le renvoi d'appels et le transfert d'appels.

- En mode de configuration dial-peer

dial-peer voice <tag> voip

srtp fallback (pour interagir avec des périphériques autres que Cisco Unified Communications Manager)

ou

voice-class sip srtp negotiation cisco (Activez cette CLI avec la commande srtp fallback pour prendre en charge la reprise SRTP avec Cisco Unified Communications Manager)

- En mode de configuration VoIP SIP globale

voix sur IP

sip

srtp fallback (pour interagir avec des périphériques autres que Cisco Unified Communications Manager)

ou

srtp negotiation cisco (Activez cette interface de ligne de commande avec la commande srtp fallback pour prendre en charge la reprise SRTP avec Cisco Unified Communications Manager)

Exemple de configuration :

Voici un exemple consolidé de configuration :

```
voice class srtp-crypto 300
  crypto 1 AES_CM_128_HMAC_SHA1_80
  crypto 2 AES_CM_128_HMAC_SHA1_32
!
dial-peer voice 100 voip
  description Homologue de numérotation SRTP entrant
  modèle de destination 1234
  session protocol sipv2
  session target ipv4:192.0.2.1
  voice-class codec 1
  voice-class sip srtp
  dtmf-relay rtp-net
  srtp
  voice-class sip srtp-crypto 300
  signalisation ip qos dscp cs3
!
dial-peer voice 200 voip
  description Dial-Peer RTP sortant
  modèle de destination 5678
  session protocol sipv2
  session target ipv4:192.0.2.2
  voice-class codec 1
  dtmf-relay rtp-net
  signalisation ip qos dscp cs3
!
```

Vérifier

Exécutez la commande pendant un appel actif pour vérifier les tronçons SRTP et RTP.

```
CUBE# show call active voice brief
```

Tronçons d'appel de téléphonie : 0

Tronçons d'appel SIP : 2

Tronçons d'appel H323 : 0

Tronçons d'appel contrôlés par l'agent d'appel : 0

Tronçons d'appel SCCP : 0

tronçons d'appel multidiffusion : 0

Nombre total de tronçons d'appel : 2

```
0 : 1 12:49:45.256 IST ven. 19 oct. 2024.1 +29060 pid:1 Answer 10008001 connected
```

```
dur 00:01:19 tx:1653/271092 rx:2831/464284 dscp:0 media:0
```

```
IP XX.XX.XX.XX:7892 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:  
off
```

```
media inactive detected:n media control rcvd:n/a timestamp:n/a
```

```
appel de longue durée détecté:n durée d'appel de longue durée:n/a horodatage:n/a
```

```
0 : 2 12:49:45.256 IST ven. 19 oct. 2024.2 +29060 pid:22 Origine 20009001 connecté
```

```
dur 00:01:19 tx:2831/452960 rx:1653/264480 dscp:0 media:0
```

```
IP XX.XX.XX.XX:7893 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:  
off
```

```
media inactive detected:n media control rcvd:n/a timestamp:n/a
```

```
appel de longue durée détecté:n durée d'appel de longue durée:n/a horodatage:n/a
```

Dépannage

Vous devez collecter ces débogages et ces journaux afin d'examiner s'il y a des problèmes d'interfonctionnement.

- debug ccsip all
- debug voip ccapi inout
- debug voip srtp packet

- debug voip srtp error
- debug voip srtp session
- Captures de paquets

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.