Connaître les bases des protocoles de voix sur IP pour un pare-feu sécurisé

Table des matières

Introduction

Ce document décrit les principes fondamentaux de divers protocoles VoIP pour aider les ingénieurs à les dépanner efficacement sur les pare-feu sécurisés.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document est destiné à être utilisé dans des scénarios de dépannage avec les périphériques suivants :

- Protection pare-feu contre les menaces (FTD)
- Dispositif de sécurité adaptatif de pare-feu sécurisé (ASA)

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.

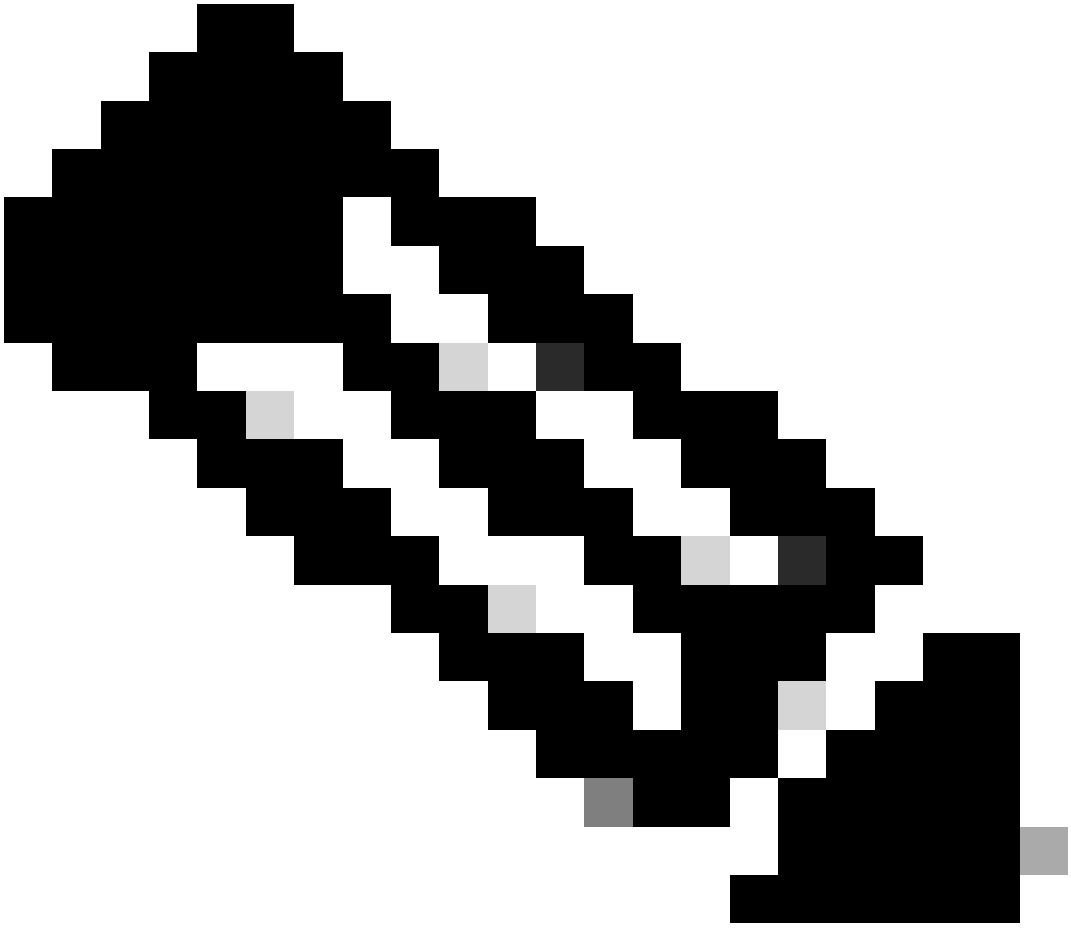
Notions de base sur VoIP

La communication est fondamentale pour les interactions humaines. Les protocoles VoIP (Voice over IP) sont devenus indispensables pour la communication humaine. C'est pourquoi il est important de connaître leurs parties lors du dépannage d'un scénario qui inclut un pare-feu (FW).

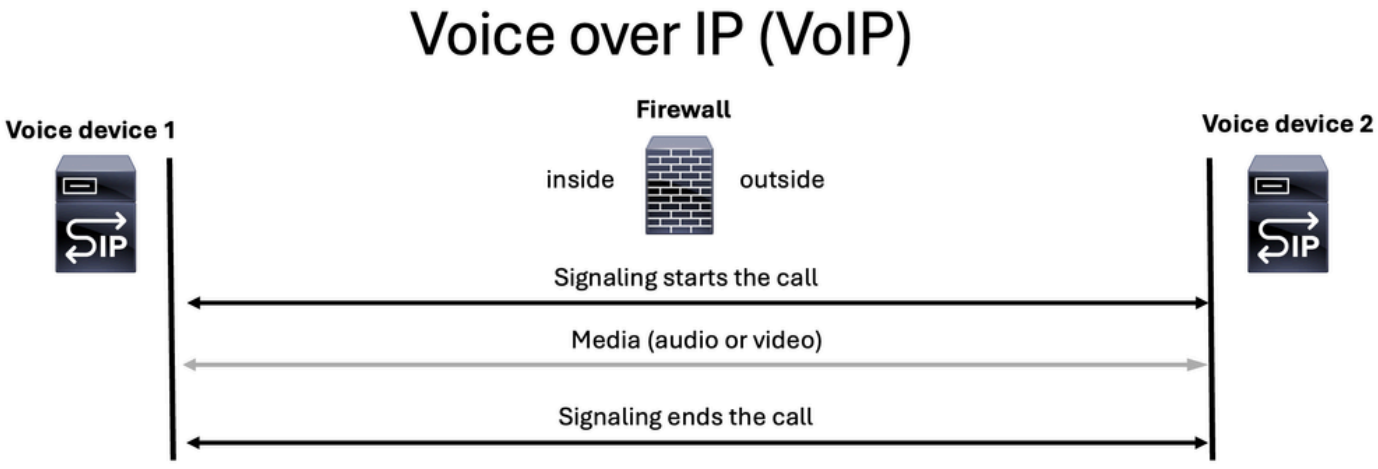
La VoIP se compose de deux parties :

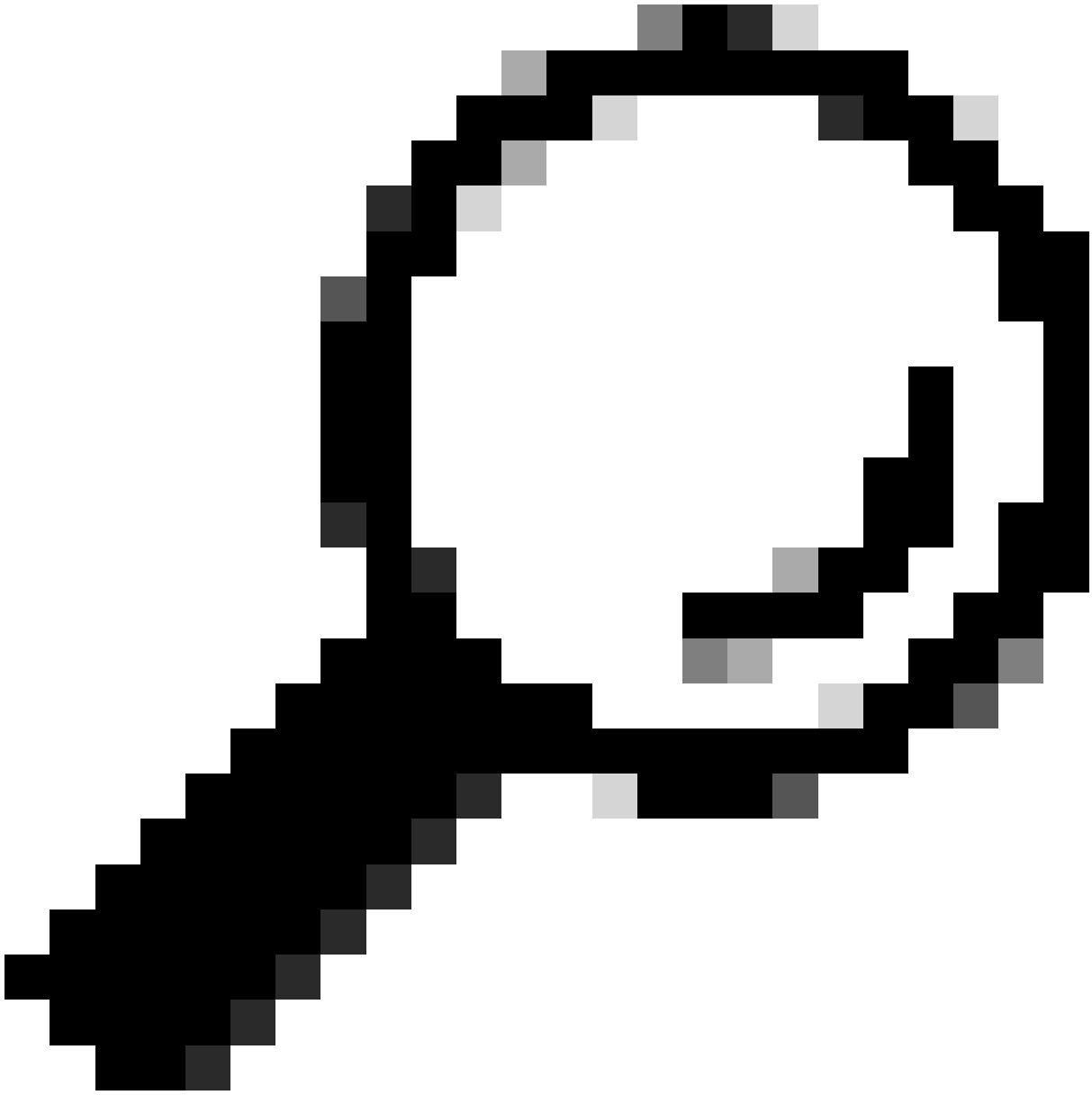
- Signalisation
- Média (voix ou vidéo)

Les communications VoIP commencent toujours par une partie de signalisation pour démarrer un appel, puis le média (voix ou vidéo) est diffusé en continu et enfin la signalisation met fin à l'appel.

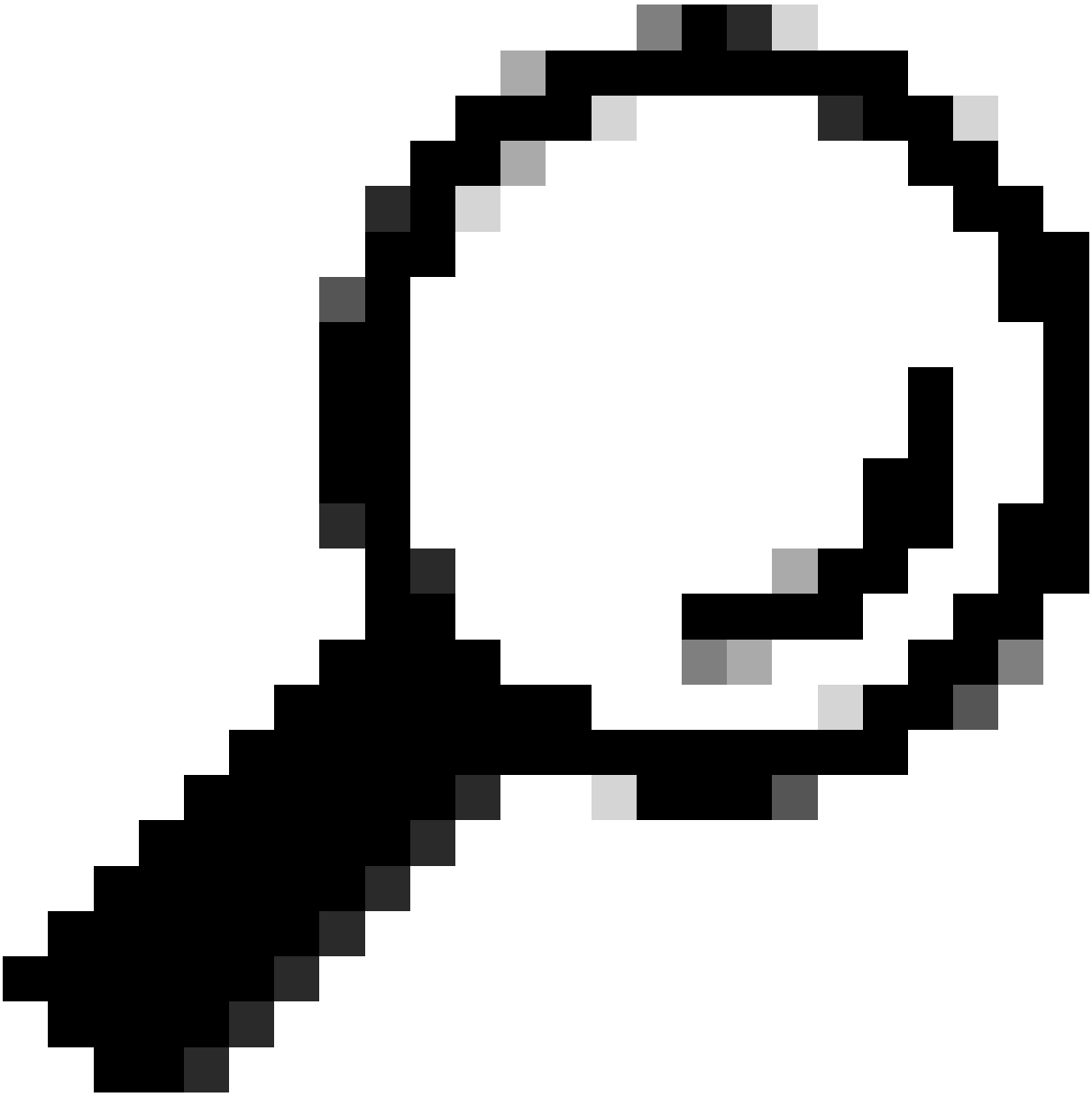


Remarque : Le protocole SIP est le protocole le plus utilisé. Il est donc représenté de manière cohérente comme l'icône du serveur vocal SIP dans la plupart des schémas.





Conseil : Lors du dépannage d'un problème vocal pour ASA ou FTD, il est essentiel d'examiner le scénario du point de vue de l'utilisateur. Vous devez déterminer si l'appel est établi ou s'il n'y a pas d'audio ou d'audio unidirectionnel. Ces informations fournissent des indications précieuses sur la question de savoir si le problème est lié au protocole de signalisation ou au protocole multimédia (voix ou vidéo).



Conseil : Un périphérique vocal peut gérer simultanément le trafic RTP (Real-time Transport Protocol) vocal, le trafic de signalisation ou les deux. Lors du dépannage des problèmes vocaux, il est essentiel de se rappeler ces principaux concepts :

++Serveurs de signalisation : Ces serveurs sont chargés de gérer uniquement le trafic de signalisation.

++Serveurs multimédia : Ces serveurs gèrent exclusivement le trafic RTP vocal.

++Certains périphériques peuvent gérer les deux tâches.

Signalisation

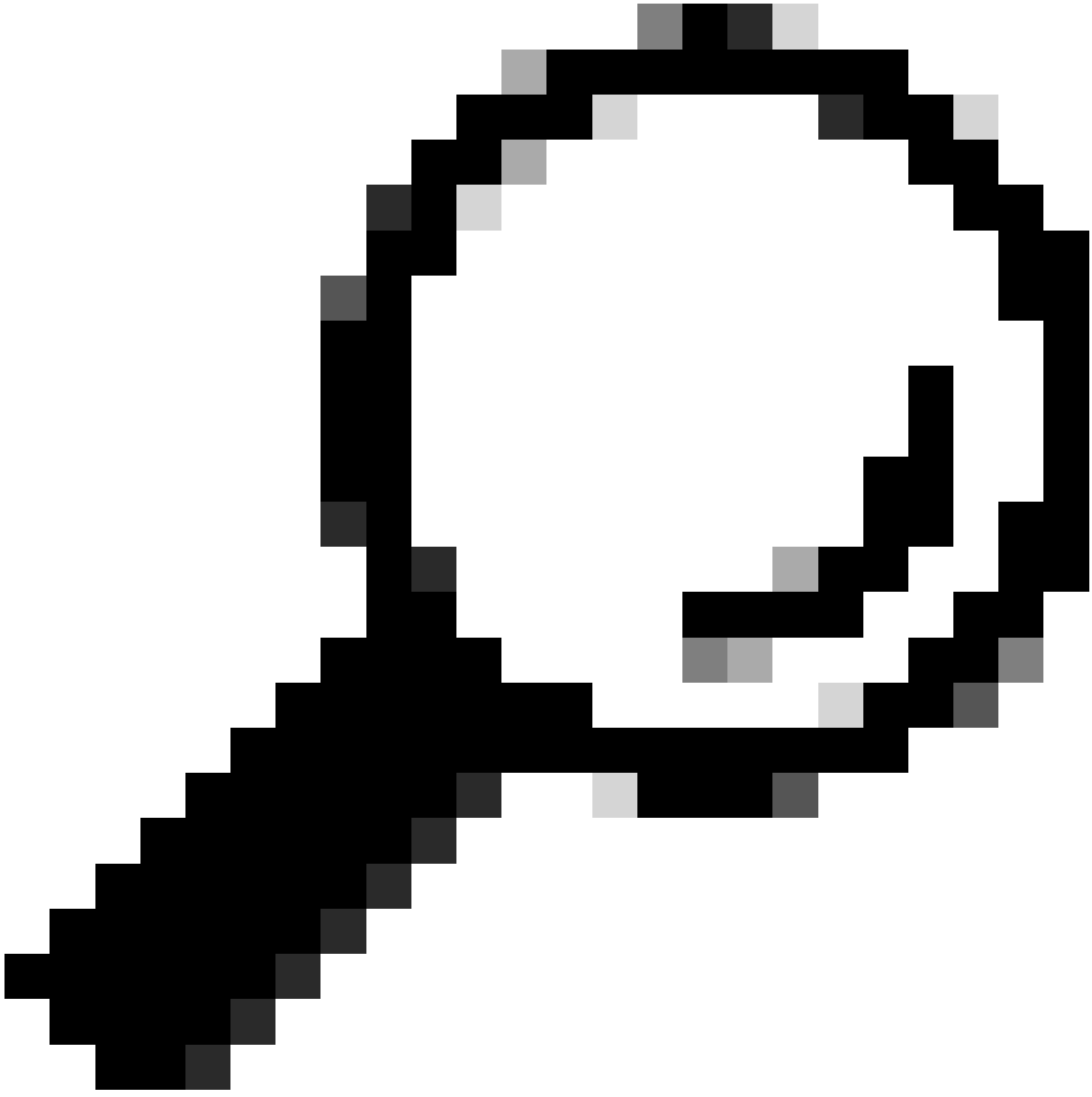
Le protocole de signalisation est la partie d'un appel qui démarre la communication vocale, mais il

remplit également les fonctions suivantes :

- Maintient la communication.
- Modifie la communication.
- Termine la communication.

Différents types de protocoles de signalisation permettent d'établir un appel. Les plus courants sont les suivants :

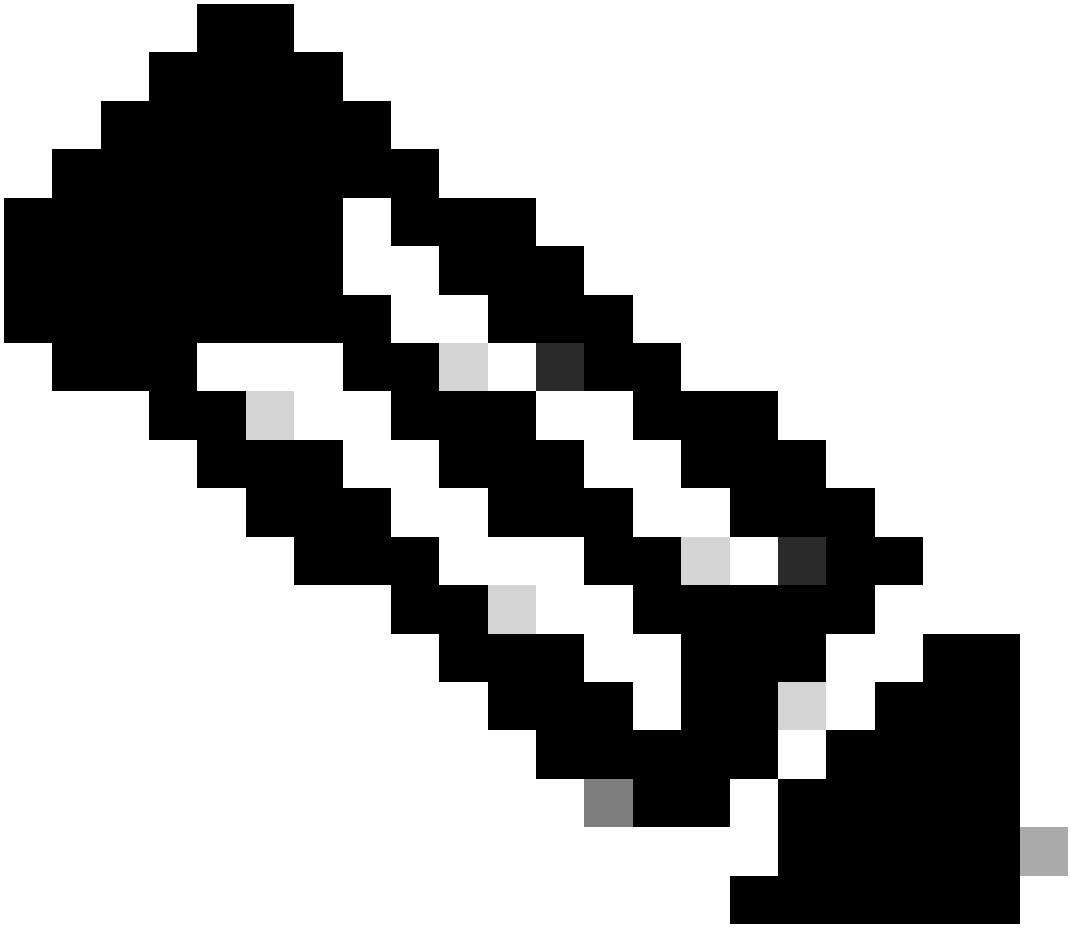
- Protocole d'ouverture de session (SIP)
- H.323
- Protocole MGCP (Media Gateway Control Protocol)
- Protocole SCCP (Skinny Call Control Protocol)



Conseil : Il est essentiel d'identifier le protocole de signalisation utilisé pour déterminer les

---

ports appropriés pour la capture de paquets sur ASA ou FTD. En outre, la topologie du flux d'appels et du réseau est utile pour comprendre le chemin de signalisation.

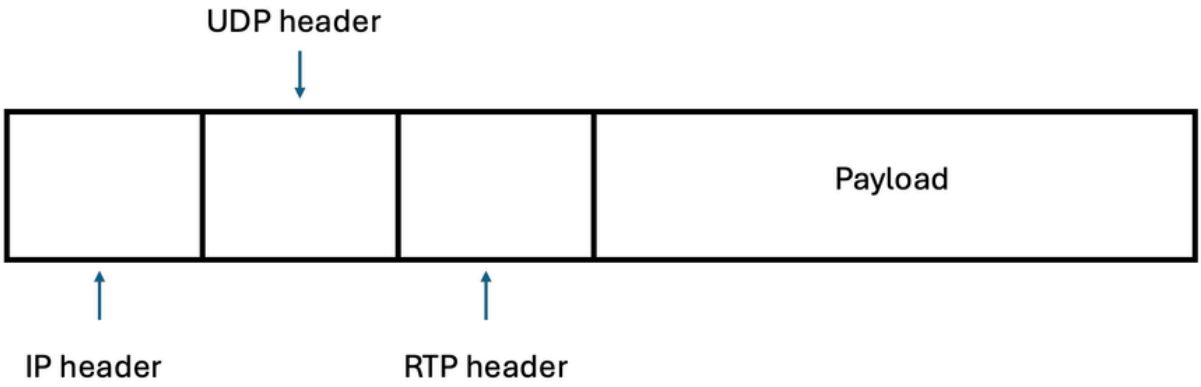


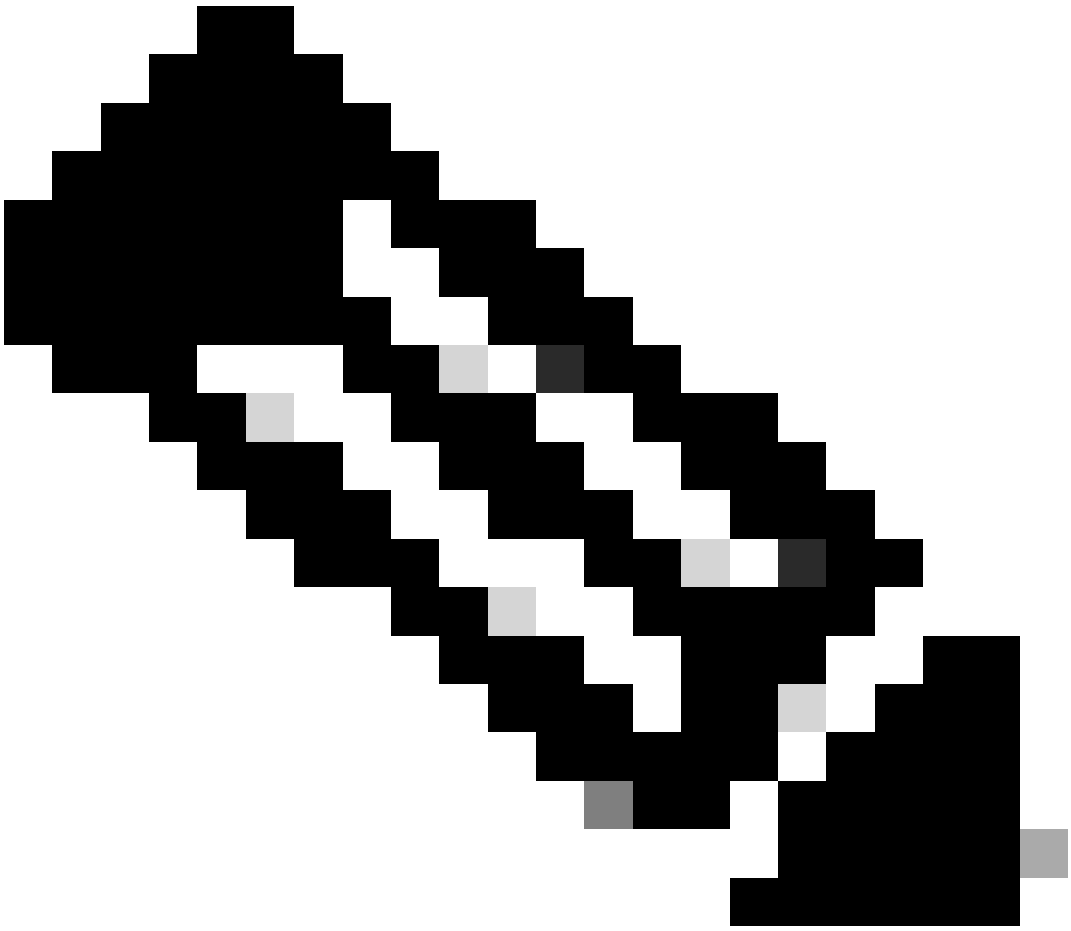
Remarque : Les paquets de signalisation comprennent les adresses IP source et de destination, ce qui facilite l’identification des parties impliquées dans l’envoi et la réception du flux de média RTP.

médias

Lorsque la signalisation est terminée et que les composants de signalisation (périphériques ou serveurs) s'accordent sur le type de support, le protocole RTP (Real Time Protocol) entre en jeu pour commencer à envoyer des supports (audio et/ou vidéo) à toutes les parties concernées.

Le protocole RTP est un protocole Internet utilisé pour la transmission multimédia en continu qui est envoyé uniquement après l'établissement de l'appel et qui s'exécute sur le protocole UDP (User Datagram Protocol).

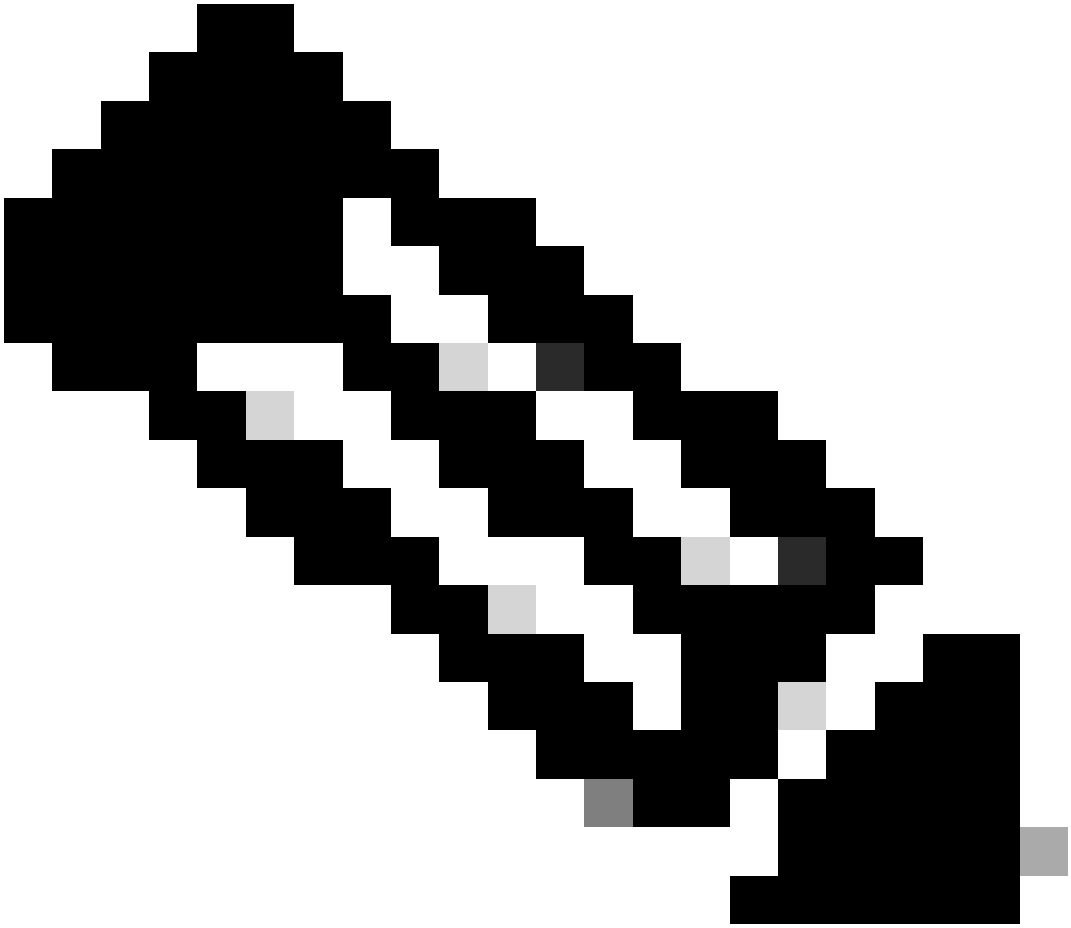




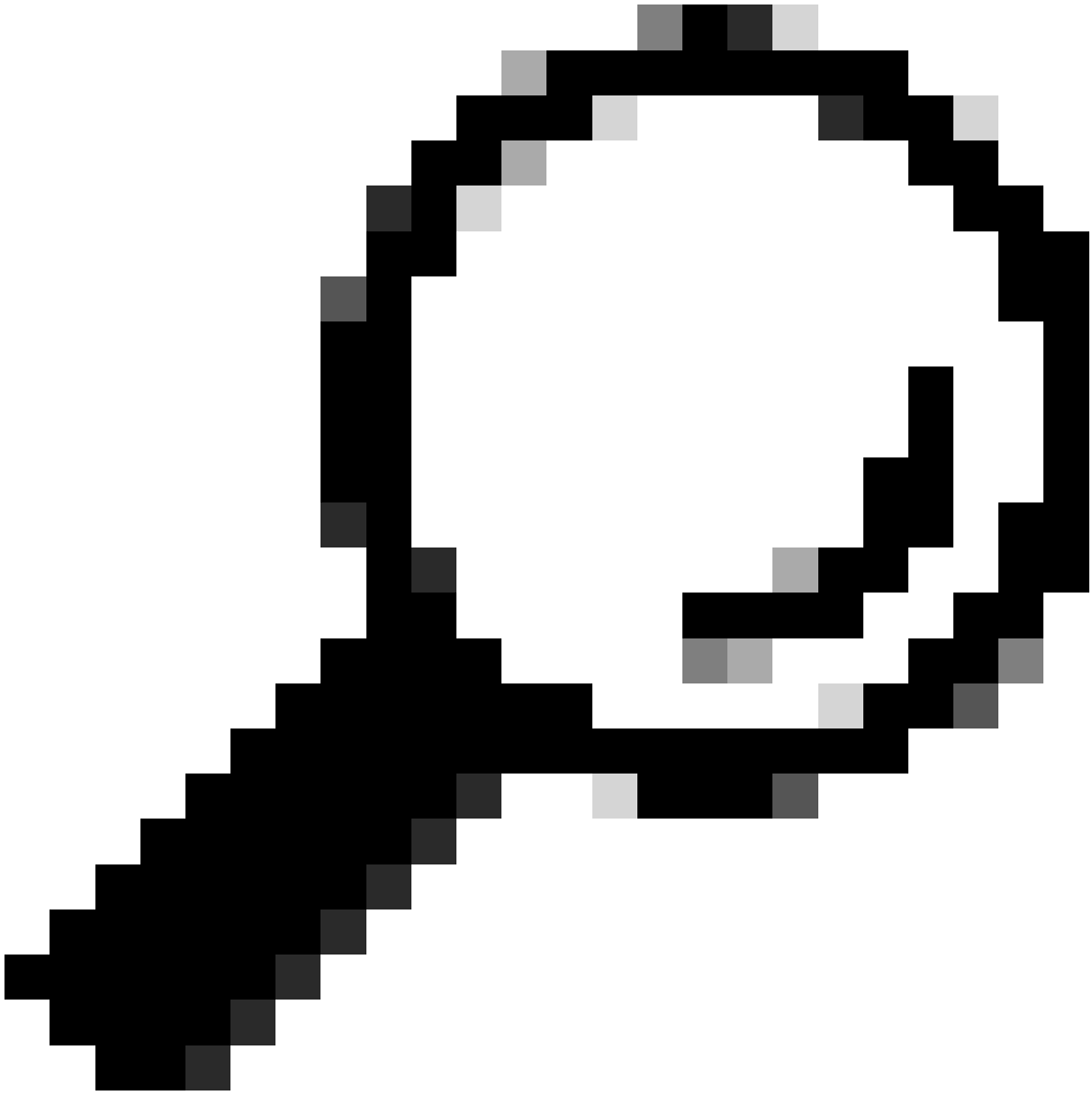
Remarque : Les supports peuvent être vocaux et/ou vidéo et se propagent sur des paquets RTP.

Les composants de signalisation (périphériques ou serveurs) déterminent les ports utilisés pour l'envoi ou la réception de supports (audio et/ou vidéo). La plage de ports la plus courante pour le

protocole RTP est généralement comprise entre 16384 et 32767 pour la plupart des périphériques.



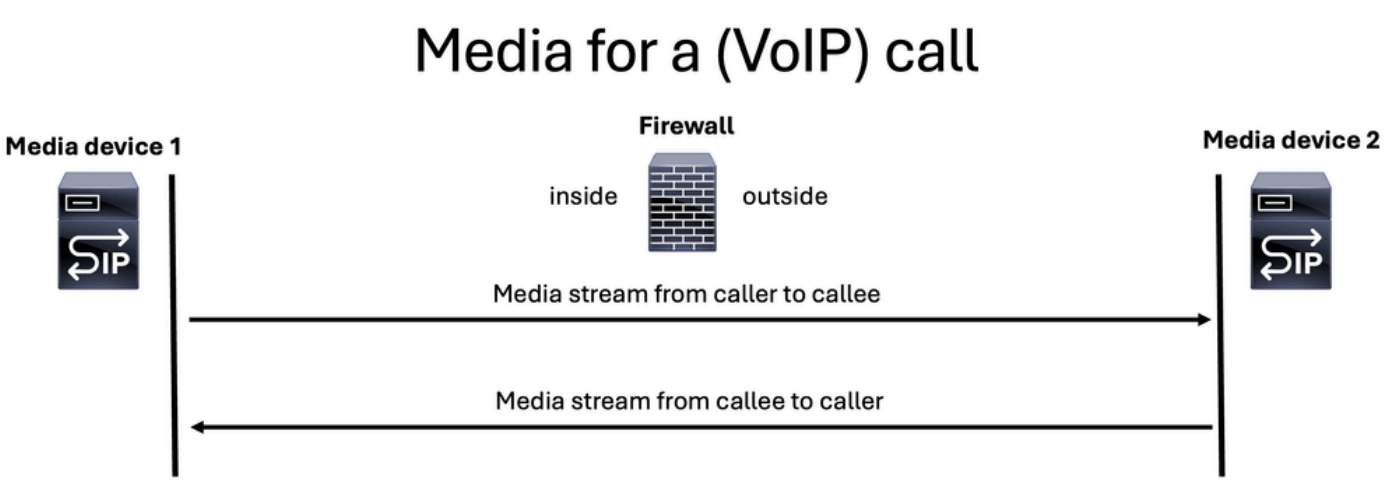
Remarque : Certains périphériques Cisco, tels que les plates-formes ASR et ISR G3, comme la plate-forme ISR4K, utilisent une plage de ports RTP normalisée de 8 000 à 48200. Il est essentiel de vérifier la plage de ports RTP spécifique configurée sur vos périphériques, car elle peut différer de ces valeurs normalisées et varier d'un périphérique tiers à l'autre.

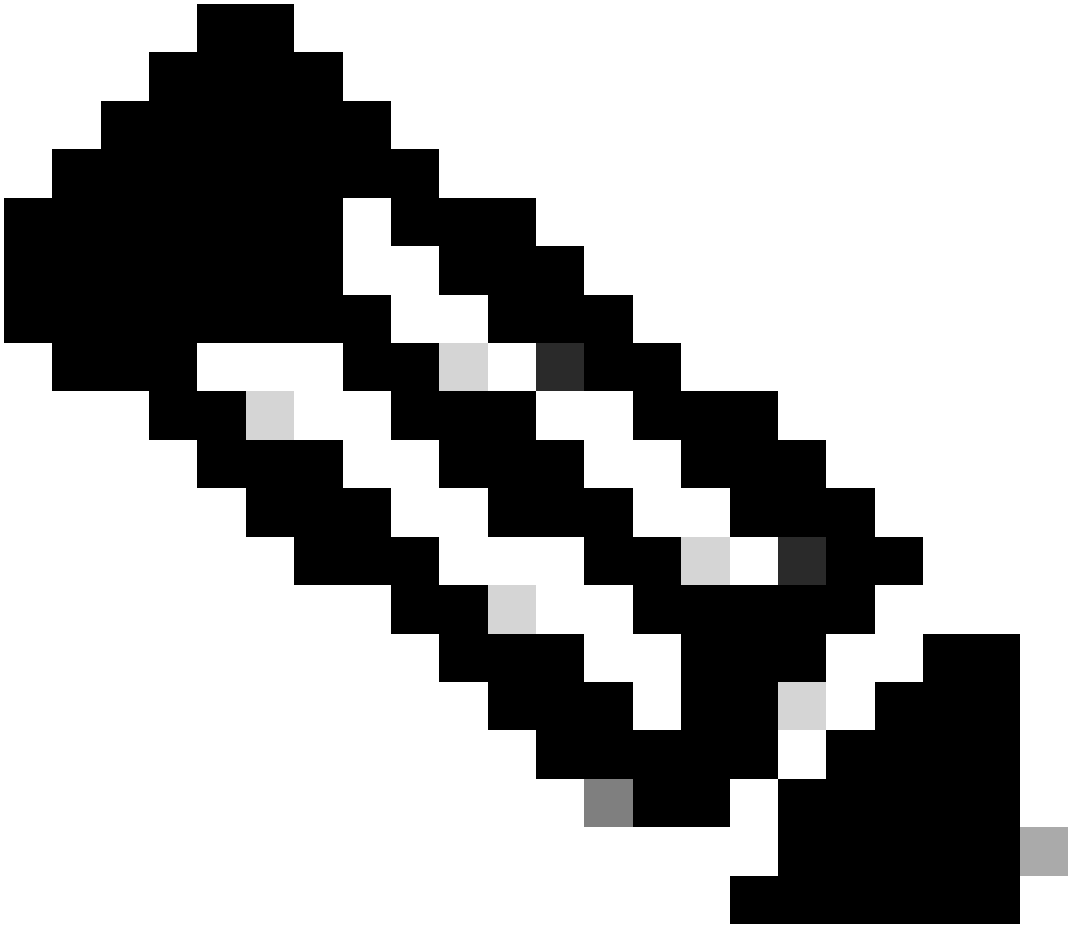


Conseil : Parfois, le chemin RTP diffère du chemin de signalisation, ce qui rend crucial l'identification des périphériques responsables de l'envoi et de la réception des paquets RTP vocaux. Cela garantit que vous capturez le trafic UDP entre les périphériques traversant l'ASA ou le FTD.

Il existe deux flux multimédias ou flux RTP qui sont générés sur un appel vocal normal :

1. Un flux multimédia de l'appelant à l'appelé
2. Un flux multimédia d'un appelant à l'autre





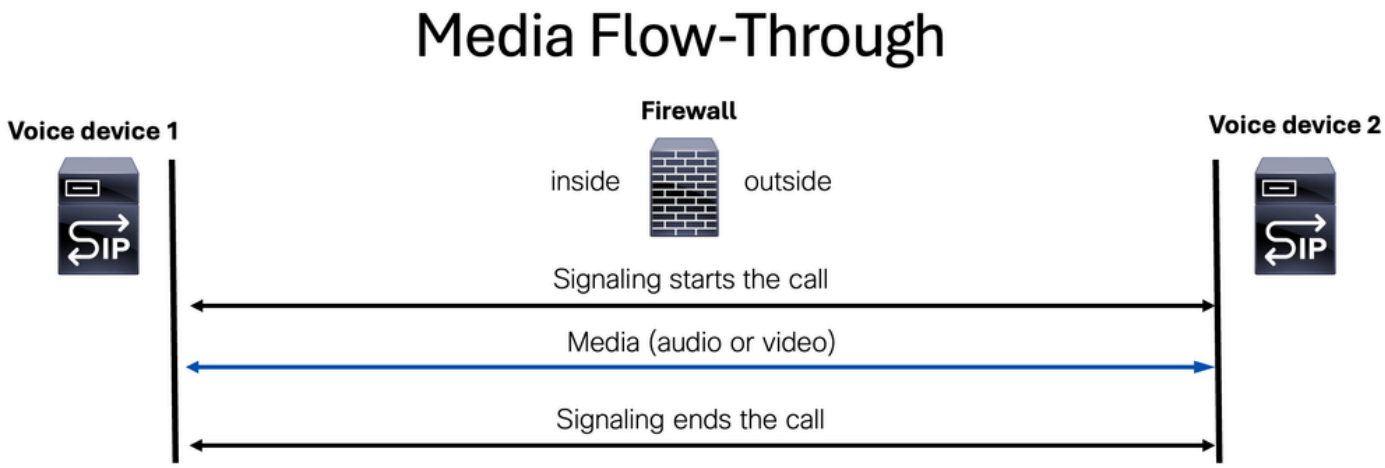
Remarque : À des fins d'illustration, l'icône du serveur SIP est utilisée pour représenter un serveur de signalisation ou un serveur multimédia dans toutes les images.

Lorsque vous abordez la diffusion multimédia en continu dans un appel vocal, il est important de mettre en évidence deux scénarios clés :

1. Flux multimédia en transit
2. Circulation Multimédia

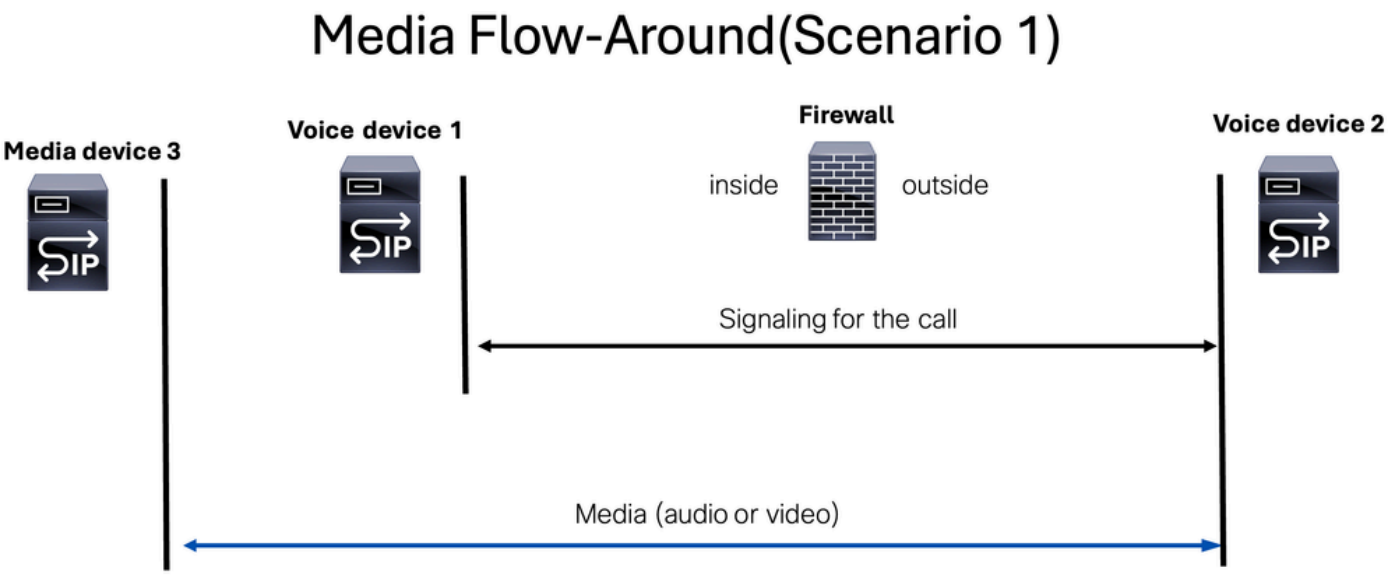
Flux multimédia en transit

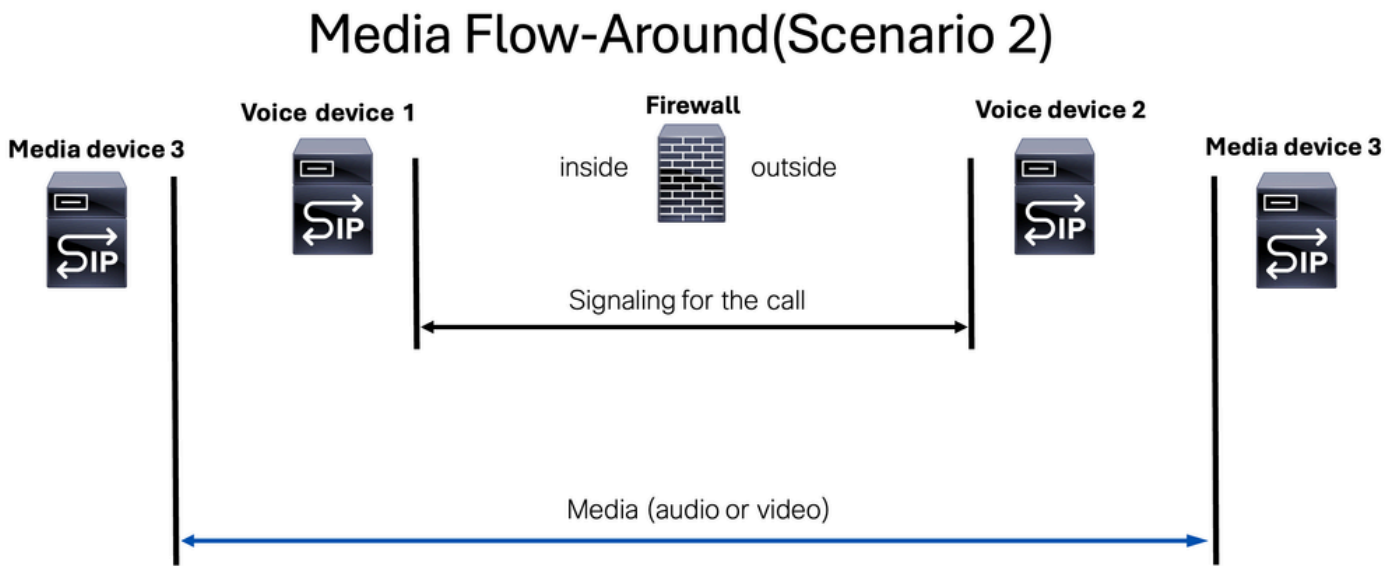
Le flux de données multimédia est un mode dans lequel les données multimédias (voix et/ou vidéo) et les paquets de signalisation sont traités par le même périphérique.



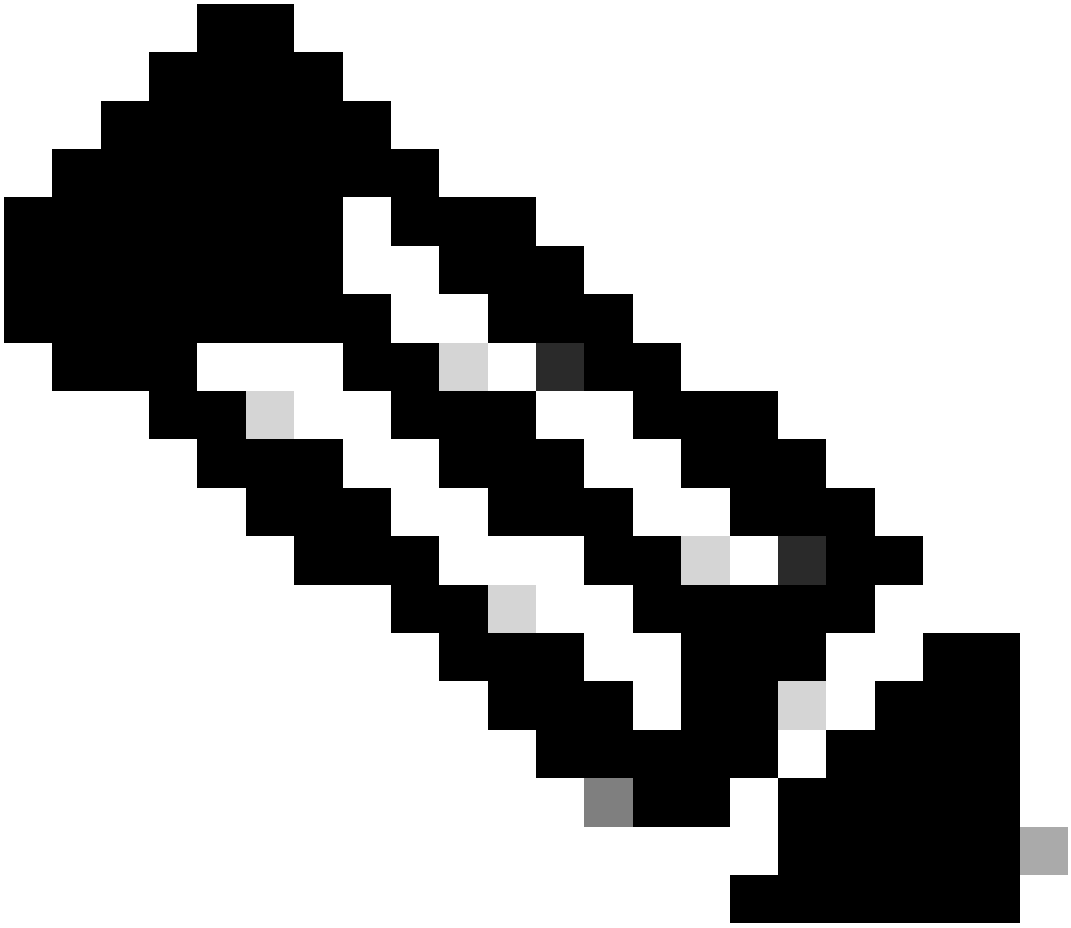
Circulation Multimédia

Le flux de données multimédia est un mode dans lequel les paquets de signalisation sont gérés par deux composants de signalisation distincts (périphériques ou serveurs), tandis que le flux de données multimédia (voix ou vidéo) est géré par un troisième périphérique appelé périphérique multimédia.





Ce mode clarifie les rôles des périphériques impliqués et la distinction entre la signalisation et les flux ou périphériques multimédias.



Remarque : Ceci est particulièrement important à mentionner lorsque le dépannage de la liste d'accès créée pourrait permettre les composants de signalisation (périphériques ou serveurs), mais si le flux de média utilise un autre périphérique de média, nous devons l'autoriser également sur la liste d'accès de notre périphérique de pare-feu.

Protocole d'ouverture de session (SIP)

SIP est un protocole de contrôle de couche application défini par l'IETF (Internet Engineering Task Force) dans la RFC 3261.

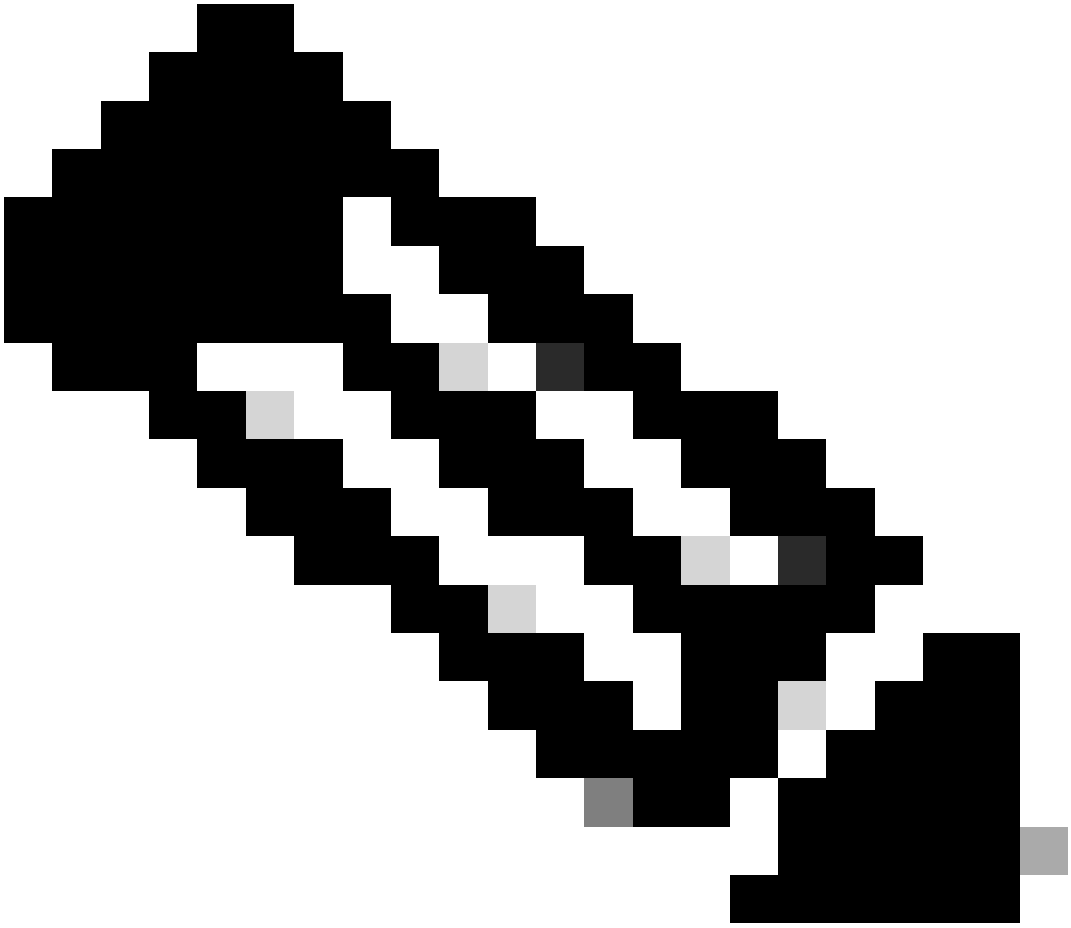
SIP est un protocole de type texte. Cela signifie que les messages SIP sont composés d'un texte lisible par l'utilisateur, de la même manière que le protocole HTTP fonctionne.

Le protocole SIP est conçu pour traiter les fonctions de signalisation et de gestion de session au sein d’un réseau de téléphonie par paquets.

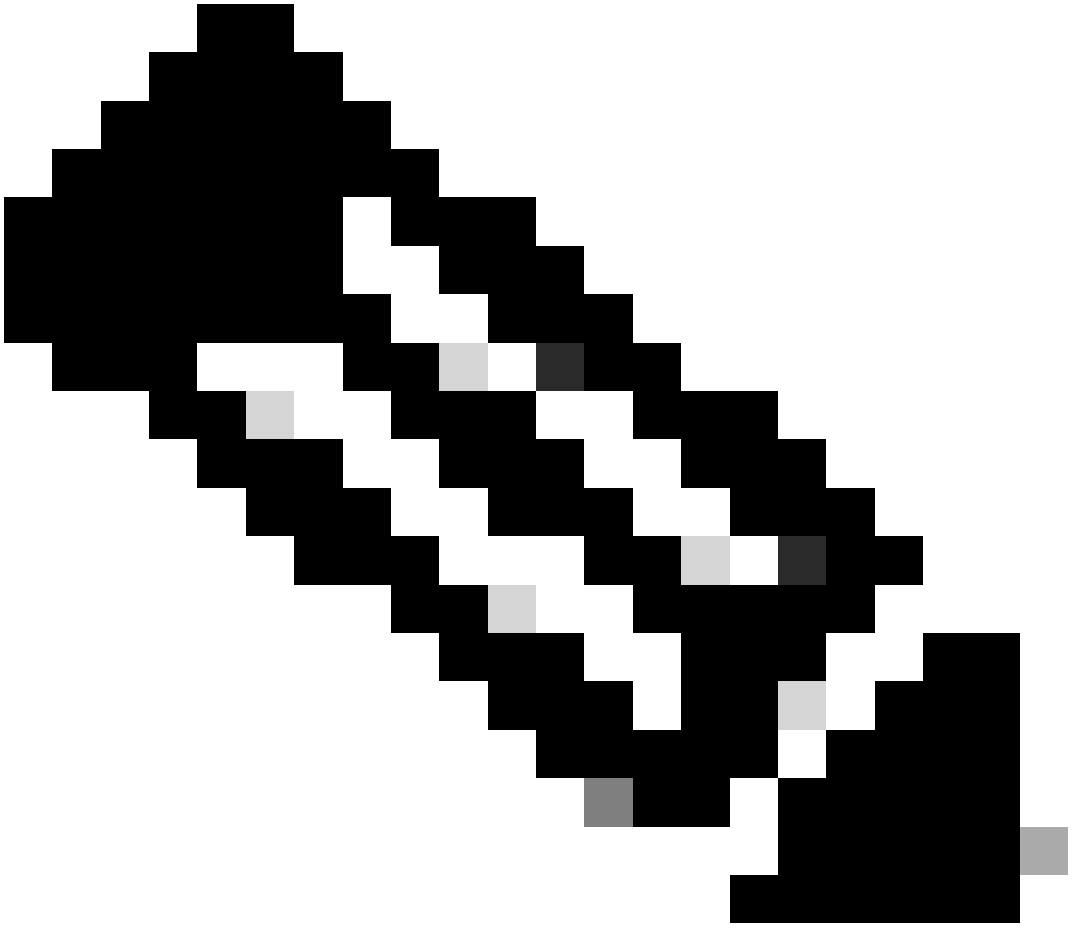
Le SIP peut :

- créer un appel
- modifier un appel
- mettre fin à un appel

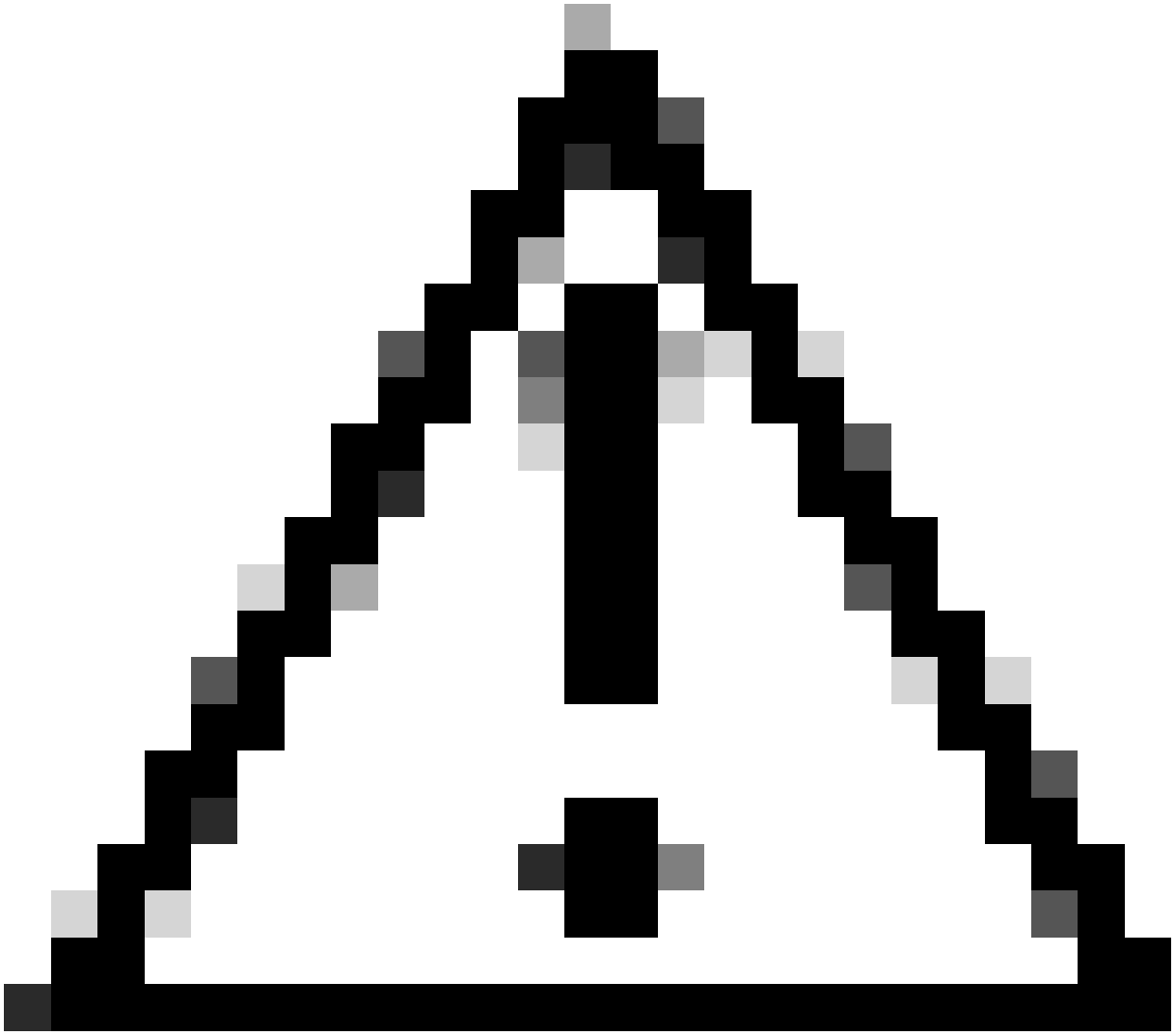
Le protocole SIP peut être utilisé avec le protocole UDP ou TCP sur le port normalisé 5060. Et si le SIP est chiffré à l'aide du protocole TLS (Transport Layer Security), il peut utiliser le port normalisé 5061.



Remarque : Lorsque la signalisation SIP est chiffrée, les paquets SIP réels ne sont pas visibles dans les captures de paquets sur les périphériques ASA ou FTD. Cependant, vous pouvez toujours observer la connexion TCP suivie de la connexion TLS entre les clients SIP et les périphériques serveur SIP.



Remarque : L'inspection SIP est activée par défaut sur Cisco Secure Firewall Threat Defense (FTD) et Secure Firewall Adaptive Security Appliance (ASA).



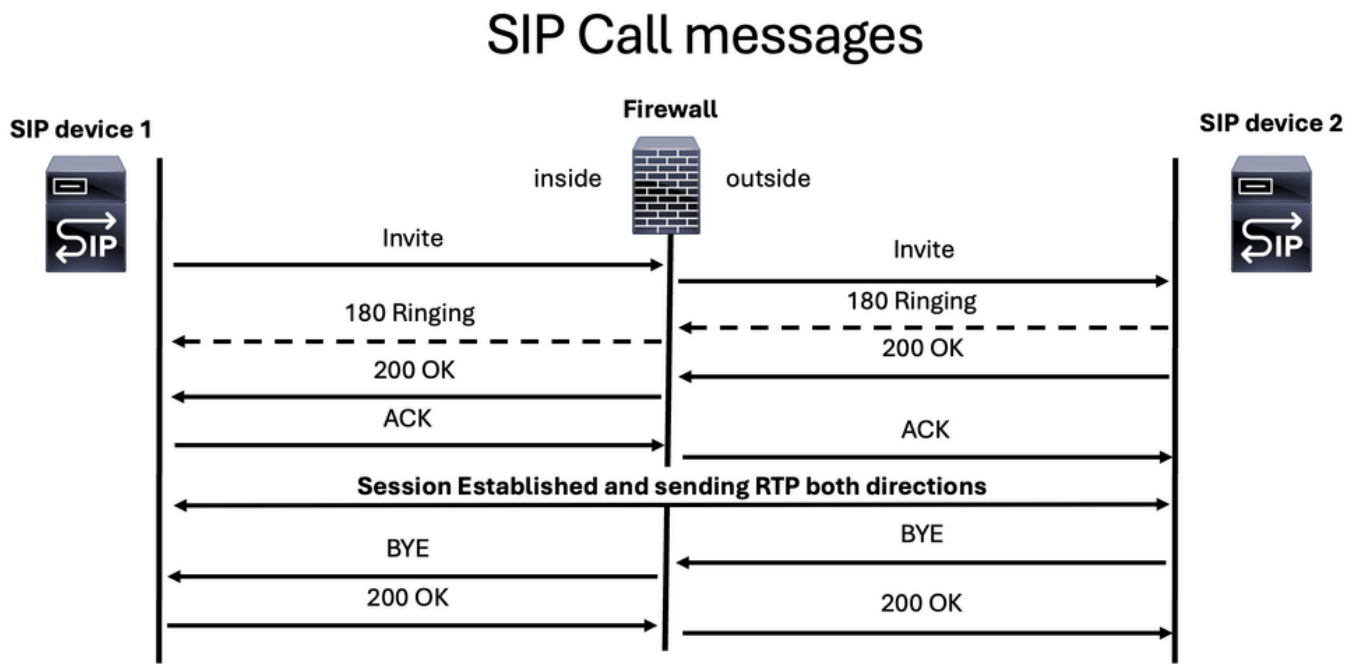
Mise en garde : Vérifiez toujours quels ports sont utilisés pour la signalisation. N'oubliez pas que le protocole SIP utilise généralement les ports 5060 ou 5061, mais certains déploiements peuvent s'écarter de ces normes et utiliser des ports différents pour le protocole SIP.

Trois scénarios peuvent être trouvés lors du dépannage d'un problème de signalisation SIP :

- Messages de signalisation d'appel SIP
- Messages SIP OPTION
- Messages SIP REGISTER

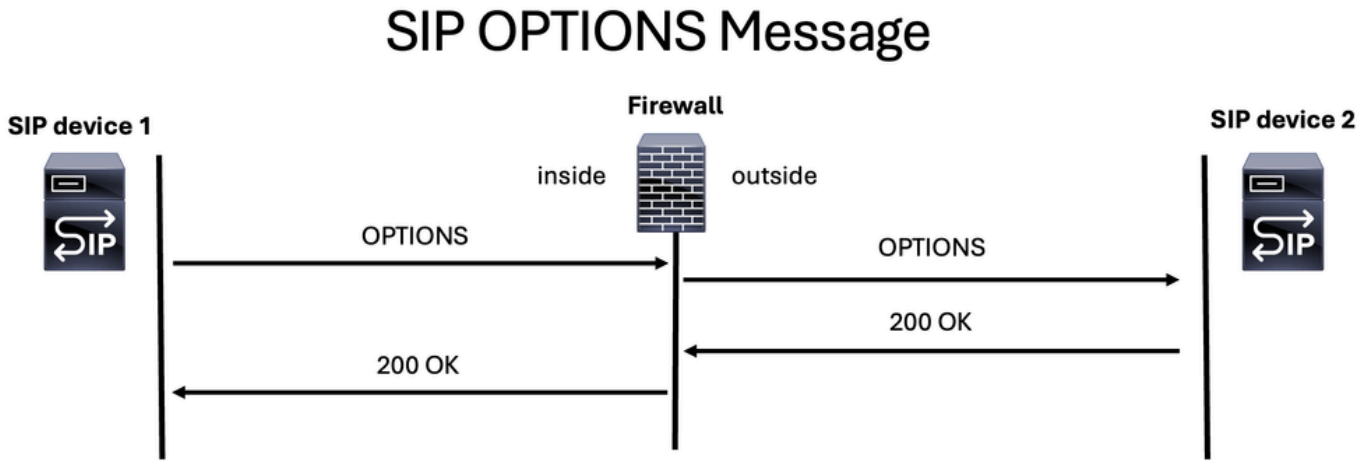
Messages d'appel SIP

Les principaux messages SIP permettant d'établir et de mettre fin à un appel vocal sont les suivants :



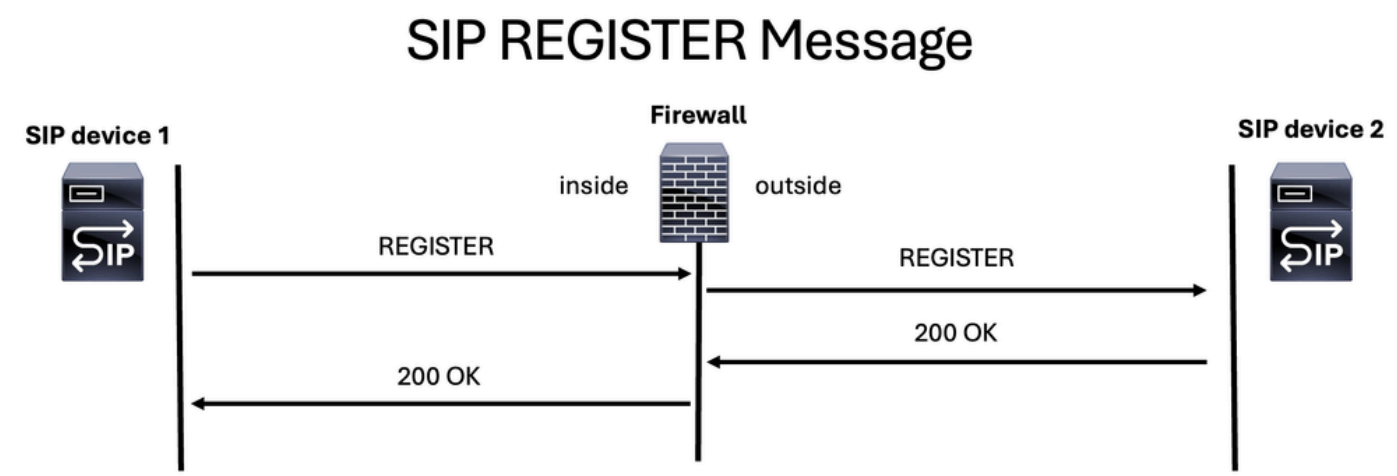
Messages SIP OPTION

Les messages SIP OPTIONS sont importants pour déterminer si un périphérique SIP est en ligne et capable de répondre. C'est comme envoyer une requête ping à un message ICMP, mais sur le monde SIP.

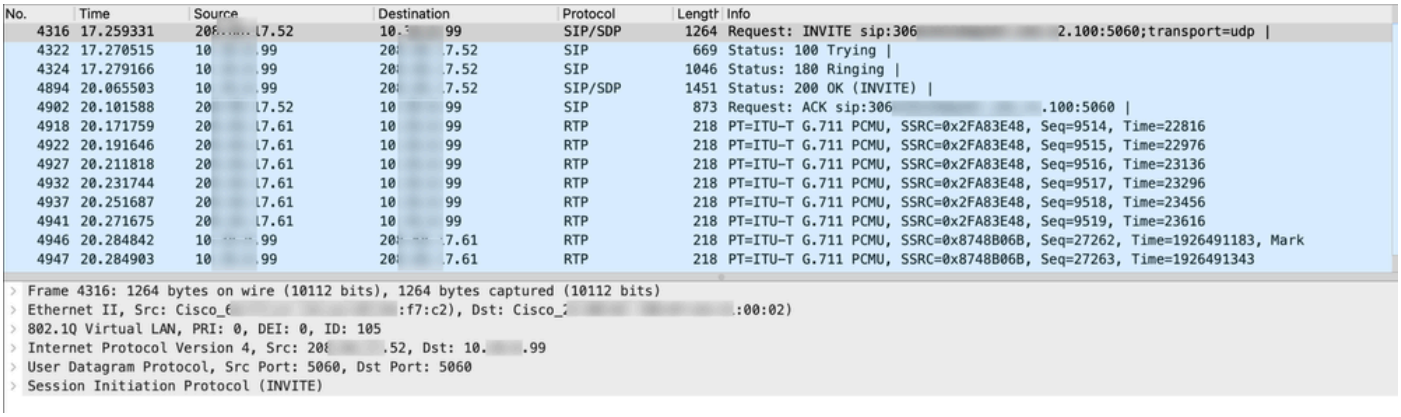


Message SIP REGISTER

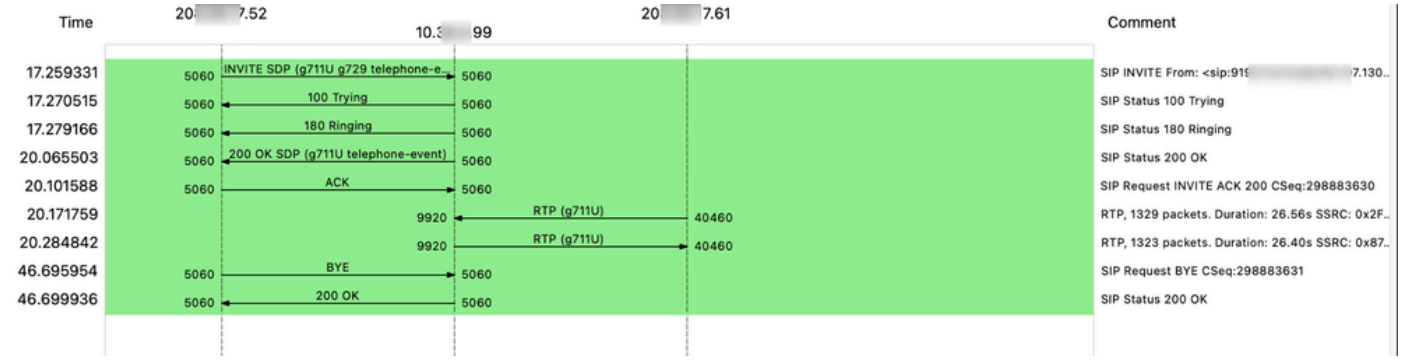
Un autre message SIP que vous pouvez trouver pendant une session de dépannage de pare-feu est le message SIP REGISTER, qui permet à un périphérique de s'enregistrer auprès d'un serveur SIP.



Cette capture de paquets affiche les requêtes et les réponses de deux périphériques SIP ainsi que le trafic (vocal) multimédia :

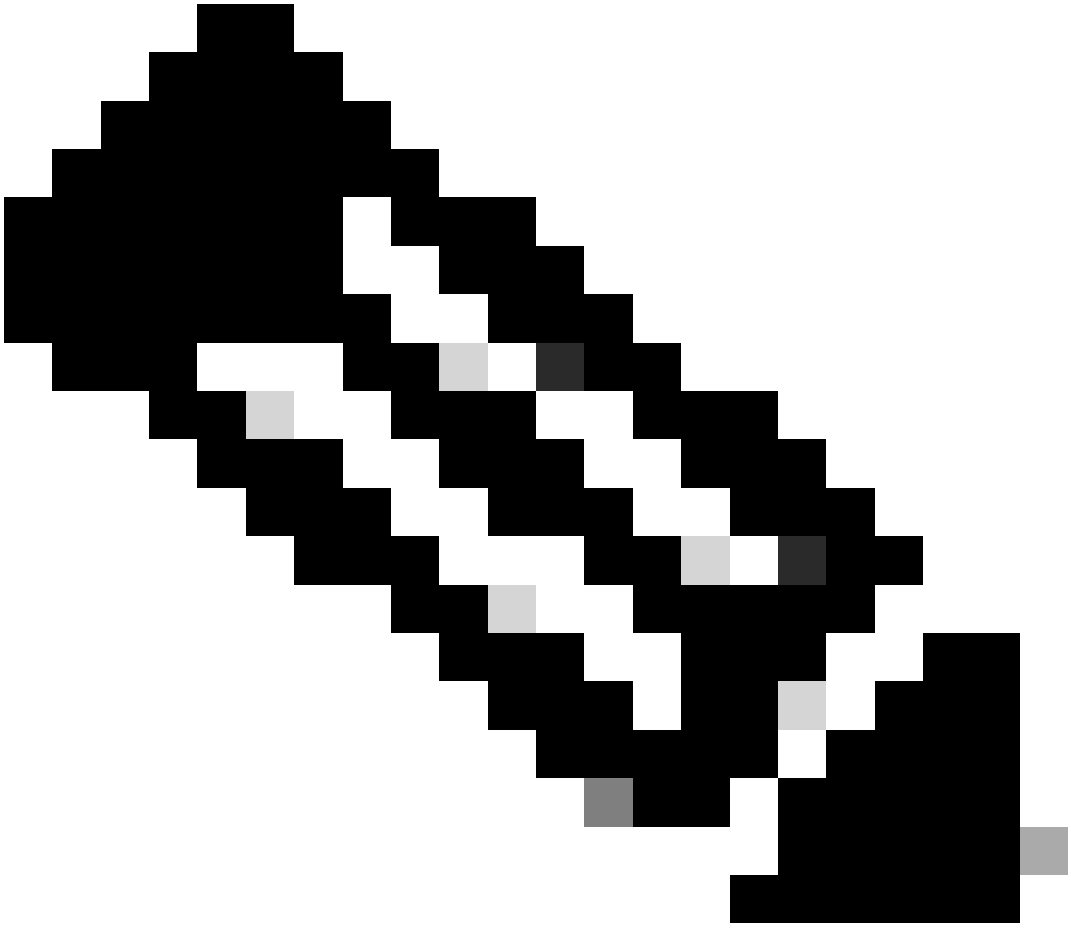


Voici un exemple de flux de signalisation SIP et de média RTP (voix) :



Protocole SDP (Session Description Protocol)

Le protocole SDP (Session Description Protocol) est une représentation standard utilisée pour décrire les flux multimédias pour les sessions multimédia. Il ne transporte pas le média lui-même, mais il est utilisé pour négocier le type et le format du média entre les points d'extrémité. Le protocole SDP est utilisé conjointement avec le protocole SIP (Session Initiation Protocol) pour gérer et négocier les caractéristiques de support d'une session.

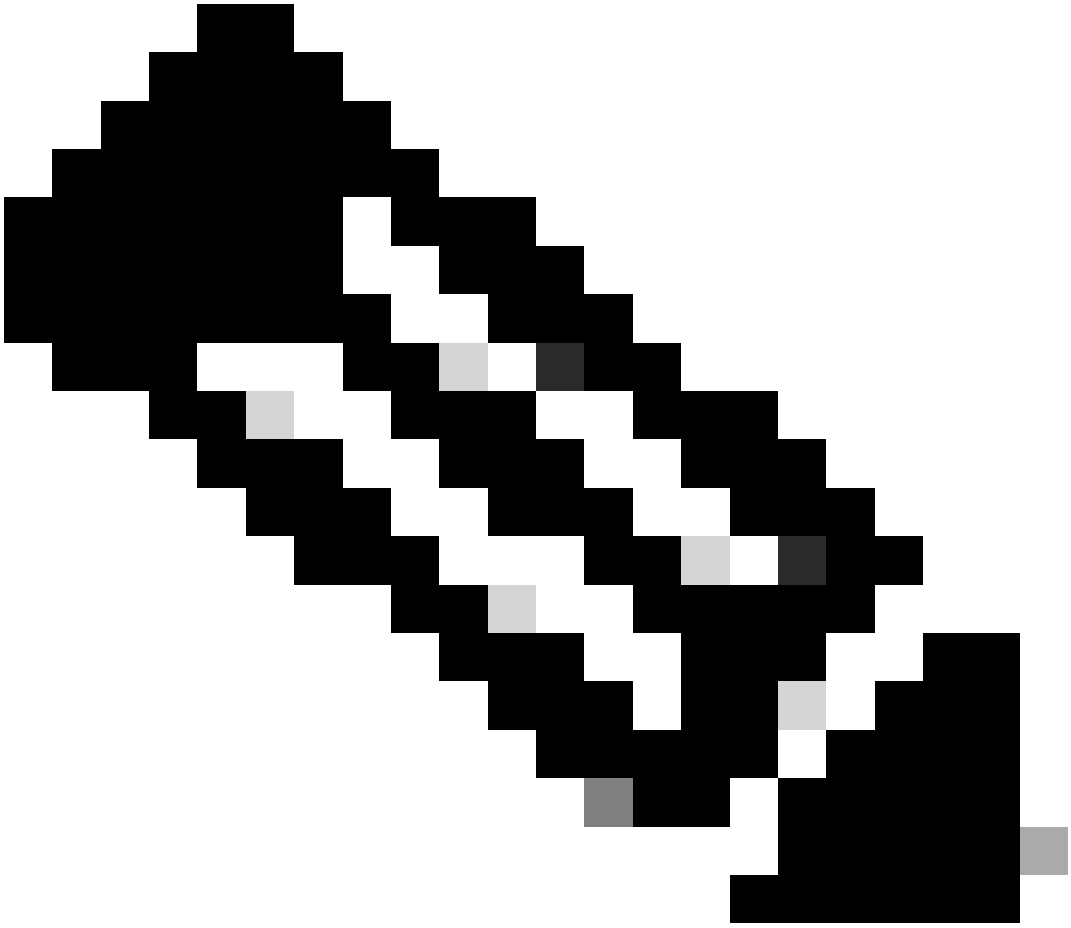


Remarque : MGCP intègre le concept de SDP, qui est utilisé dans le même but.

Voici un exemple de message SDP dans un protocole SIP :

```
INVITE sip:2003@192.168.245.9:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.245.6:5060;branch=z9hGXXX5763
Remote-Party-ID:


       ;party=calling;screen=no;privacy=off
From:


        ;tag=4E3XXXC-A9F
To:
```

```
Date: Thu, 17 Aug 2025 13:48:52 GMT
Call-ID: 2A7BE22B-XXXXXXXXX-XXXXXXXXX-F940DC75@192.168.245.6
Supported: 100rel,timer,resource-priority,replaces,sdp-anat
Min-SE:  1800
Cisco-Guid: 0350227076-XXXXXXXXX-XXXXXXXXX-1670485135
User-Agent: Cisco-SIPGateway/IOS-15.5.3.S4b
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO, REGISTER
CSeq: 101 INVITE
Timestamp: 150299CC32
Contact:



Expires: 180
Allow-Events: telephone-event
Max-Forwards: 69
Content-Type: application/sdp    <========Session Description Protocol message start
Content-Disposition: session;handling=required
Content-Length: 266

v=0
o=CiscoSystemsSIP-GW-UserAgent 7317 4642 IN IP4 192.168.245.6
s=SIP Call
c=IN IP4 192.168.245.6
t=0 0
m=audio 8266 RTP/AVP 18 127
c=IN IP4 192.168.245.6
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:127 telephone-event/8000
a=fmtp:127 0-16
a=ptime:20
```



Remarque : Certains des messages SDP contiennent les paramètres suivants dans l'exemple :

++c-IN IP4 : Adresse IP du serveur multimédia

++m=audio : Cela indique que le type de support est audio.

8 266 ++ : Il s'agit du numéro de port sur lequel le flux audio doit être envoyé.

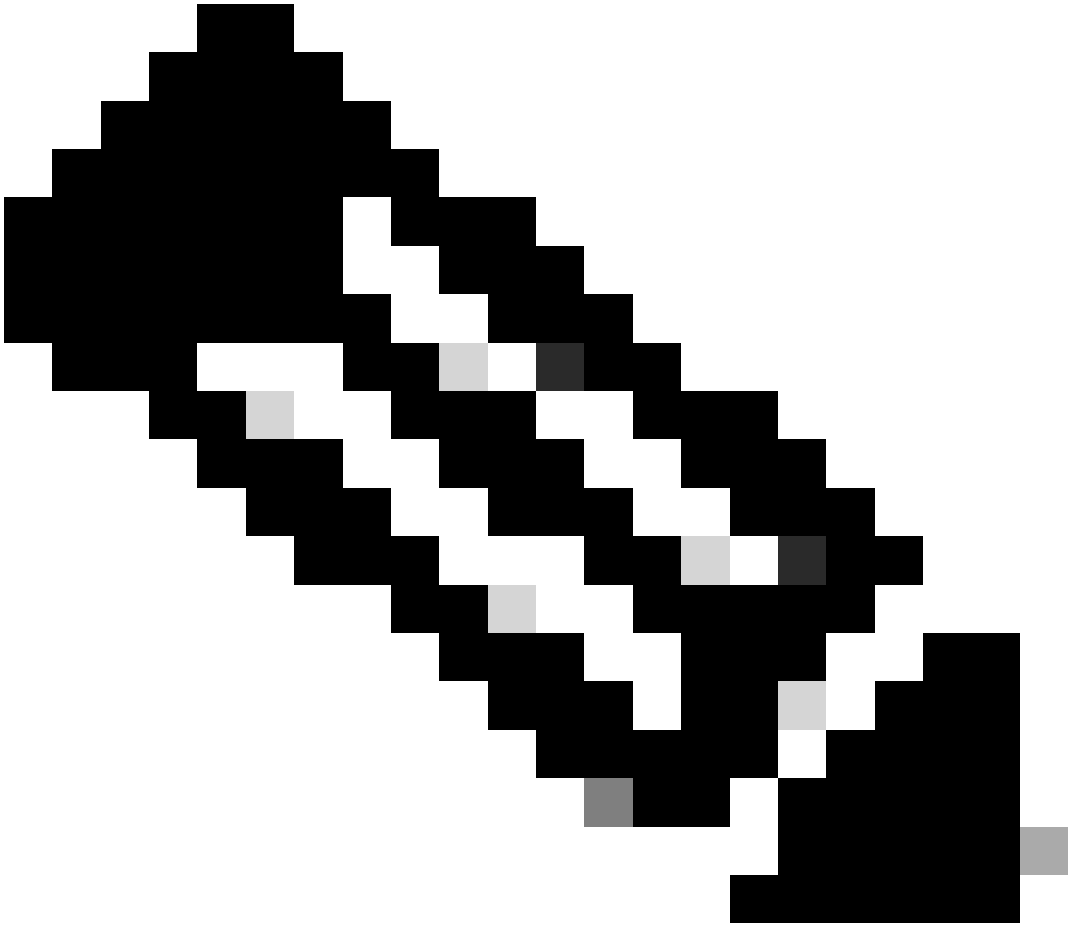
++RTP/AVP : Indique le protocole de transport, qui est RTP à l'aide du profil audio/vidéo (AVP).

18 127 ++ : Il s'agit des types de données utiles pour les codecs audio. Le type de charge utile 18 correspond généralement au codec G.729, et 127 est un type de charge utile dynamique qui peut être attribué à un codec selon la négociation entre les points d'extrémité.

Le protocole SDP (Session Description Protocol) se trouve dans plusieurs messages SIP, tels que

: INVITE, 183 Session en cours, 200 OK, ACK, etc. SDP sert de méthode de réponse pour échanger des fonctionnalités vocales et/ou vidéo entre les parties. Lors du dépannage des problèmes d'appel, il est essentiel de comprendre trois concepts principaux :

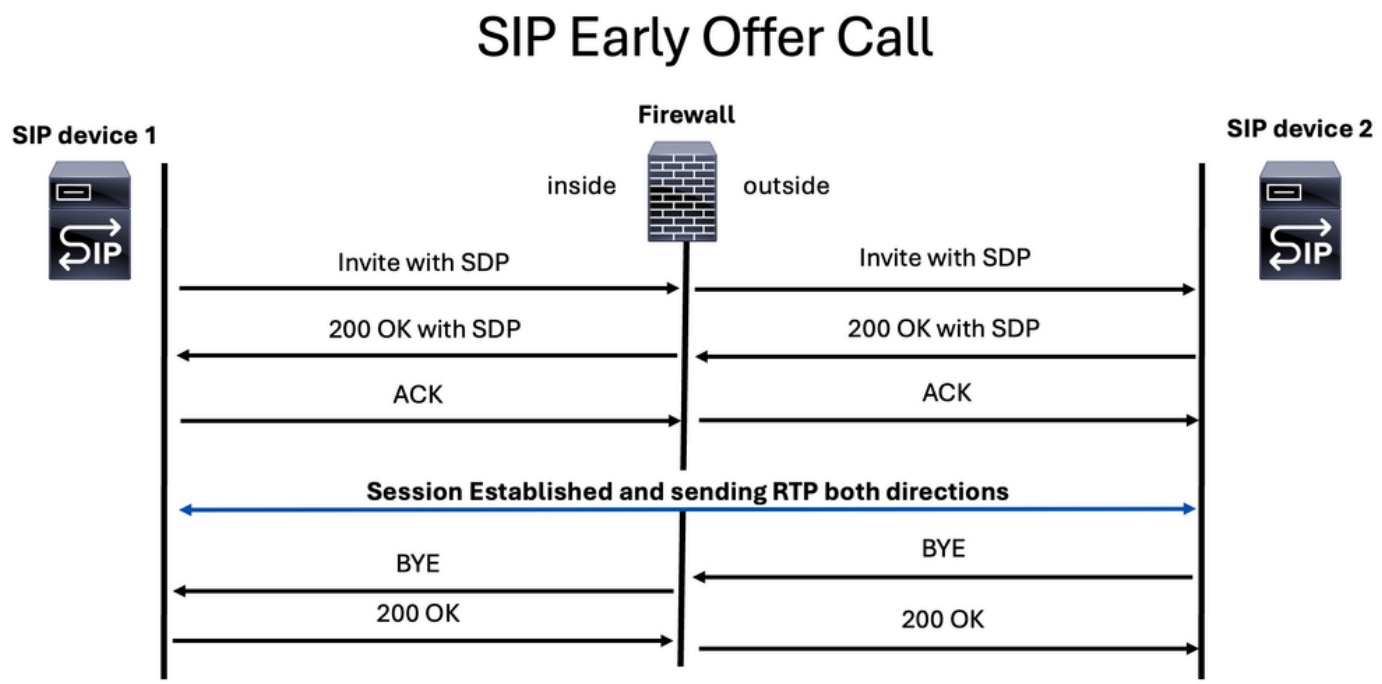
1. Offre anticipée
2. Offre différée
3. Premiers médias



> Remarque : Il est essentiel de comprendre la destination des messages SDP, car la fonctionnalité d'inspection sur le pare-feu peut modifier les adresses IP non seulement dans les en-têtes SIP, mais aussi dans la section SDP.

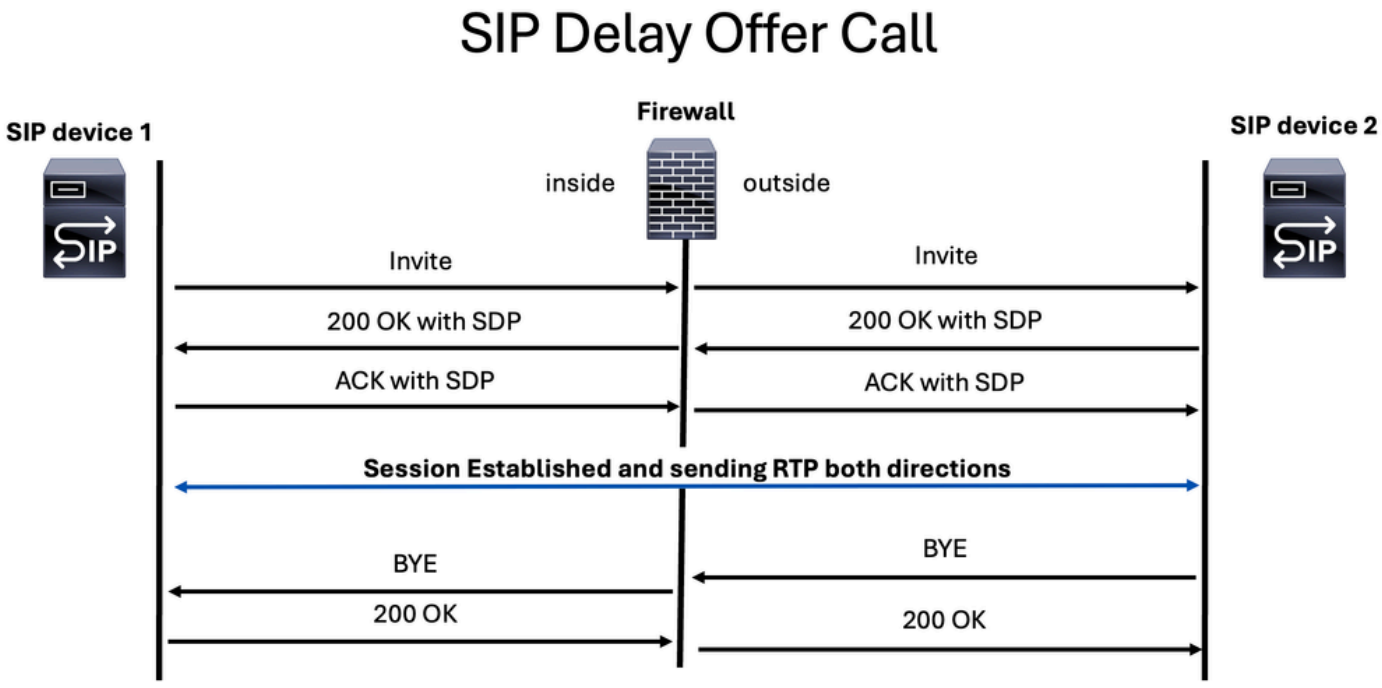
Offre anticipée

Les paramètres de support sur SDP se trouvent ici dans les messages INVITE et 200 OK SIP.



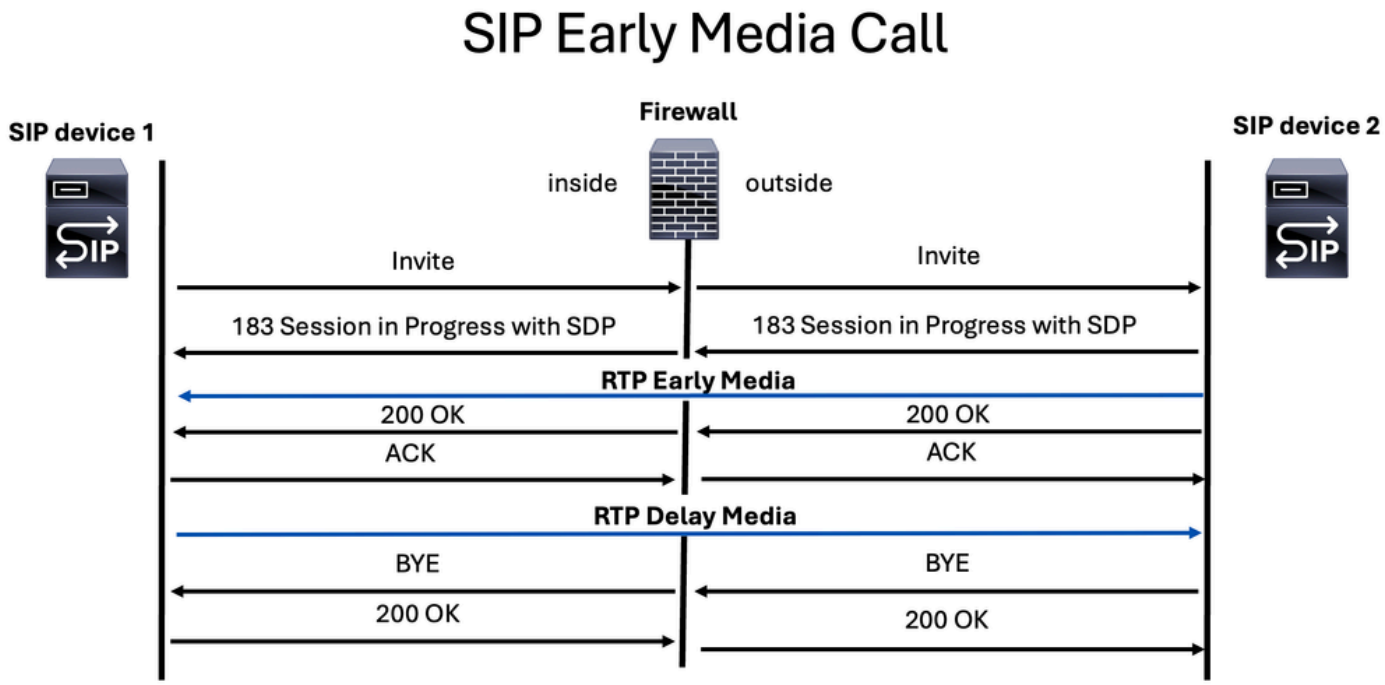
Offre différée

Avec cette méthode, le SDP se trouve sur 200 messages OK et ACK SIP.



Premiers médias

Les premiers supports sont transmis via un message SIP spécifique appelé « réponse de progression de la session 183 ». Ce message inclut le protocole SDP (Session Description Protocol) contenant les paramètres de support pour l'appelé. Il est généralement utilisé par les opérateurs et les fournisseurs SIP pour envoyer des messages vocaux automatisés ou d'autres supports à l'appelant avant que l'appel ne soit officiellement connecté.

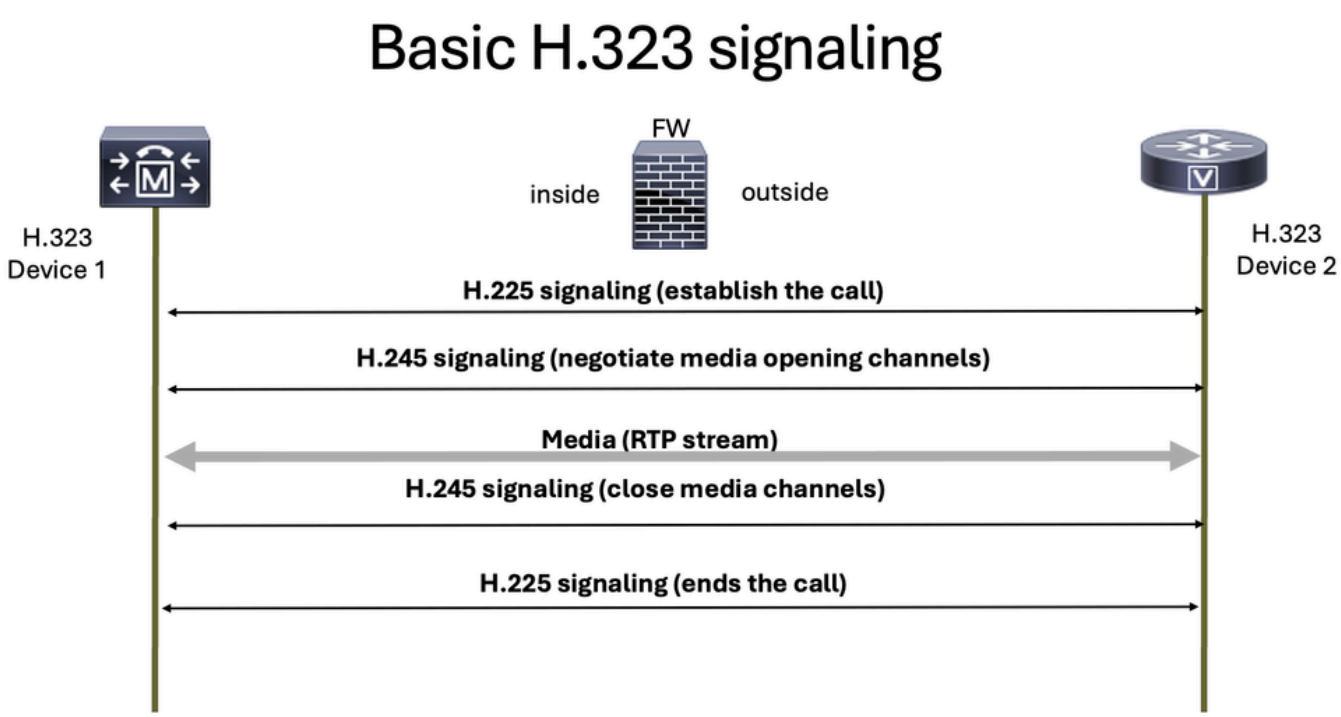


H.323

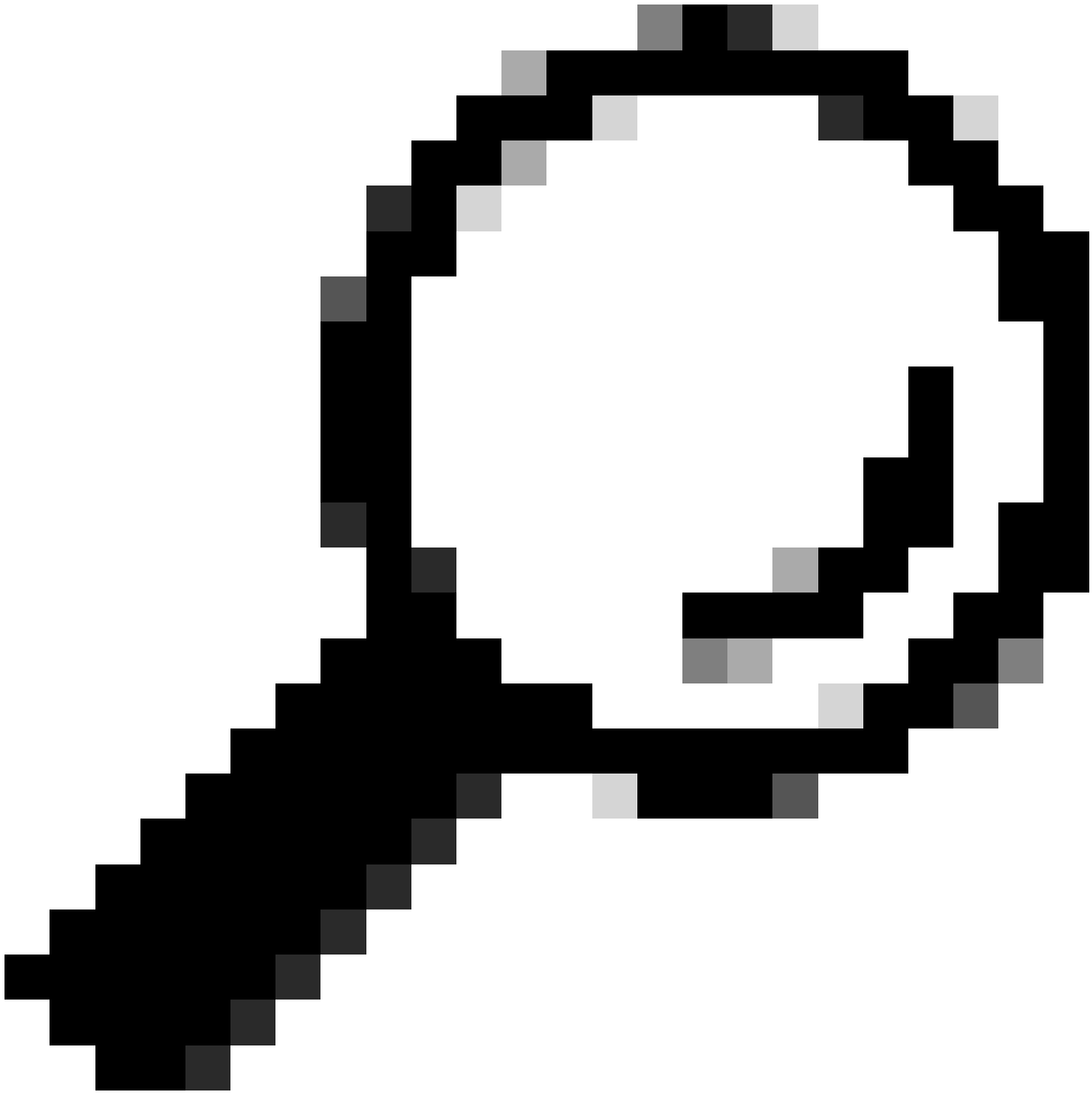
H.323 est un ensemble de protocoles définis par l'Union internationale des télécommunications (UIT) pour les communications vocales, vidéo et de données sur des réseaux à commutation de paquets, tels qu'Internet.

Le protocole H.323 est composé de deux composants principaux :

1. H.225 : Il gère la signalisation des appels, y compris l'établissement et la fin des appels.
2. H.245 : Il est responsable de l'échange des capacités et de l'ouverture et de la fermeture des canaux audio et vidéo.



Les ports utilisés par le protocole de signalisation H.323 sont 1718, 1719 et 1720.

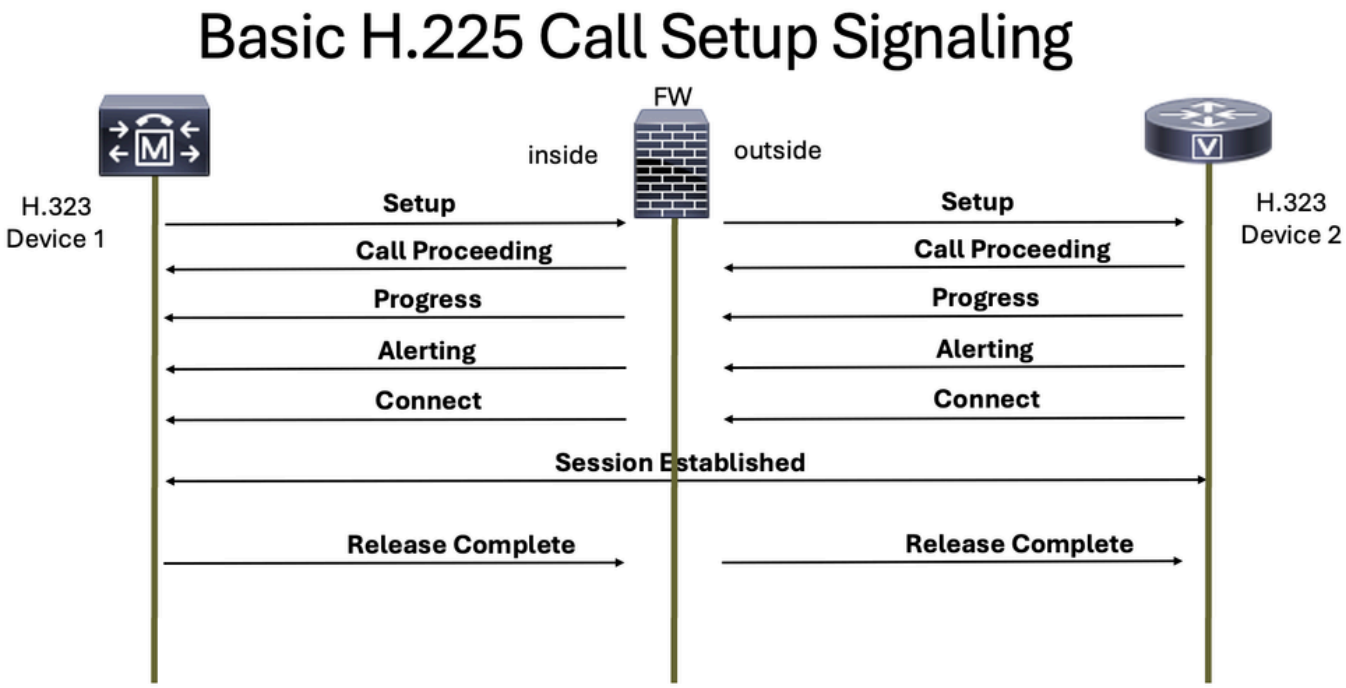


Conseil : Les communications sécurisées du protocole H.323 peuvent rencontrer des problèmes lors de la commutation du protocole UDP au protocole TCP en raison de l'utilisation de TLS pour le chiffrement, ce qui peut entraîner le blocage par erreur de la connexion par un pare-feu en tant qu'activité suspecte. Il est donc essentiel de configurer le pare-feu pour autoriser le trafic UDP et TCP pour les points d'extrémité ou les serveurs H.323.

H.323 est un protocole qui possède deux modes de fonctionnement : démarrage lent et démarrage rapide.

H.225

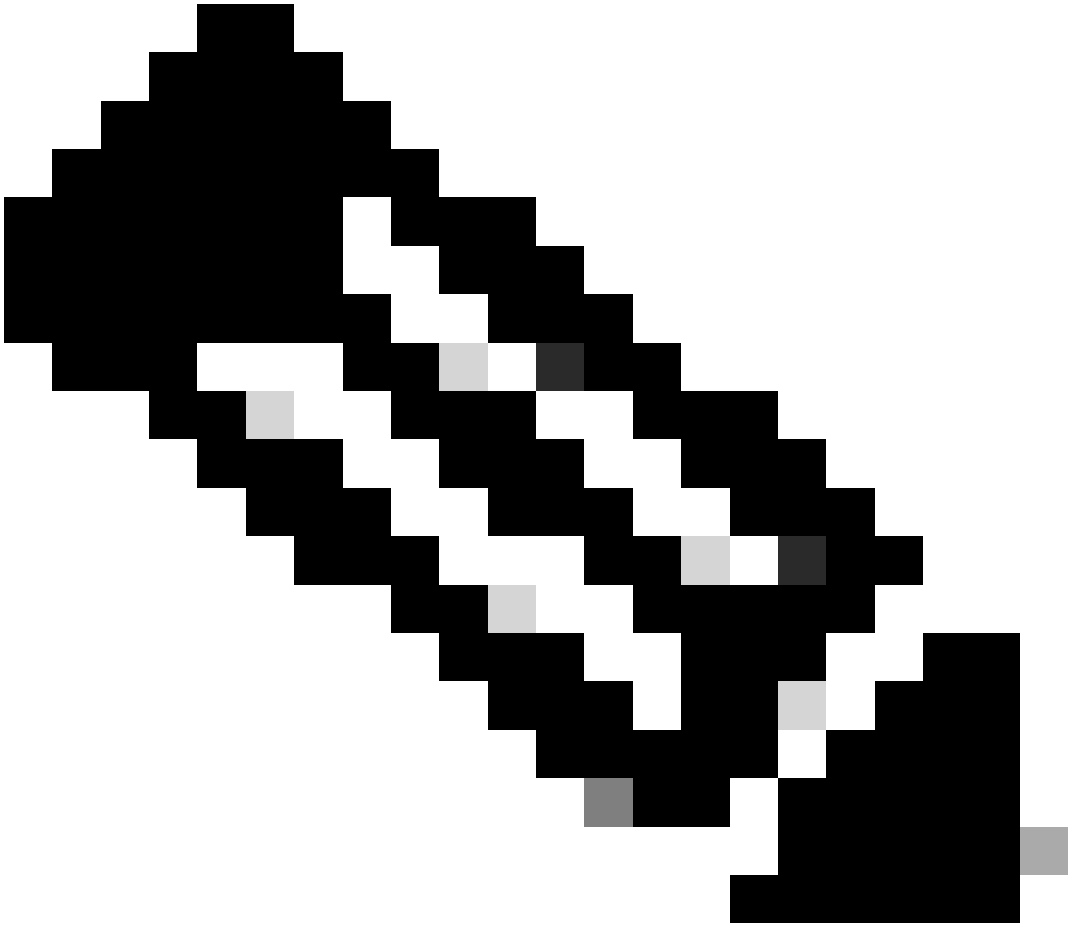
Ce protocole est chargé de configurer l'appel et de mettre fin à un appel vocal lorsque l'un des interlocuteurs raccroche.



H,245

H.245 offre les fonctionnalités suivantes :

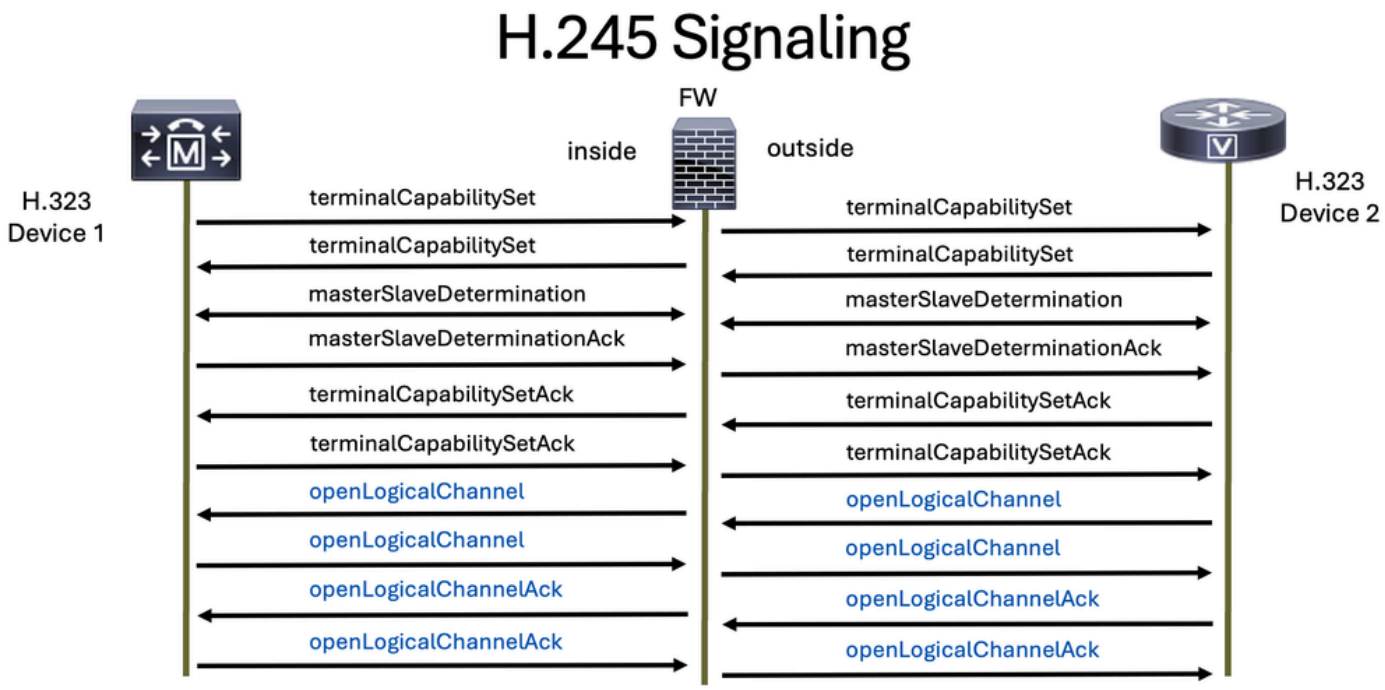
- échange des capacités du terminal
- Déterminations maître/esclave
- Signalisation de canal logique



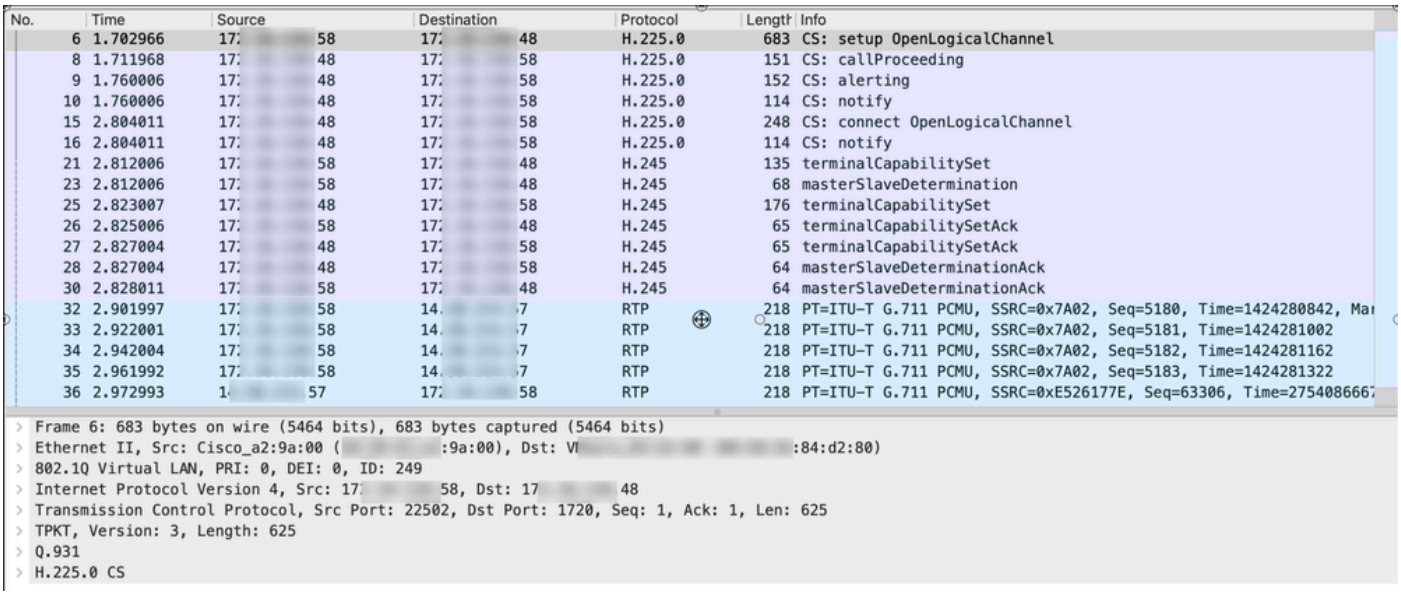
Remarque : Les termes Maître et Esclave utilisés dans ce document sont codés en dur dans le protocole H.323 d'origine et ne reflètent pas les politiques ou les valeurs de notre société. Nous nous engageons à promouvoir une langue inclusive et respectueuse.

Le protocole H.245 est envoyé après réception du message de connexion H.225.

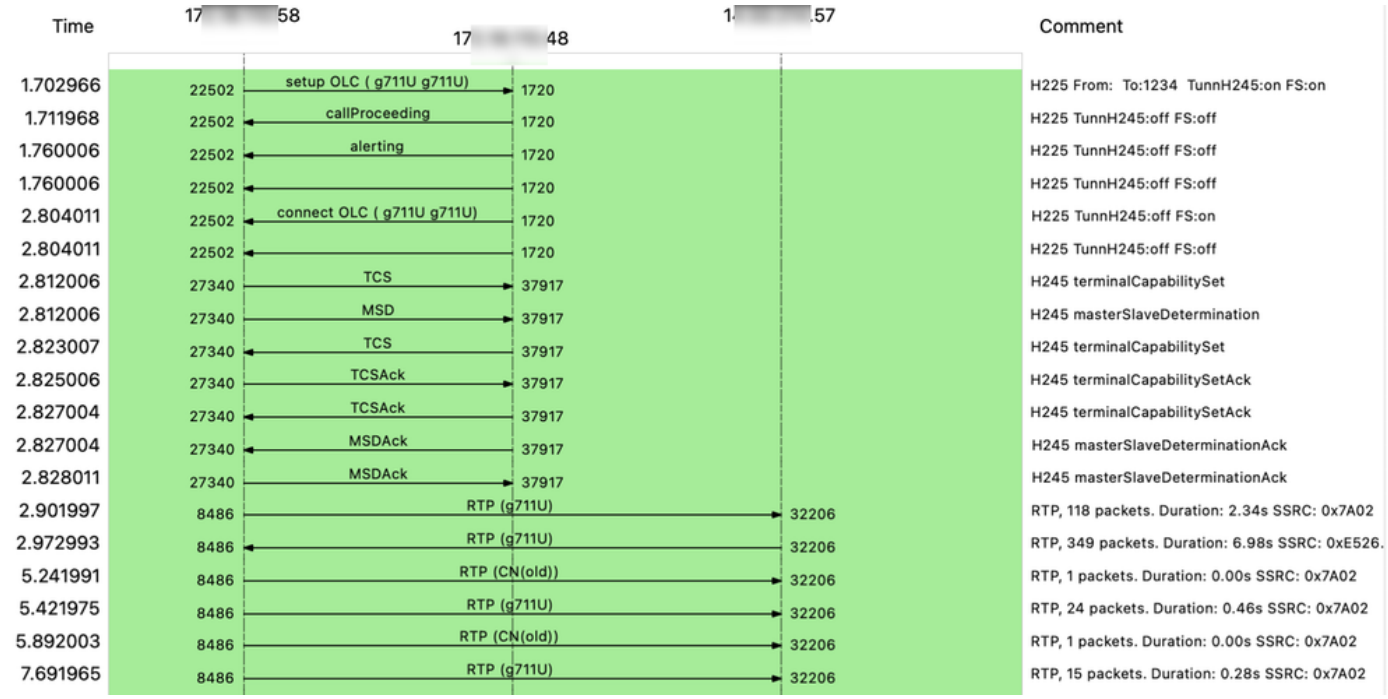
Ce protocole aide à déterminer quel protocole vocal est utilisé pour le protocole RTP, et il est spécifié sur le canal logique d'ouverture et les messages de canal logique de fermeture pour lui.

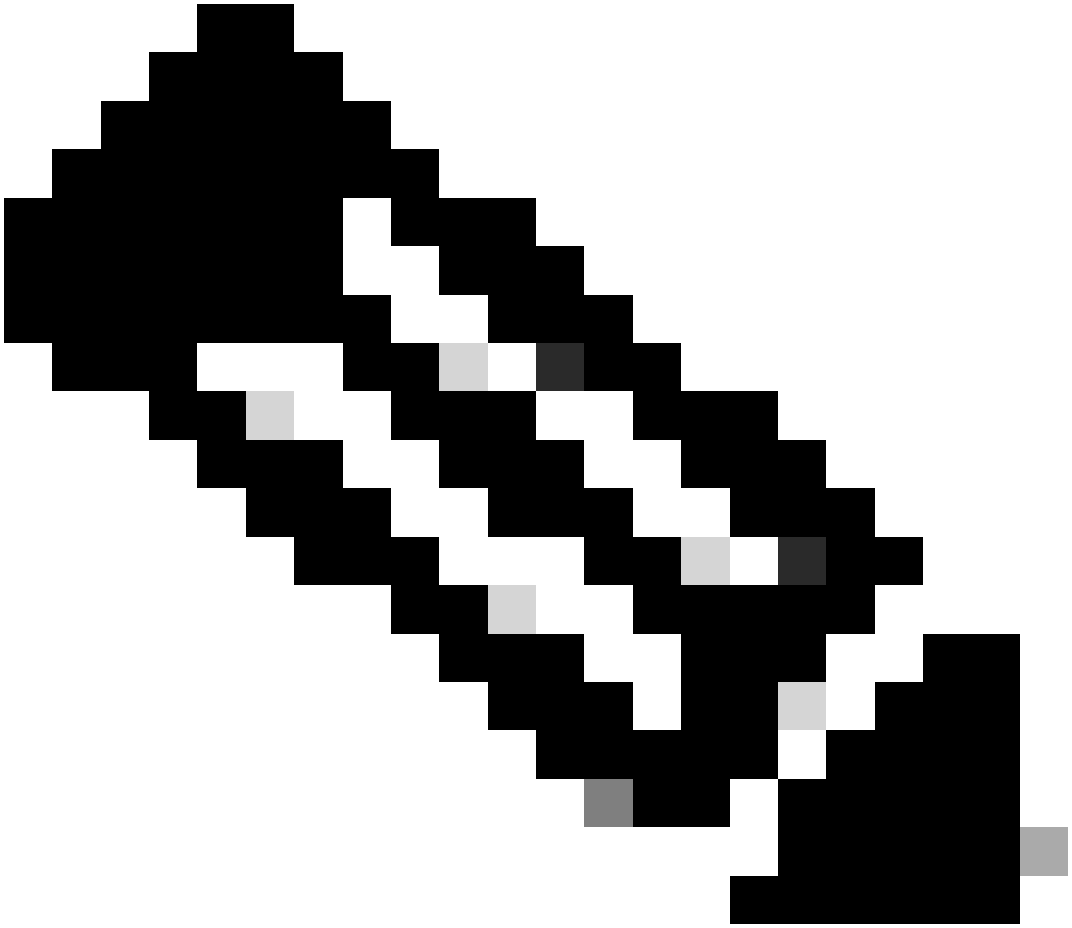


Cette capture de paquets affiche les requêtes et les réponses de deux périphériques H.323 avec H.225 et H.245, ainsi que le trafic média (voix) :



Voici un exemple d'un flux de signalisation H.323 avec H.225 et H.245 et un média RTP (voix) :

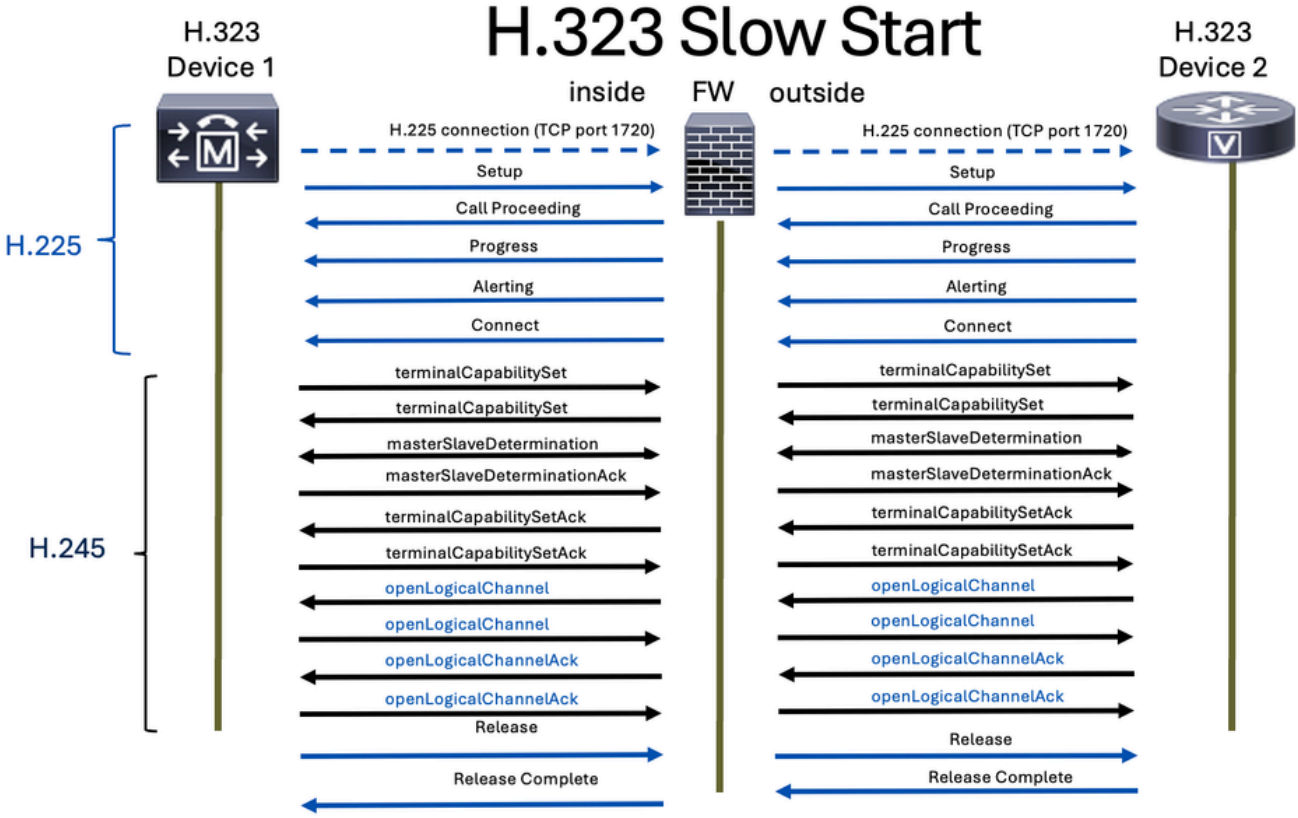

Time
Comment
1.702966 22502 setup OLC (g711U g711U) 1720 H225 From: To:1234 TunnH245:on FS:on
1.711968 22502 callProceeding 1720 H225 TunnH245:off FS:off
1.760006 22502 alerting 1720 H225 TunnH245:off FS:off
1.760006 22502 1720 H225 TunnH245:off FS:off
2.804011 22502 connect OLC (g711U g711U) 1720 H225 TunnH245:off FS:on
2.804011 22502 1720 H225 TunnH245:off FS:off
2.812006 27340 TCS 37917 H245 terminalCapabilitySet
2.812006 27340 MSD 37917 H245 masterSlaveDetermination
2.823007 27340 TCS 37917 H245 terminalCapabilitySet
2.825006 27340 TCSAck 37917 H245 terminalCapabilitySetAck
2.827004 27340 TCSAck 37917 H245 terminalCapabilitySetAck
2.827004 27340 MSDAck 37917 H245 masterSlaveDeterminationAck
2.828011 27340 MSDAck 37917 H245 masterSlaveDeterminationAck
2.901997 8486 RTP (g711U) 32206 RTP, 118 packets. Duration: 2.34s SSRC: 0x7A02
2.972993 8486 RTP (g711U) 32206 RTP, 349 packets. Duration: 6.98s SSRC: 0xE526.
5.241991 8486 RTP (CN(old)) 32206 RTP, 1 packets. Duration: 0.00s SSRC: 0x7A02
5.421975 8486 RTP (g711U) 32206 RTP, 24 packets. Duration: 0.46s SSRC: 0x7A02
5.892003 8486 RTP (CN(old)) 32206 RTP, 1 packets. Duration: 0.00s SSRC: 0x7A02
7.691965 8486 RTP (g711U) 32206 RTP, 15 packets. Duration: 0.28s SSRC: 0x7A02



Remarque : L'inspection H.323 est activée par défaut sur Cisco Secure Firewall Threat Defense (FTD) et Secure Firewall Adaptive Security Appliance (ASA).

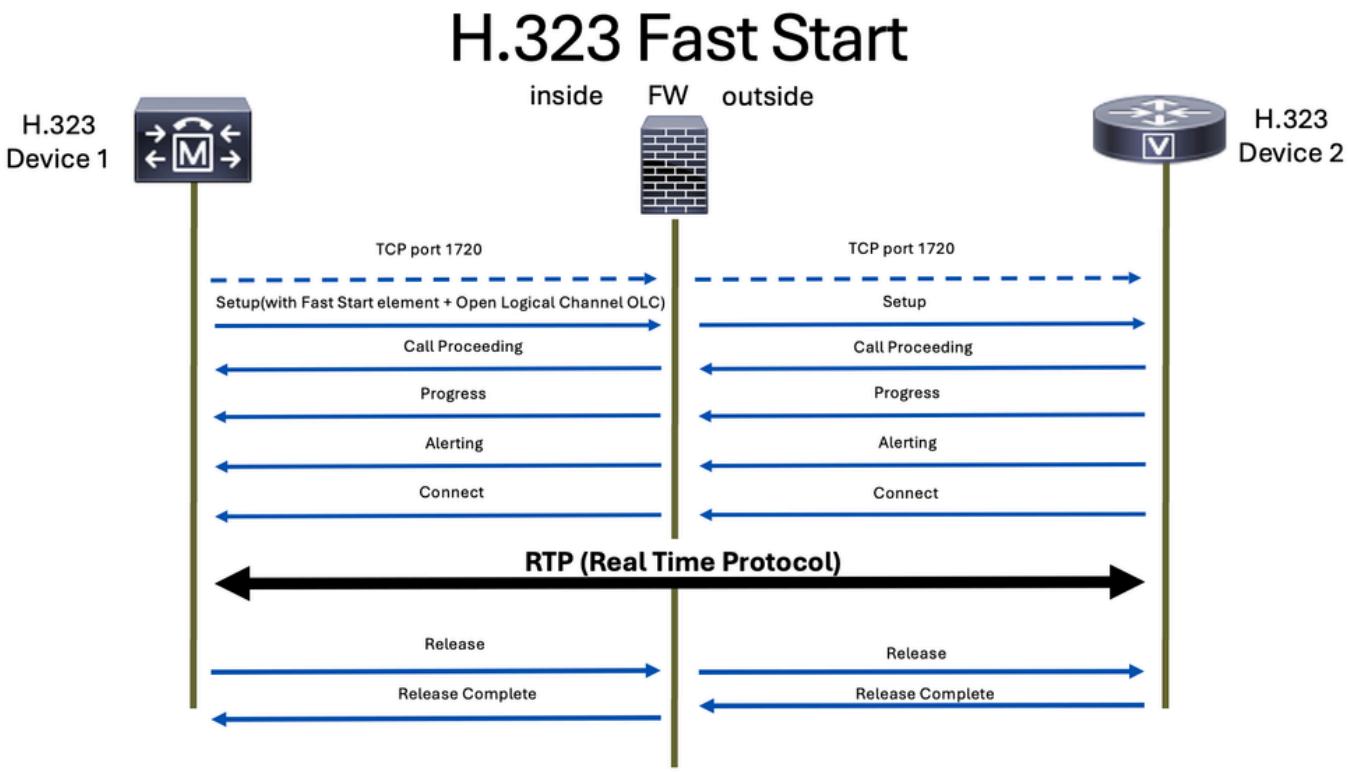
Démarrage lent

En mode de démarrage lent, le processus d'établissement d'appel implique plusieurs étapes de signalisation avant l'établissement des canaux multimédias. Les étapes comprennent la configuration, la poursuite de l'appel, l'alerte et la connexion. Après ces étapes, la négociation de support H.245 est effectuée séparément. Cela signifie que les canaux multimédias ne sont établis qu'une fois la signalisation d'appel initiale terminée, ce qui peut allonger le temps de configuration.



Démarrage rapide

En revanche, le mode de démarrage rapide permet la négociation de support dans le message de configuration initiale. Cela signifie que les canaux multimédias peuvent être établis plus rapidement, car la négociation est effectuée dans le cadre de la configuration initiale de l'appel. Le démarrage rapide rationalise le processus en réduisant le nombre de messages échangés et la quantité de traitement nécessaire avant l'établissement des canaux multimédias.

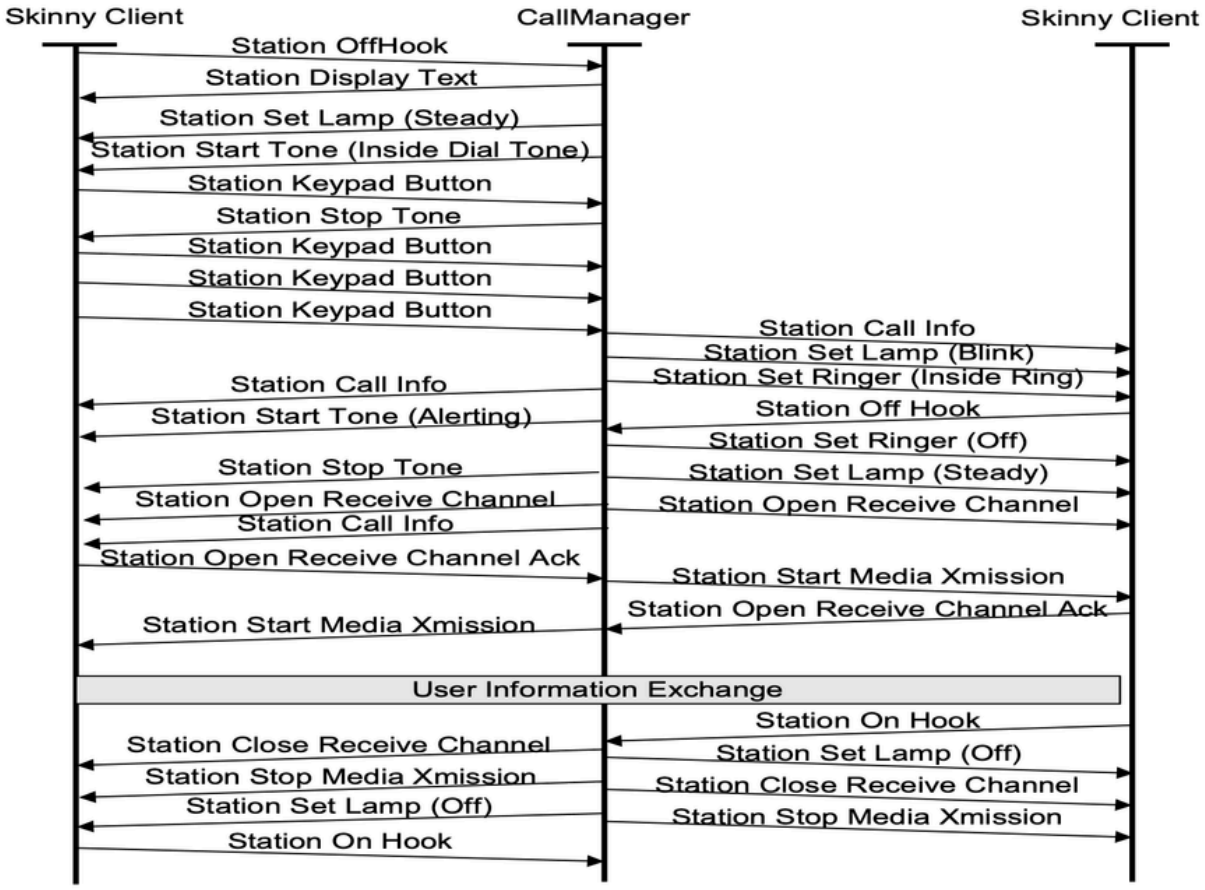


SCCP

Skinny Client Control Protocol (SCCP), souvent appelé simplement Skinny, est un protocole de signalisation propriétaire de Cisco. Il est principalement utilisé par les routeurs Cisco Unified Communications Manager (CUCM), Cisco Unified Communications Manager Express (CME) et les téléphones IP Cisco pour faciliter la configuration et le contrôle des appels.

Le protocole SCCP utilise le protocole TCP sur le port 2000 pour le protocole SCCP non sécurisé et le port 2443 pour le protocole SCCP sécurisé.

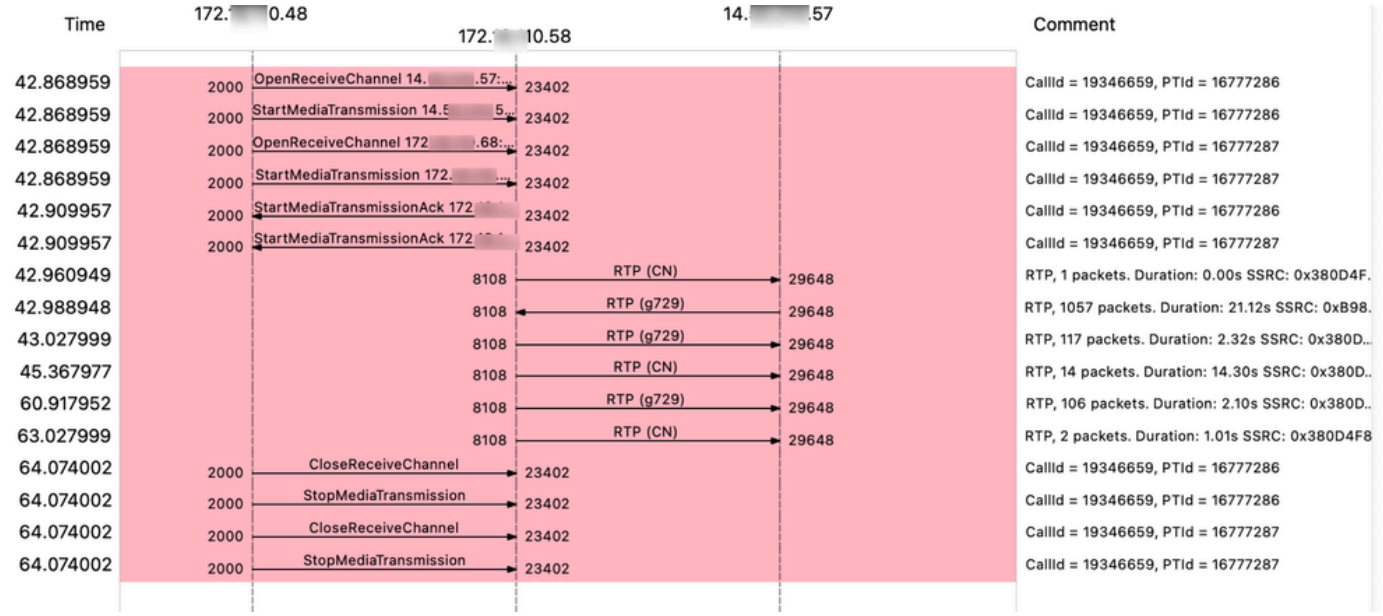
Voici les messages SCCP courants que vous pouvez trouver sur un appel SCCP :



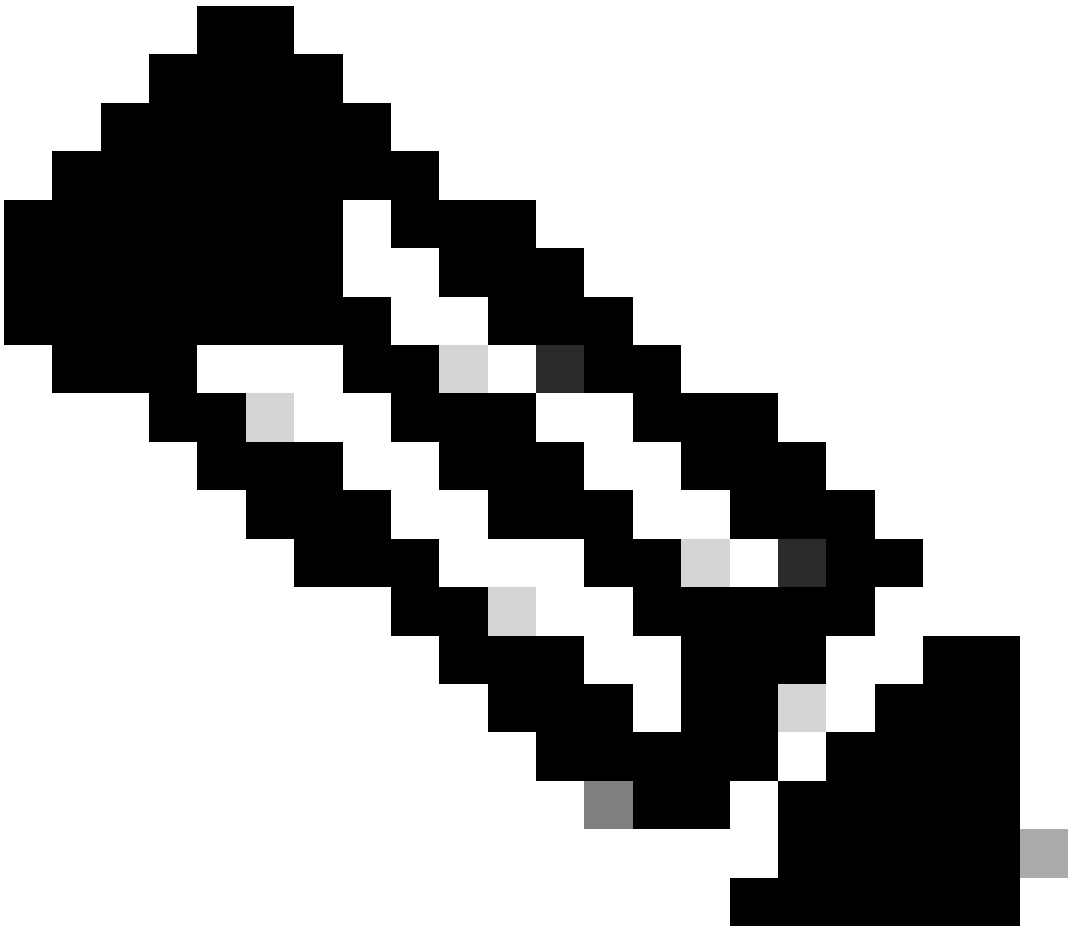
Cette capture de paquets affiche les requêtes et les réponses de deux périphériques SCCP, ainsi que le trafic média (vocal) :

No.	Time	Source	Destination	Protocol	Length	Info
42	11.170041	172. .0.48	172. 0.58	SKINNY/REQ	202	OpenReceiveChannel
58	13.307028	172. .0.48	172. 0.58	SKINNY/REQ	202	StartMediaTransmission
59	13.307028	172. .0.48	172. 0.58	SKINNY/REQ	202	OpenReceiveChannel
60	13.307028	172. .0.48	172. 0.58	SKINNY/REQ	202	StartMediaTransmission
62	13.309042	172. .0.58	172. 0.48	SKINNY/RESP	110	StartMediaTransmissionAck
64	13.309042	172. .0.58	172. 0.48	SKINNY/RESP	158	OpenReceiveChannelAck StartMediaTransmissionAck
66	13.390031	14.5 .57	172. 0.58	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7B4D4E5D, Seq=54086, Time=2101901655, Mark
67	13.409027	14.5 .57	172. 0.58	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7B4D4E5D, Seq=54087, Time=2101901815
68	13.429031	14.5 .57	172. 0.58	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7B4D4E5D, Seq=54088, Time=2101901975
69	13.451033	14.5 .57	172. 0.58	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7B4D4E5D, Seq=54089, Time=2101902135
70	13.453031	172. 0.58	14. .57	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x50, Seq=0, Time=585879569

Voici un exemple de flux de signalisation SCCP et de média RTP (voix) :



Time	172.[redacted]0.48		172.[redacted]10.58	14.[redacted].57	Comment
42.868959	2000	OpenReceiveChannel 14.[redacted].57:...	23402		CallId = 19346659, PTId = 16777286
42.868959	2000	StartMediaTransmission 14.5[redacted]5...	23402		CallId = 19346659, PTId = 16777286
42.868959	2000	OpenReceiveChannel 172[redacted].68:...	23402		CallId = 19346659, PTId = 16777287
42.868959	2000	StartMediaTransmission 172.[redacted]...	23402		CallId = 19346659, PTId = 16777287
42.909957	2000	StartMediaTransmissionAck 172.[redacted]	23402		CallId = 19346659, PTId = 16777286
42.909957	2000	StartMediaTransmissionAck 172.[redacted]	23402		CallId = 19346659, PTId = 16777287
42.960949		8108 RTP (CN)		29648	RTP, 1 packets. Duration: 0.00s SSRC: 0x380D4F.
42.988948		8108 RTP (g729)		29648	RTP, 1057 packets. Duration: 21.12s SSRC: 0xB98.
43.027999		8108 RTP (g729)		29648	RTP, 117 packets. Duration: 2.32s SSRC: 0x380D...
45.367977		8108 RTP (CN)		29648	RTP, 14 packets. Duration: 14.30s SSRC: 0x380D..
60.917952		8108 RTP (g729)		29648	RTP, 106 packets. Duration: 2.10s SSRC: 0x380D..
63.027999		8108 RTP (CN)		29648	RTP, 2 packets. Duration: 1.01s SSRC: 0x380D4F8
64.074002	2000	CloseReceiveChannel	23402		CallId = 19346659, PTId = 16777286
64.074002	2000	StopMediaTransmission	23402		CallId = 19346659, PTId = 16777286
64.074002	2000	CloseReceiveChannel	23402		CallId = 19346659, PTId = 16777287
64.074002	2000	StopMediaTransmission	23402		CallId = 19346659, PTId = 16777287



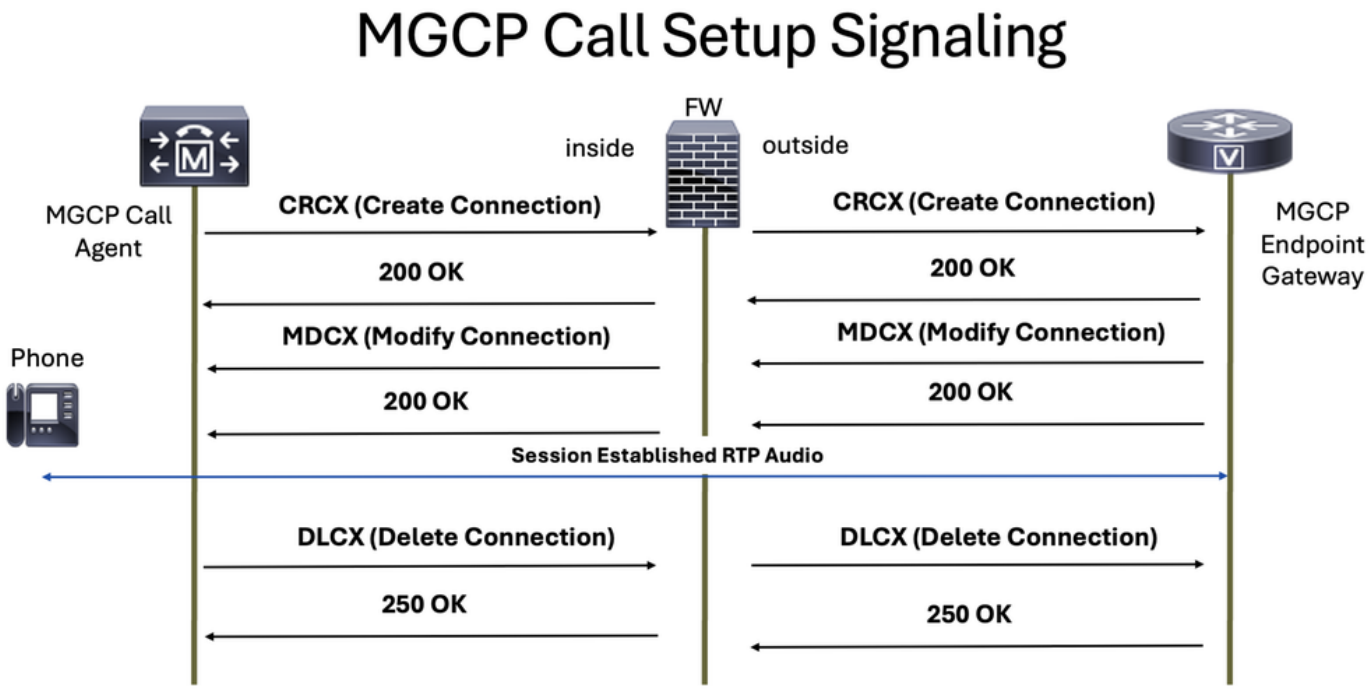
Remarque : L'inspection SCCP est activée par défaut sur Cisco Secure Firewall Threat Defense (FTD) et Secure Firewall Adaptive Security Appliance (ASA).

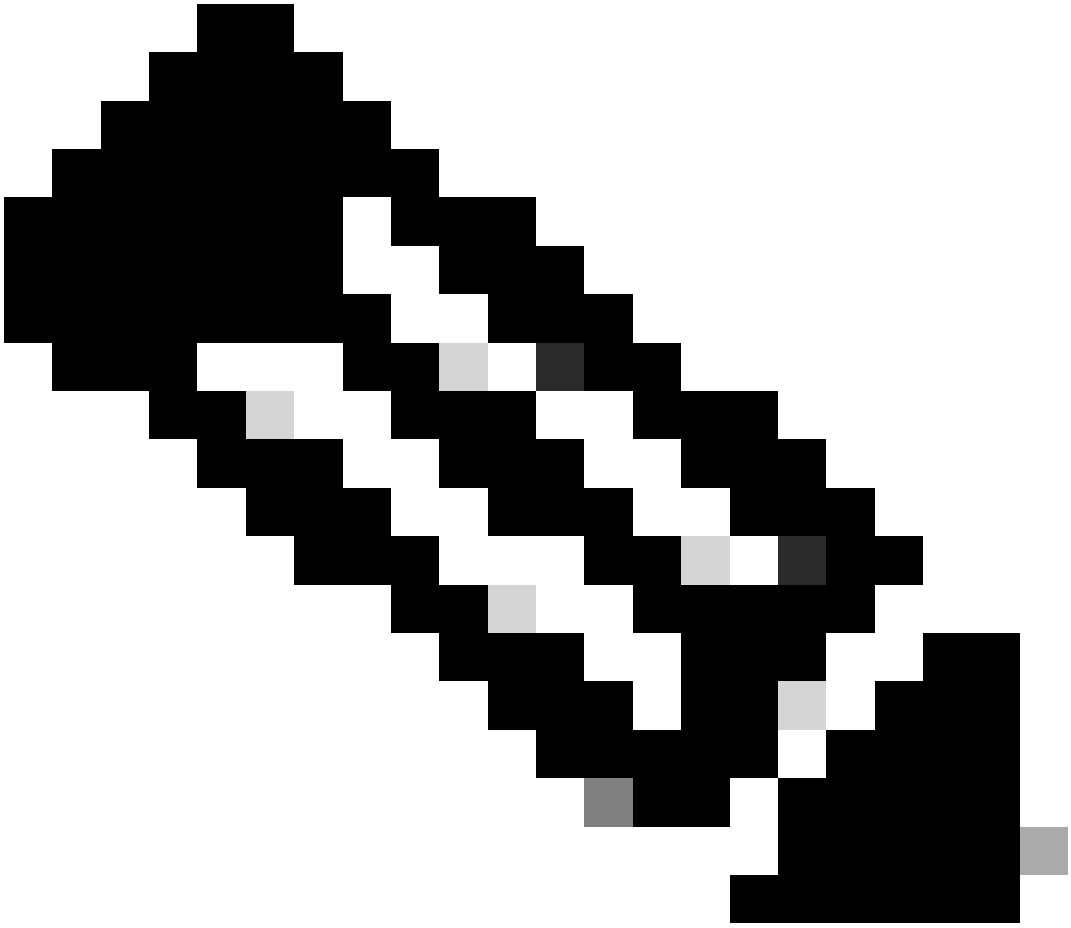
MGCP

Le protocole MGCP (Media Gateway Control Protocol) est un protocole utilisé pour le contrôle des appels VoIP par un périphérique de contrôle d'appel, par exemple CUCM.

Le protocole de signalisation MGCP est défini sur le document RFC 2705 et utilise les ports TCP 2428 et UDP 2427 pour la communication.

Les paquets normaux MGCP que vous attendez pour une communication d'appel sont :



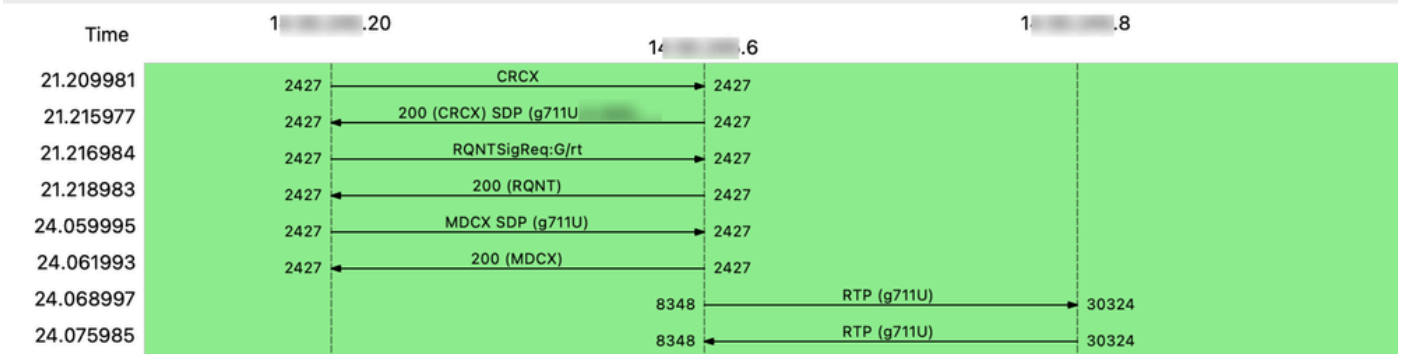


> Remarque : L'inspection MGCP n'est pas activée dans la stratégie d'inspection par défaut sur Cisco Secure Firewall Threat Defense (FTD) et Secure Firewall Adaptive Security Appliance (ASA). Vous devez donc l'activer si vous avez besoin de cette inspection.

Cette capture de paquets affiche les requêtes et les réponses de deux périphériques MGCP, ainsi que le trafic média (vocal) :

No.	Time	Source	Destination	Protocol	Length	Info
12	21.209981	1[redacted].20	1[redacted].6	MGCP	213	CRCX 509 S0/SU1/DS1-0/1@[redacted] MGCP 0.1
13	21.215977	1[redacted].6	1[redacted].20	MGCP/SDP	213	200 509 OK
14	21.216984	1[redacted].20	1[redacted].6	MGCP	144	RQNT 511 S0/SU1/DS1-0/1@[redacted] MGCP 0.1
18	21.218983	1[redacted].6	1[redacted].20	MGCP	57	200 511 OK
20	24.059995	1[redacted].20	1[redacted].6	MGCP/SDP	342	MDCX 513 S0/SU1/DS1-0/1@[redacted] MGCP 0.1
21	24.061993	1[redacted].6	1[redacted].20	MGCP	57	200 513 OK
22	24.068997	1[redacted].6	1[redacted].8	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7AE2, Seq=5377, Time=584785512
23	24.075985	1[redacted].8	1[redacted].6	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0xF22F508, Seq=39645, Time=128207581
24	24.088985	1[redacted].6	1[redacted].8	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7AE2, Seq=5378, Time=584785672
25	24.095988	1[redacted].8	1[redacted].6	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0xF22F508, Seq=39646, Time=128207741
26	24.108988	1[redacted].6	1[redacted].8	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7AE2, Seq=5379, Time=584785832
27	24.115991	1[redacted].8	1[redacted].6	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0xF22F508, Seq=39647, Time=128207901

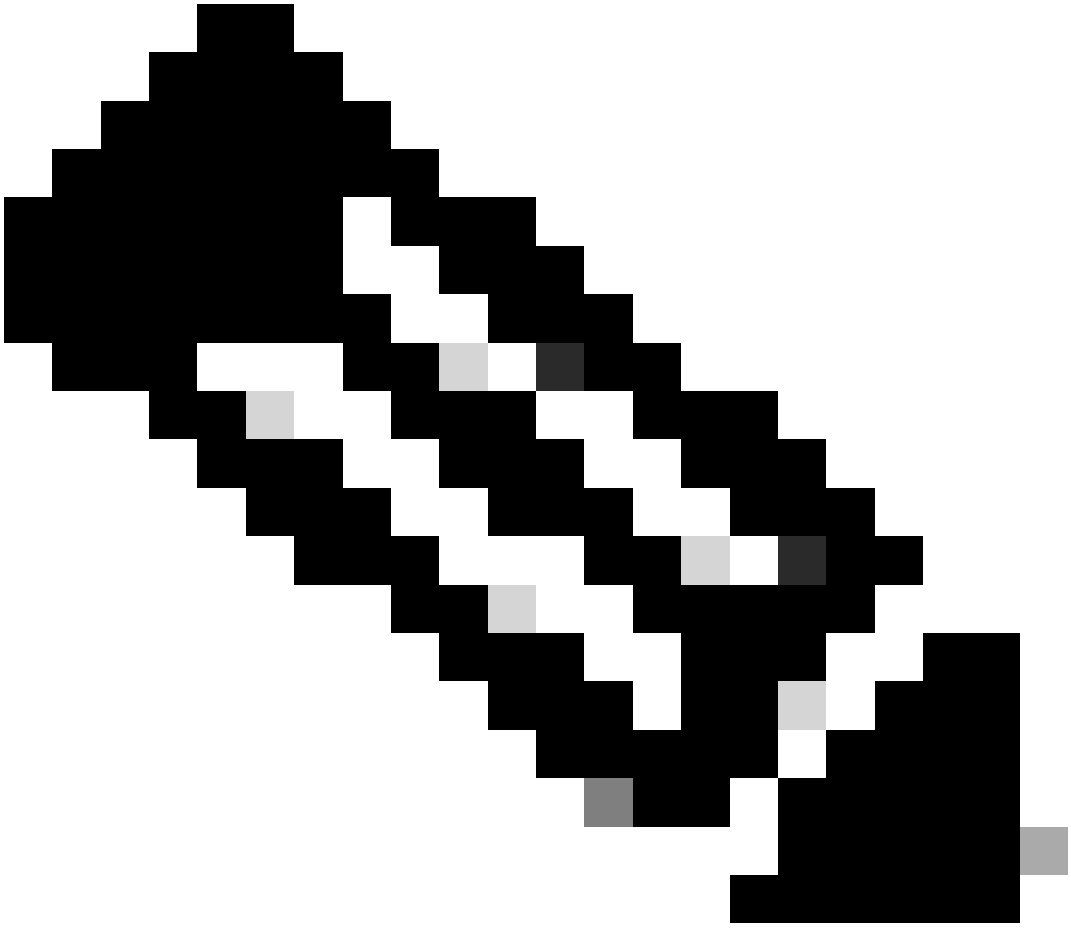
Voici un exemple de flux de signalisation MGCP et de média RTP (voix) :



Meilleures pratiques

Pour ASA :

- Utilisez une règle d’autorisation qui autorise le trafic vers et depuis les deux composants de signalisation (périphériques ou serveurs). Cela peut être limité par les ports utilisés sur le protocole VoIP de signalisation spécifié.
- Autorisez la plage de ports RTP entre les périphériques multimédias qui peuvent envoyer et/ou recevoir des flux audio et/ou vidéo.



Remarque : N'oubliez pas que ces périphériques audio ou multimédias peuvent être différents des composants de signalisation (périphériques ou serveurs).

Pour FTD :

- Définissez des règles de préfiltre pour les composants de signalisation (périphériques ou serveurs) et définissez le port spécifique pour limiter uniquement le trafic pour le protocole de signalisation spécifié.
- Configurez le préfiltre pour le protocole RTP audio et/ou vidéo.

Dépannage

Lors du dépannage de problèmes vocaux, vous devez savoir si le problème est de signalisation ou de support (voix ou vidéo) ou les deux, voici quelques exemples qui peuvent vous aider à différencier ceci :

Exemple de problèmes de signalisation :

++L’utilisateur signale que l’appel n’est pas établi.

++L’utilisateur ne peut pas appeler d’autres utilisateurs ou numéros.

++La ligne principale SIP ne s’affiche pas, car le message SIP OPTIONS ne reçoit pas de réponse.

++Mon appareil ne peut pas s'enregistrer.

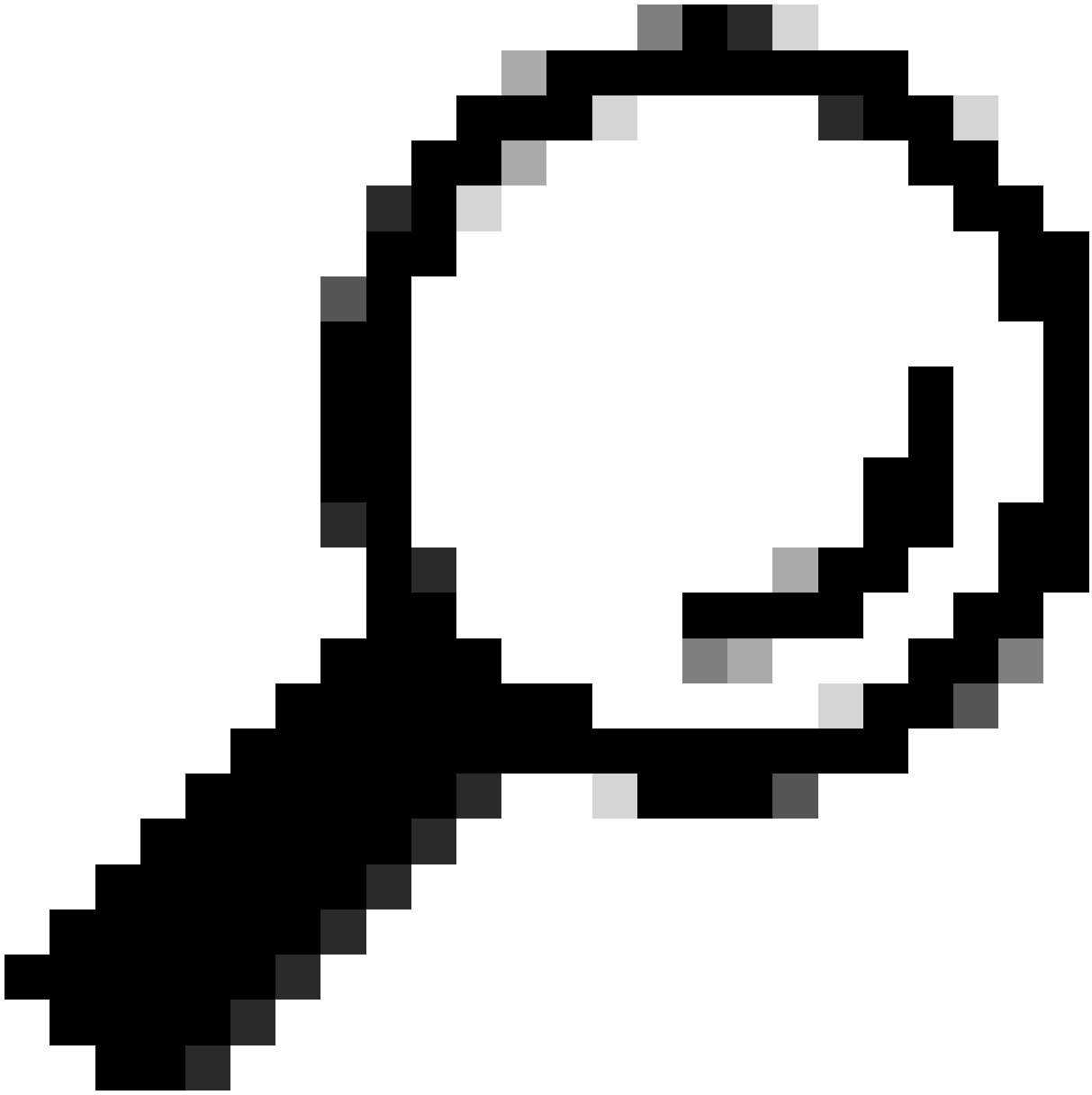
Exemple de problèmes de support (voix ou vidéo) :

++Il y a un problème audio unidirectionnel.

++Il n’y a pas d’audio sur appel.

++Il n’y a aucune vidéo.

++L’appel est silencieux.



Conseil : Pendant un appel vidéo, le SDP peut négocier jusqu'à trois lignes média (m-lignes) : audio, vidéo et image. Chaque ligne m correspond à un flux RTP (Real-Time Transport Protocol) distinct par branche d'appel, ce qui signifie qu'il peut y avoir jusqu'à trois flux RTP distincts, un pour chaque type de support, sur chaque branche de l'appel.

Dépannage des problèmes de signalisation sur le pare-feu

Pour le dépannage de la partie signalisation, vous devez vous assurer de :

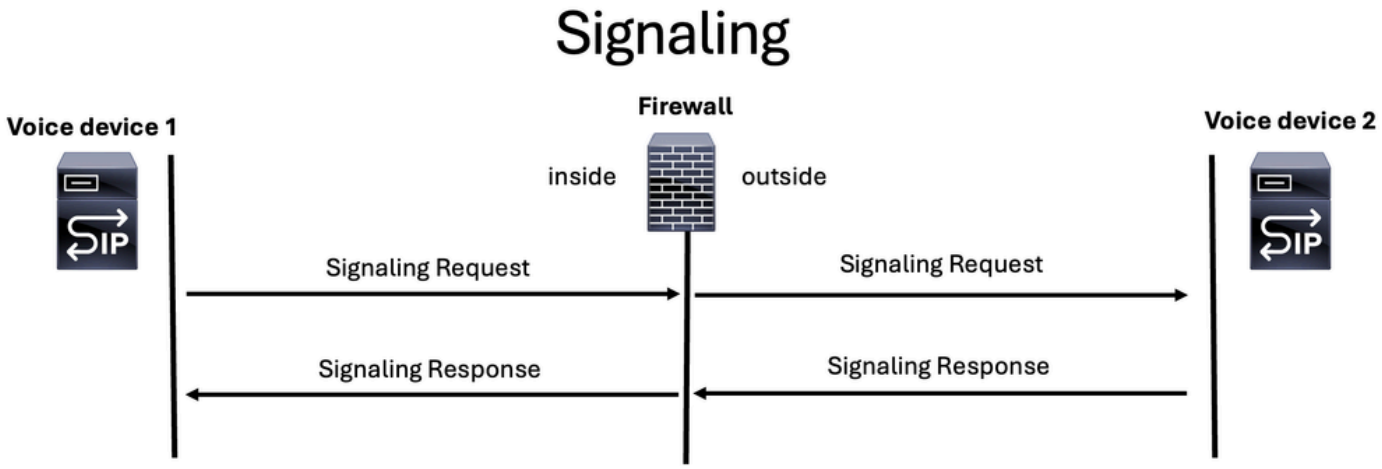
++Identifiez tous les composants de signalisation (périphériques ou serveurs) impliqués dans l'appel à partir de l'interface d'entrée et de sortie et configurez les critères de correspondance appropriés sur les captures de paquets sur l'interface de ligne de commande de Secure FW.

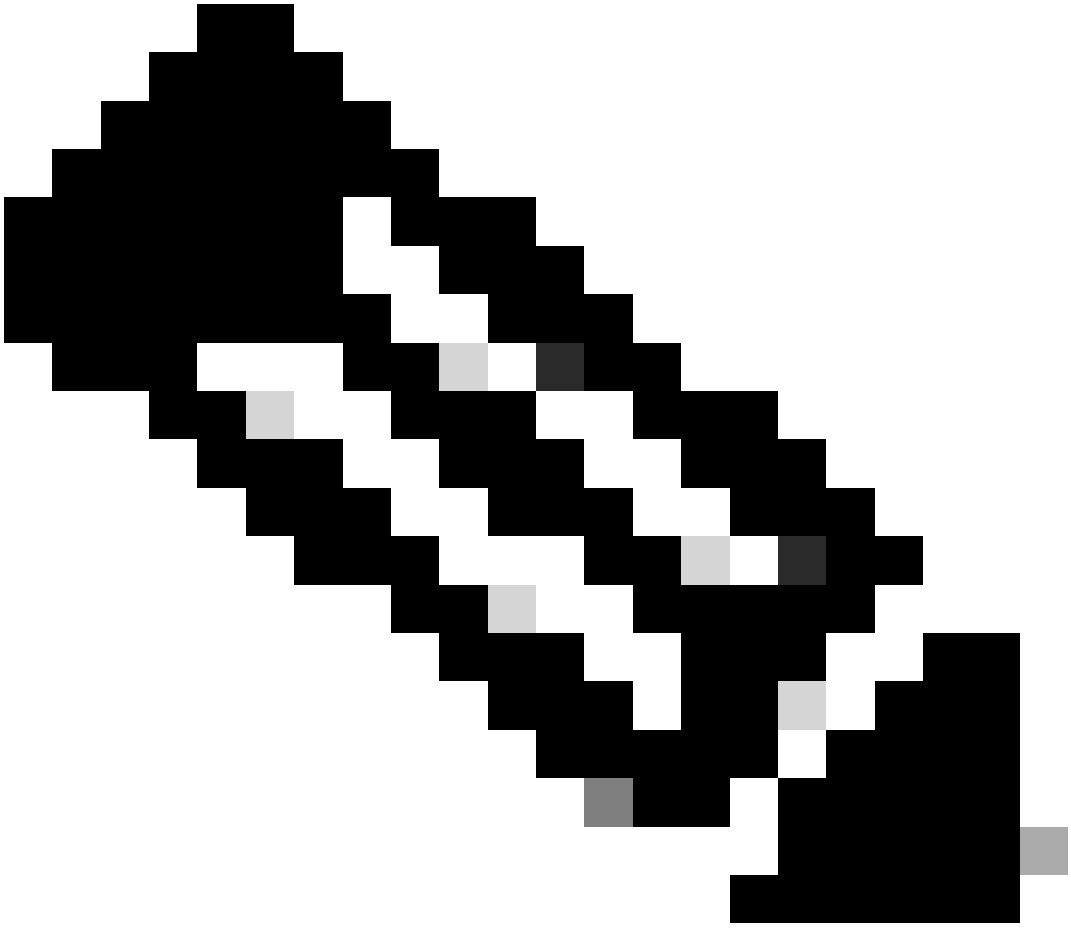
++Souvenez-vous que le nombre de messages de signalisation à l'interface d'entrée doit

correspondre à l’interface de sortie.

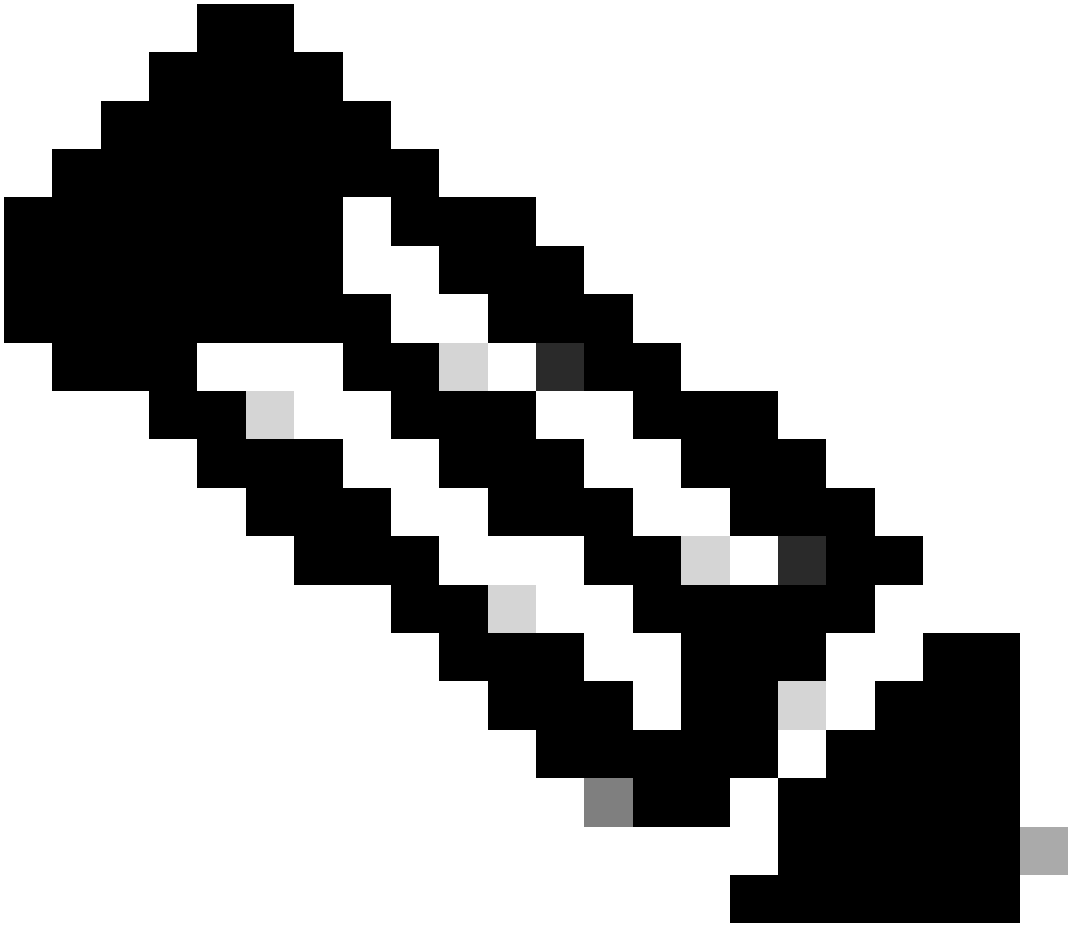
++La capture de paquets peut être plus efficace en spécifiant si le protocole de signalisation utilise TCP ou UDP et en filtrant le numéro de port attendu. Comme tous les protocoles de signalisation fonctionnent sur IP, l’application de ces filtres sur l’interface de ligne de commande permet de limiter la quantité de trafic que vous voyez dans vos captures.

++Pour les interfaces de sortie uniquement, assurez-vous que l’adresse IP NAT attribuée au trafic sortant est spécifiée dans votre filtre de capture de paquets. Vous êtes ainsi assuré de capturer le trafic correct tel qu’il apparaît sur l’interface de sortie.





Remarque : n'oubliez pas que, quel que soit le protocole de signalisation utilisé pour la voix, il doit toujours y avoir une requête et une réponse, et doit être cohérent sur les interfaces d'entrée et de sortie.

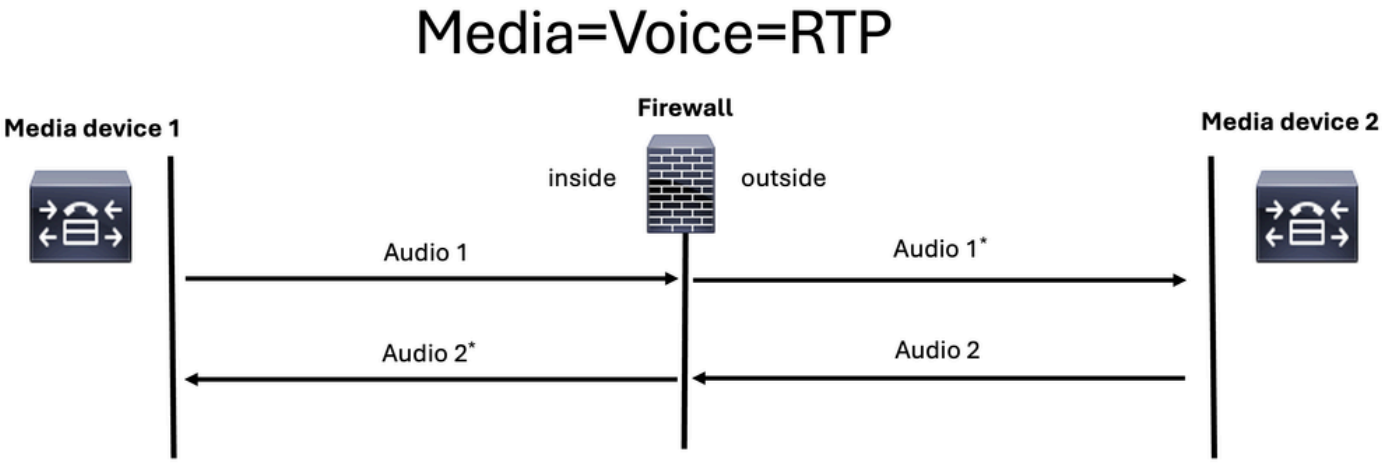


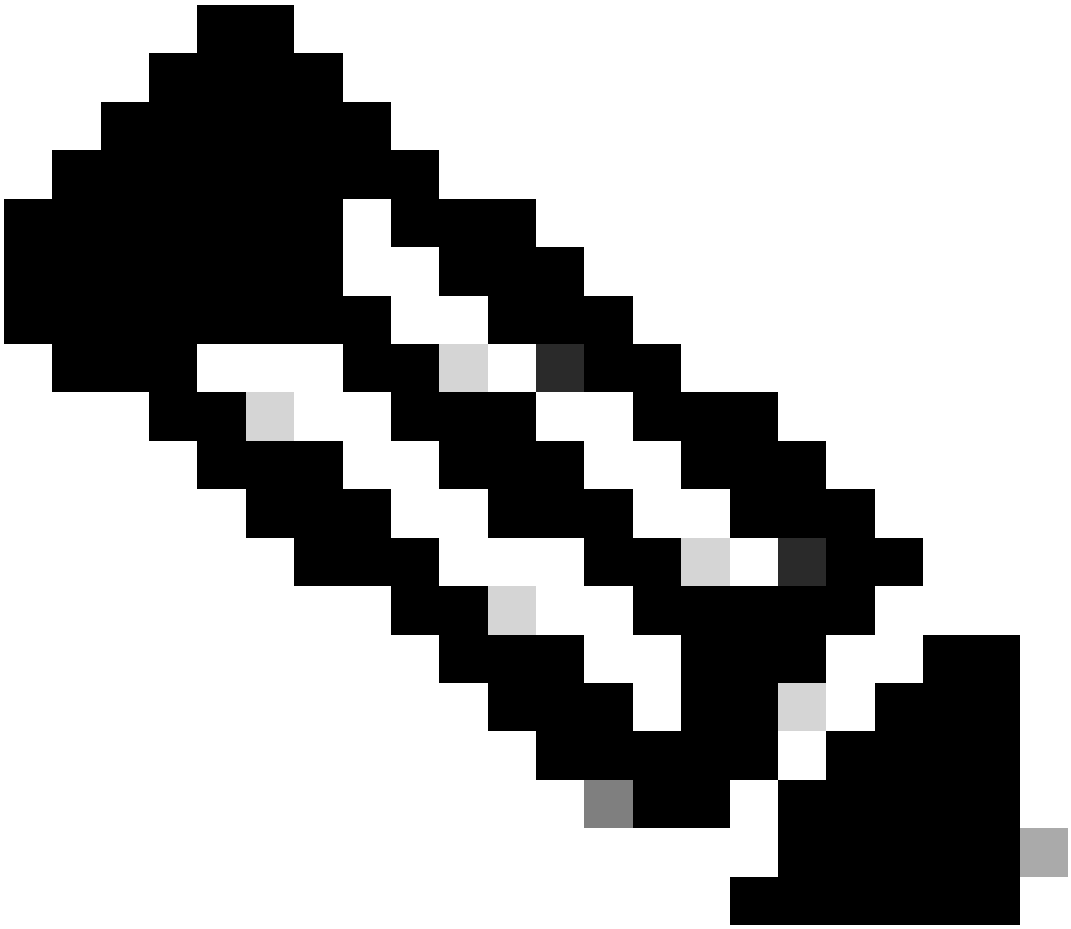
Remarque : dans la mesure du possible, assurez-vous qu'un seul pare-feu est impliqué dans le chemin de communication. Dans certains déploiements, la signalisation vocale et les flux multimédias peuvent traverser des pare-feu distincts. Dans ce cas, veillez à inclure tous les pare-feu appropriés dans votre processus de dépannage

Dépannage des problèmes de support sur le pare-feu

Du point de vue du pare-feu, 4 flux doivent être analysés lors du dépannage de problèmes audio unidirectionnels, bidirectionnels ou sans audio :

1. Flux RTP de l'appelant vers l'appelé (interface d'entrée).
2. Flux RTP de l'appelant vers l'appelé (interface de sortie).
3. Flux RTP de l'appelant à l'appelant (interface de sortie).
4. Flux RTP de l'appelant à l'appelant (interface d'entrée).



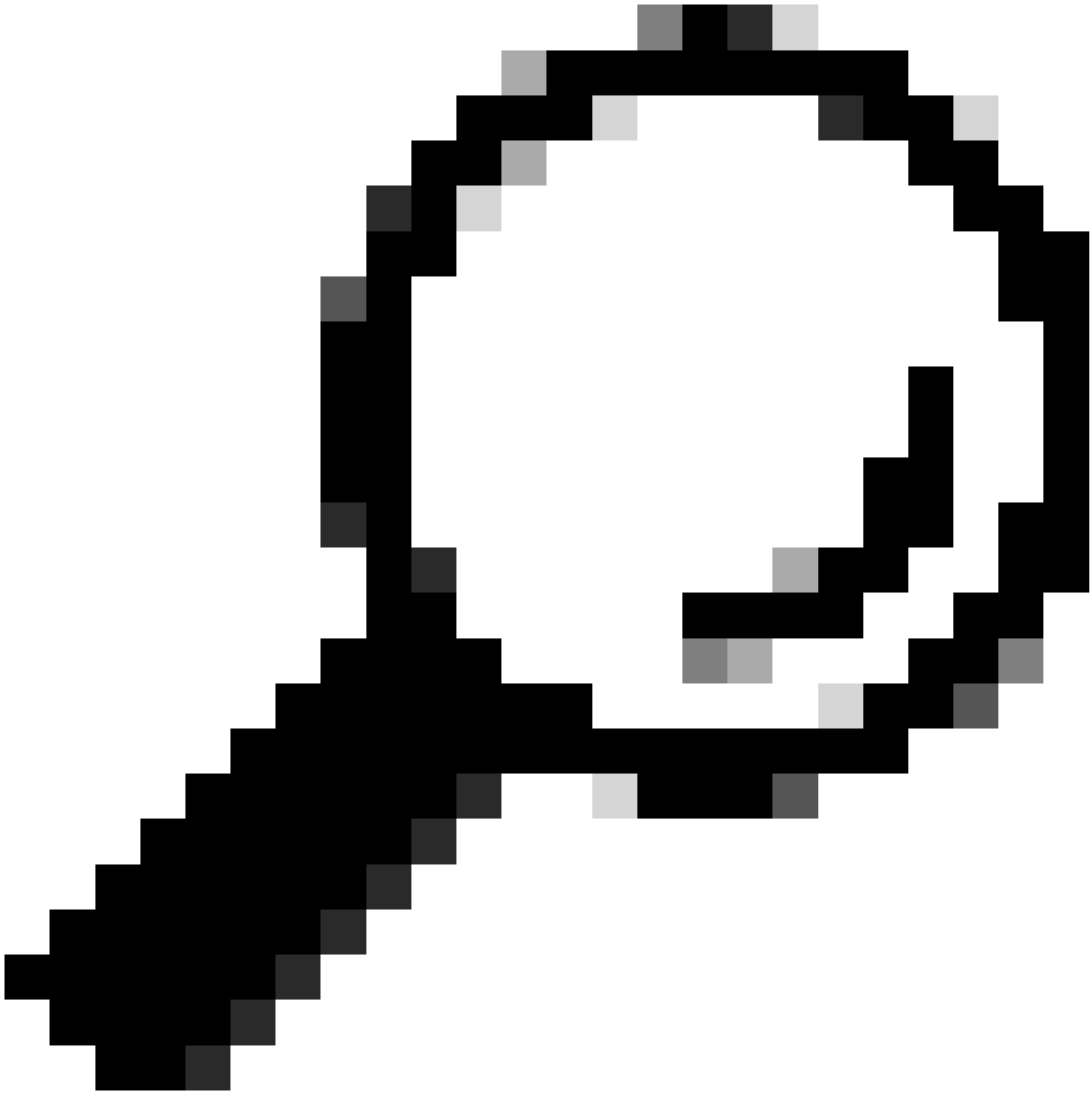


Remarque : Assurez-vous d'effectuer le dépannage à l'aide des captures de paquets CLI en mode ASA ou LINA sur le FTD, car cela offre une plus grande flexibilité pour appliquer plusieurs correspondances dans une capture de paquets unique.

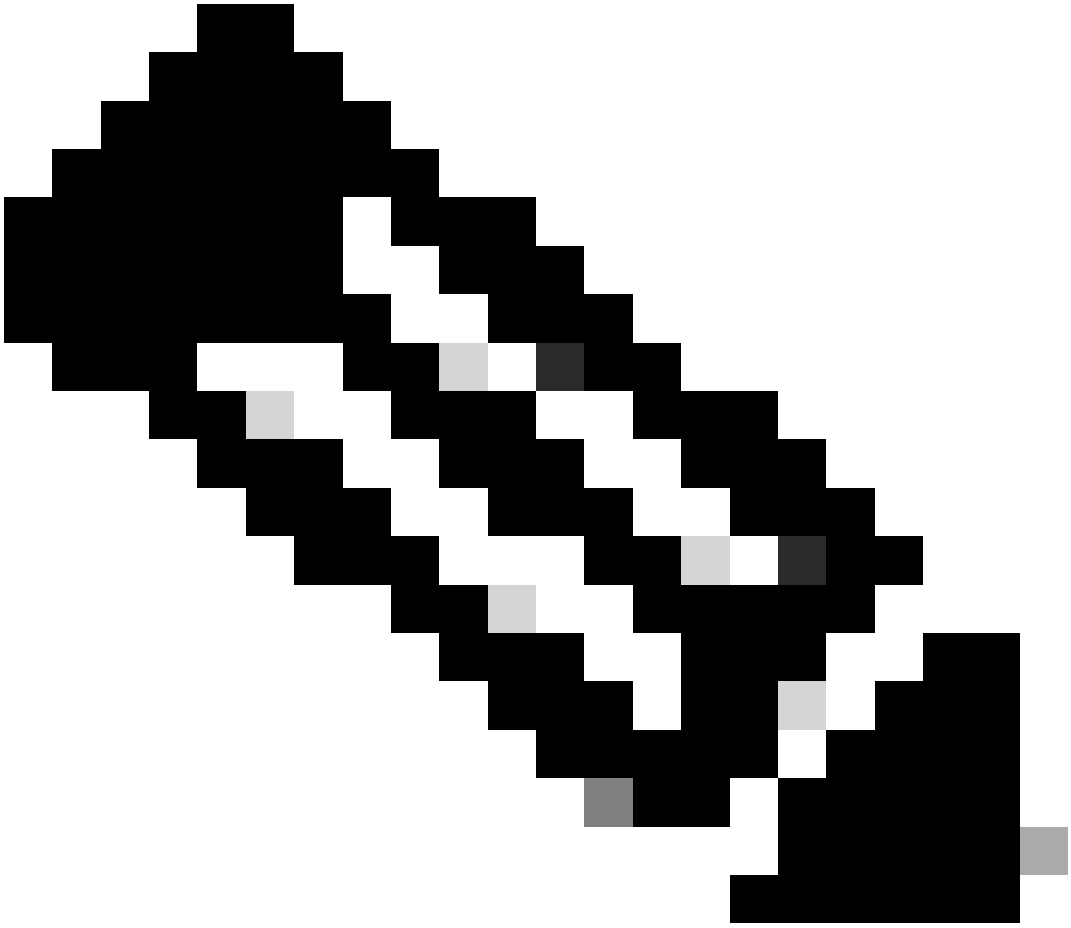
Dépannage des appels SIP

Lors du dépannage de problèmes vocaux sur un pare-feu sécurisé (ASA ou FTD), vous devez effectuer les étapes suivantes :

1. Assurez-vous de disposer du flux d'appels et du schéma de topologie.
2. Assurez-vous de comprendre le problème du point de vue de l'utilisateur.
3. Comprendre le chemin du protocole de signalisation.
4. Comprendre le chemin du protocole RTP de support.
5. Effectuez des captures de paquets sur les interfaces d’entrée et de sortie.
6. Examinez les règles de configuration ACL et NAT.
7. Vérifiez que le trafic de signalisation SIP n'est pas bloqué par le pare-feu. En outre, comparez les interfaces d'entrée et de sortie pour analyser le flux du trafic vocal.
8. Vérifiez que le trafic multimédia RTP n'est pas bloqué par le pare-feu en comparant le flux de trafic sur les interfaces d'entrée et de sortie.
9. Assurez-vous que les dispositifs de signalisation prennent en charge l'inspection et, si ce n'est pas le cas, désactivez-la.



Conseil : Les messages de signalisation SIP entrant dans le FW doivent également être identiques à ceux quittant le FW.



Remarque : Les conseils de dépannage de SIP peuvent également être appliqués aux protocoles H.323, MGCP et SCCP.

Informations connexes

- Configuration des captures de paquets ASA avec CLI
- Utiliser les captures Firepower Threat Defense

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.