Ken de basisprincipes van Voice over IP-protocollen voor veilige firewall

Inhoud

Inleiding

Dit document beschrijft de basisprincipes van verschillende VoIP-protocollen om technici te helpen bij het effectief oplossen van problemen op Secure Firewalls.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is bedoeld voor gebruik bij het oplossen van problemen met deze apparaten:

- Beveiligde Firewall Threat Defence (FTD)
- Secure Firewall Adaptive Security Appliance (ASA)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

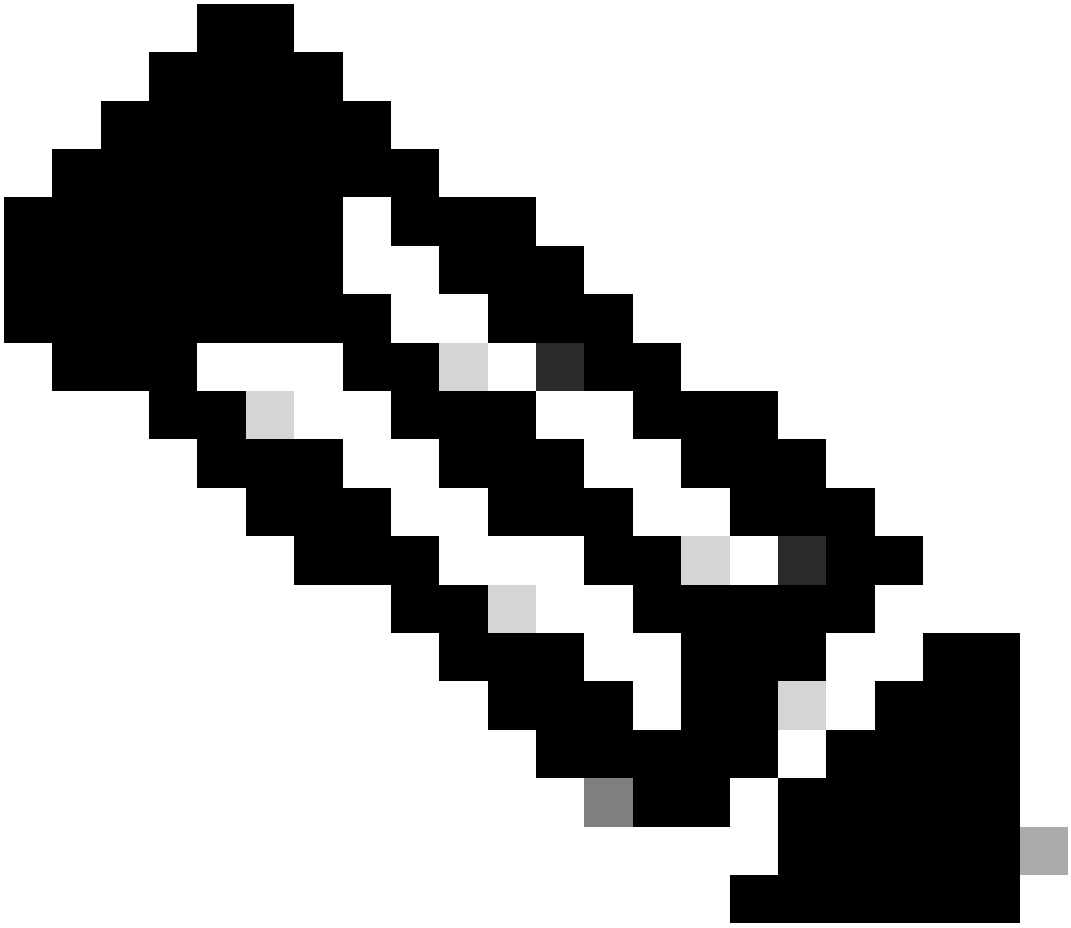
Basisprincipes van VoIP

Communicatie is fundamenteel voor menselijke interacties, Voice over IP (VoIP)-protocollen zijn onmisbaar geworden voor menselijke communicatie. Daarom is het belangrijk om hun onderdelen te kennen bij het oplossen van problemen met een scenario dat een firewall (FW) bevat.

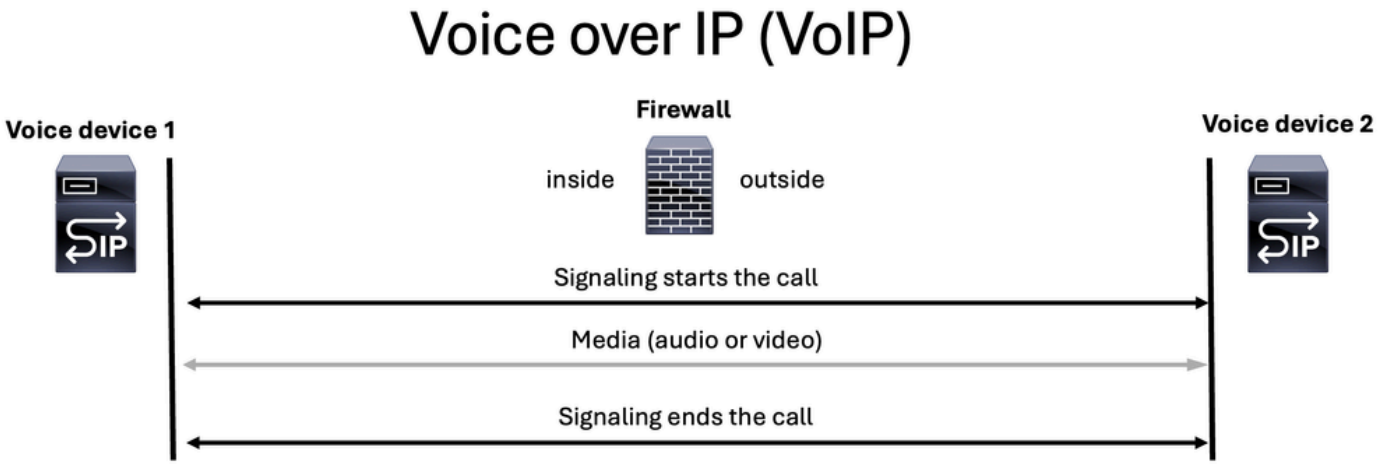
De VoIP bestaat uit twee delen:

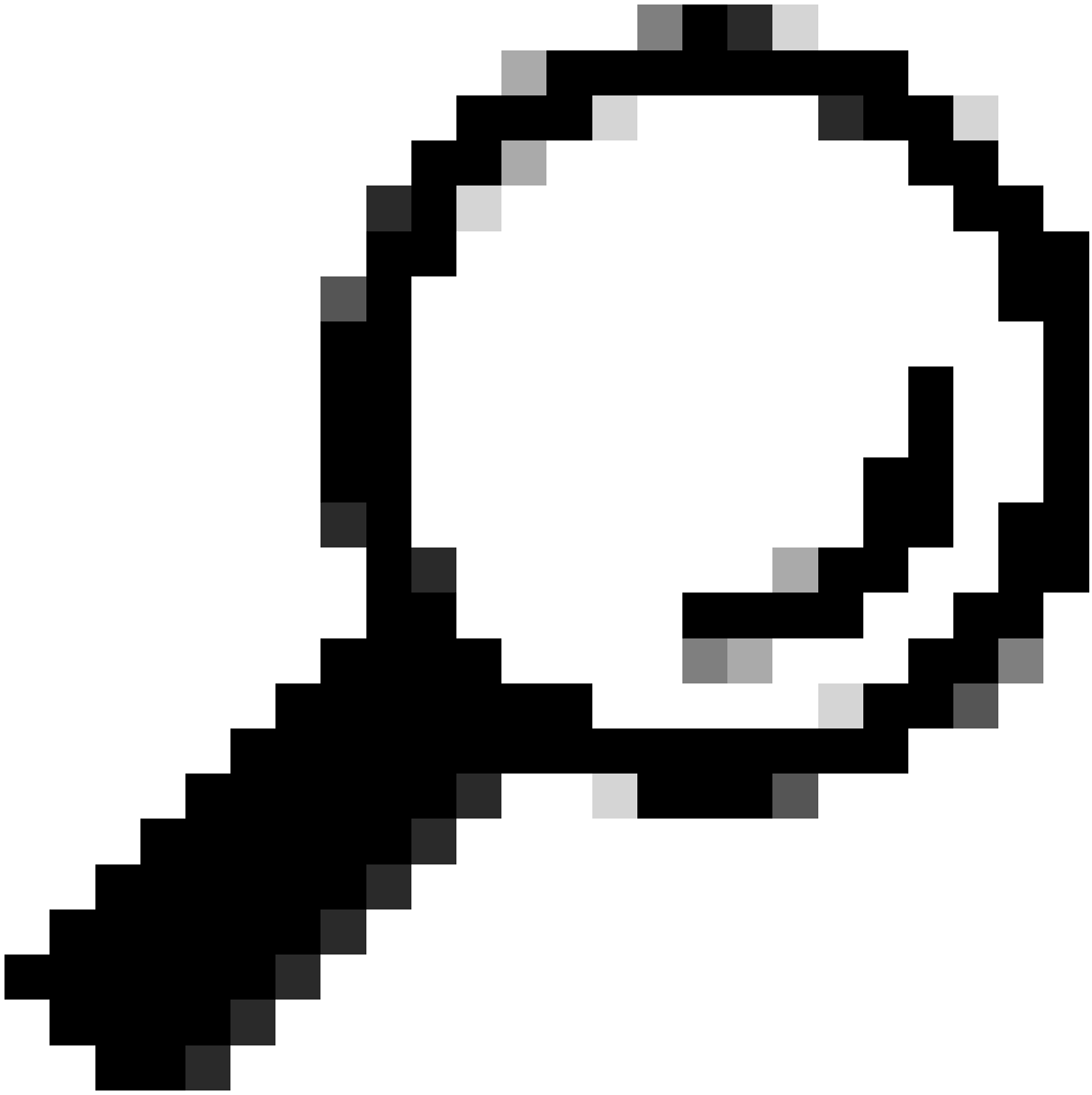
- Signalering
- Media (spraak of video)

VoIP-communicatie begint altijd met een signaleringsgedeelte om een gesprek te starten, vervolgens wordt de media (spraak of video) gestreamd en eindigt de signalering het gesprek.

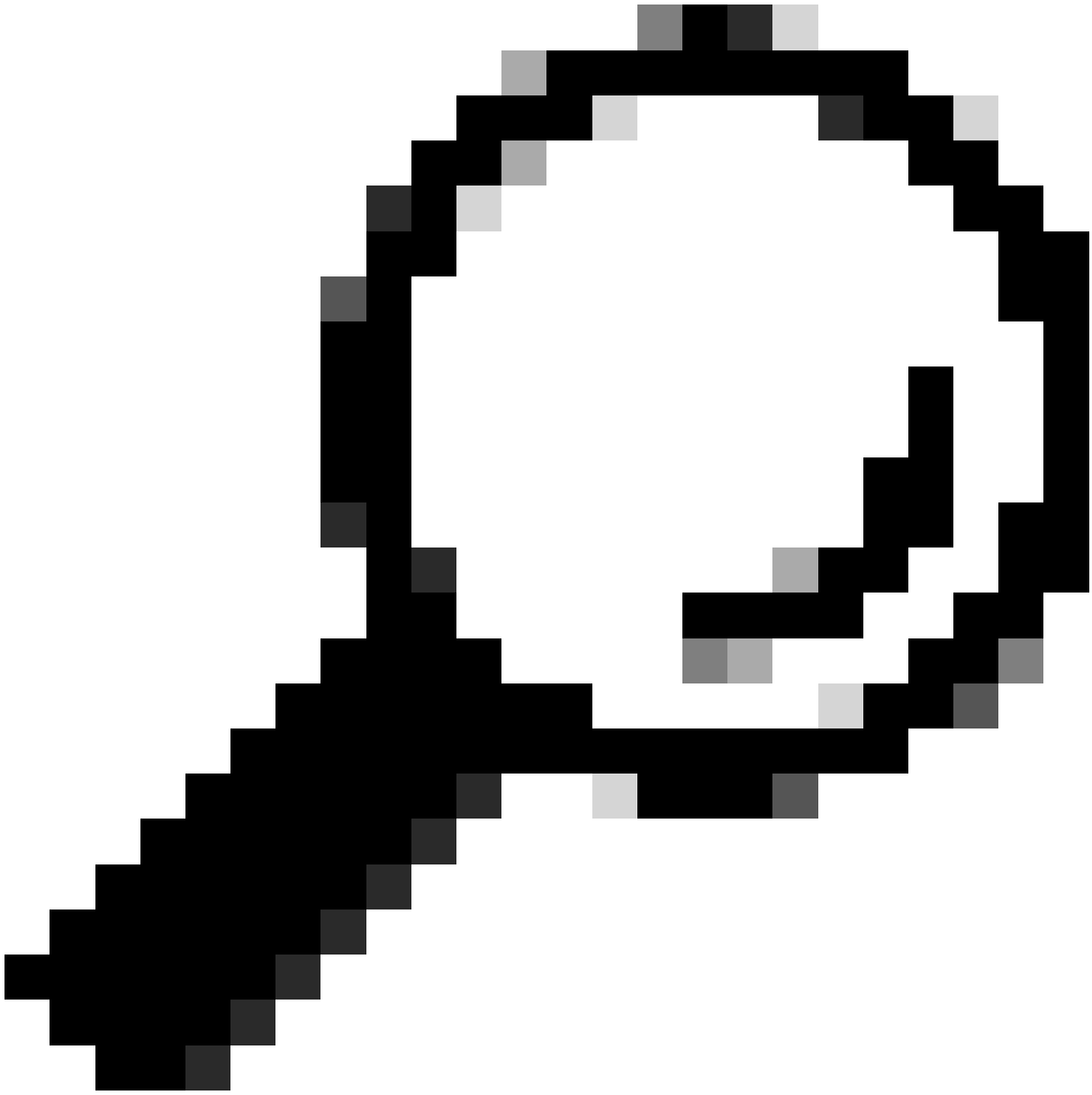


Opmerking: SIP is het meest gebruikte protocol, dus het wordt consequent weergegeven als het SIP-spraakserverpictogram in veel van de diagrammen.





Tip: Bij het oplossen van een spraakprobleem voor ASA of FTD is het cruciaal om het scenario vanuit het perspectief van de gebruiker te bekijken. U moet bepalen of het gesprek tot stand is gebracht of dat er geen audio of eenrichtingsaudio is. Deze informatie geeft waardevolle aanwijzingen over de vraag of het probleem ligt bij het signaleringsprotocol of het media-protocol (spraak of video).



Tip: Een spraakapparaat kan zowel het RTP-verkeer (Voice Real-time Transport Protocol), het signaleringsverkeer of beide tegelijkertijd beheren. Bij het oplossen van stemproblemen is het essentieel om deze hoofdconcepten te onthouden:

++signaleringsservers: Deze servers zijn verantwoordelijk voor het afhandelen van alleen signaleringsverkeer.

++Mediaservers: Deze servers verwerken uitsluitend RTP-verkeer.

++Sommige apparaten kunnen beide taken aan.

Signalering

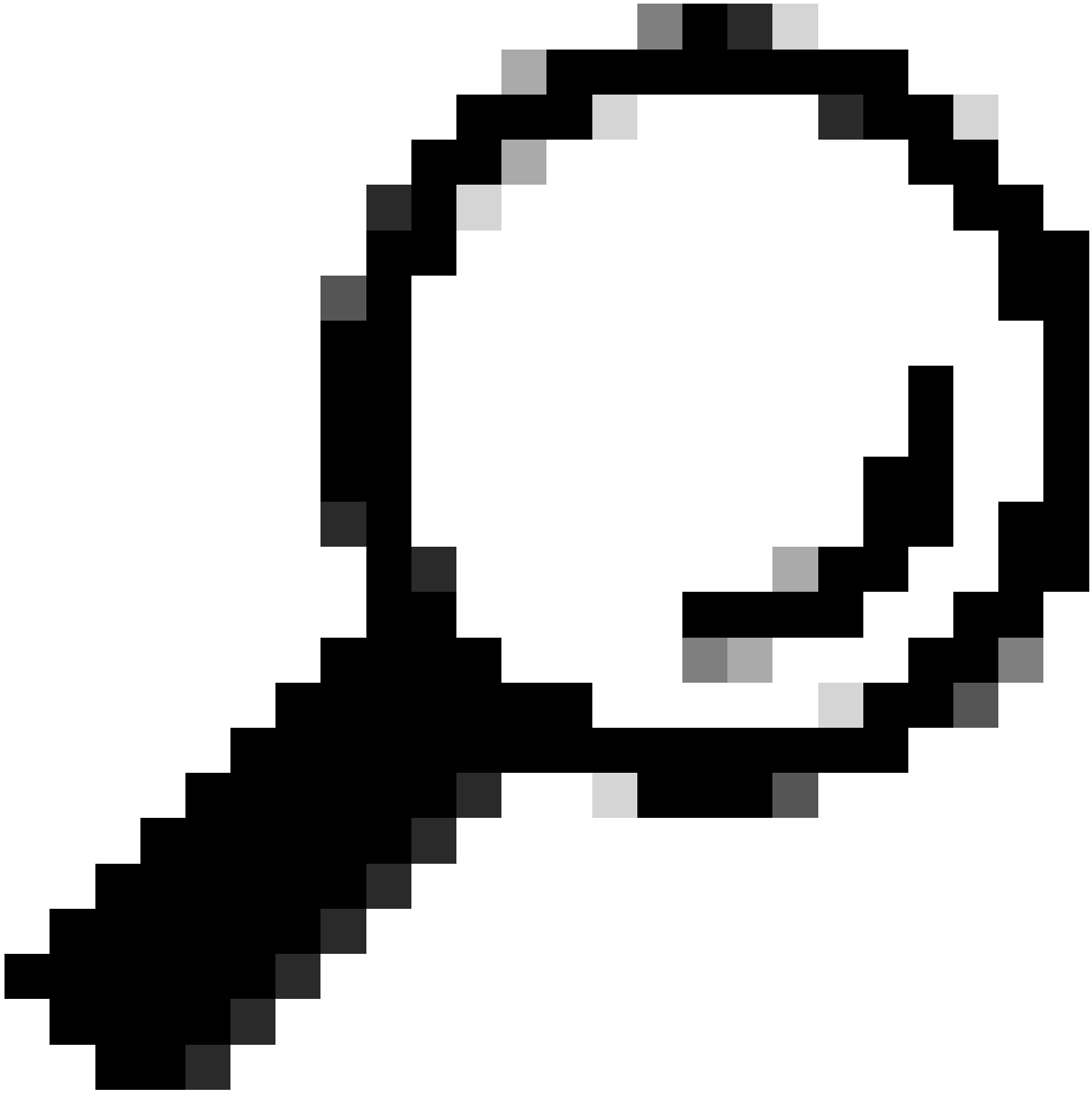
Het signaleringsprotocol is het deel van een oproep dat de spraakcommunicatie start, maar niet

alleen dat, het voert ook deze functies uit:

- Houdt de communicatie op peil.
- Wijzigt de communicatie.
- Beëindigt de communicatie.

Verschillende soorten signaleringsprotocollen helpen een oproep tot stand te brengen en de meest voorkomende zijn:

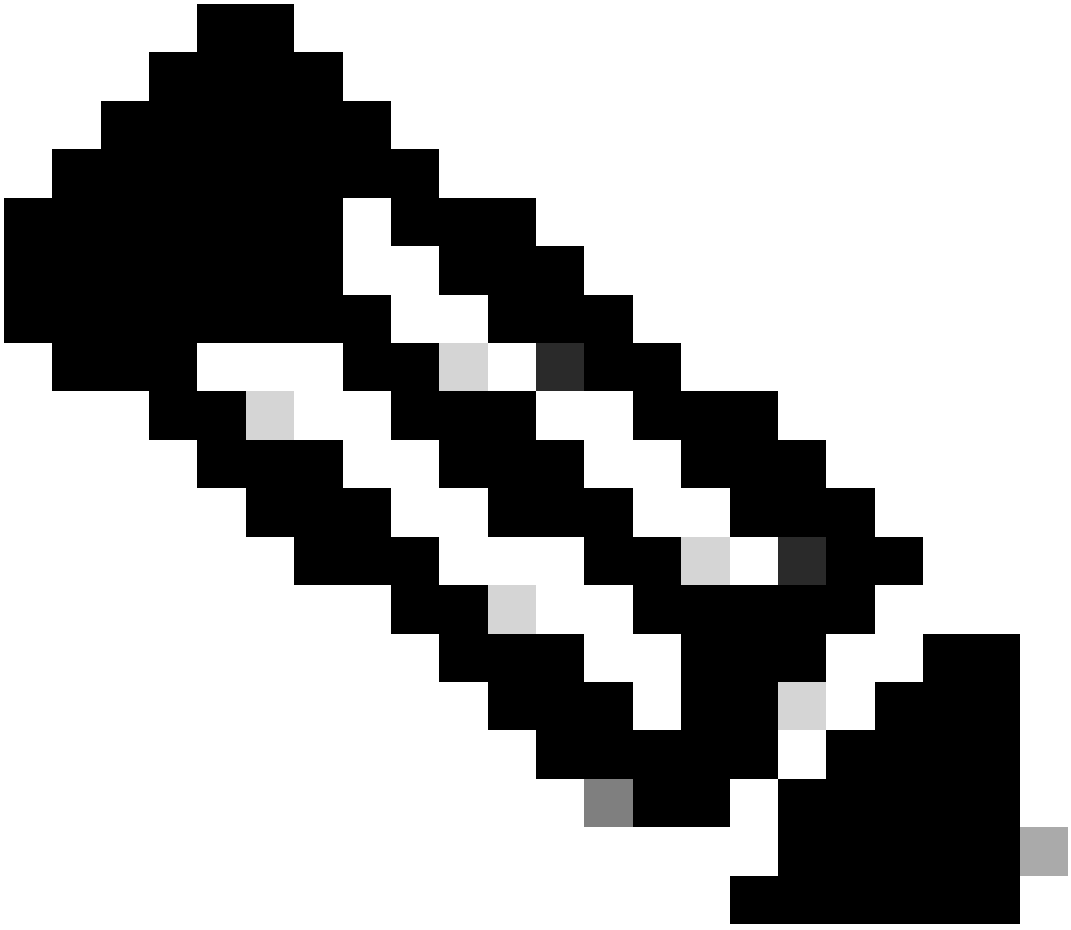
- Session Initiation Protocol (SIP)
- H.323
- Media Gateway Control Protocol (MGCP)
- Skinny Call Control Protocol (SCCP)



Tip: Het is essentieel om het gebruikte signaleringsprotocol te identificeren om de juiste

---

poorten voor pakketopname op ASA of FTD te bepalen. Bovendien is het hebben van een oproepstroom en netwerktopologie gunstig voor het begrijpen van het signaleringspad.

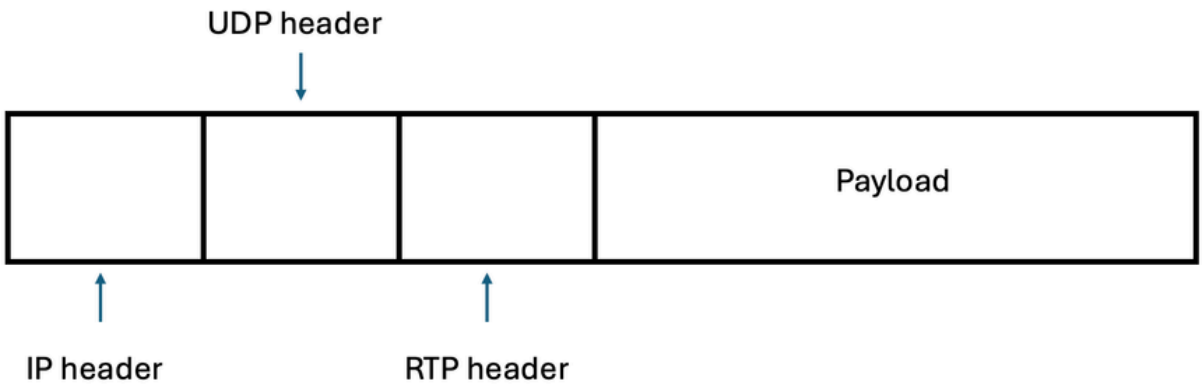


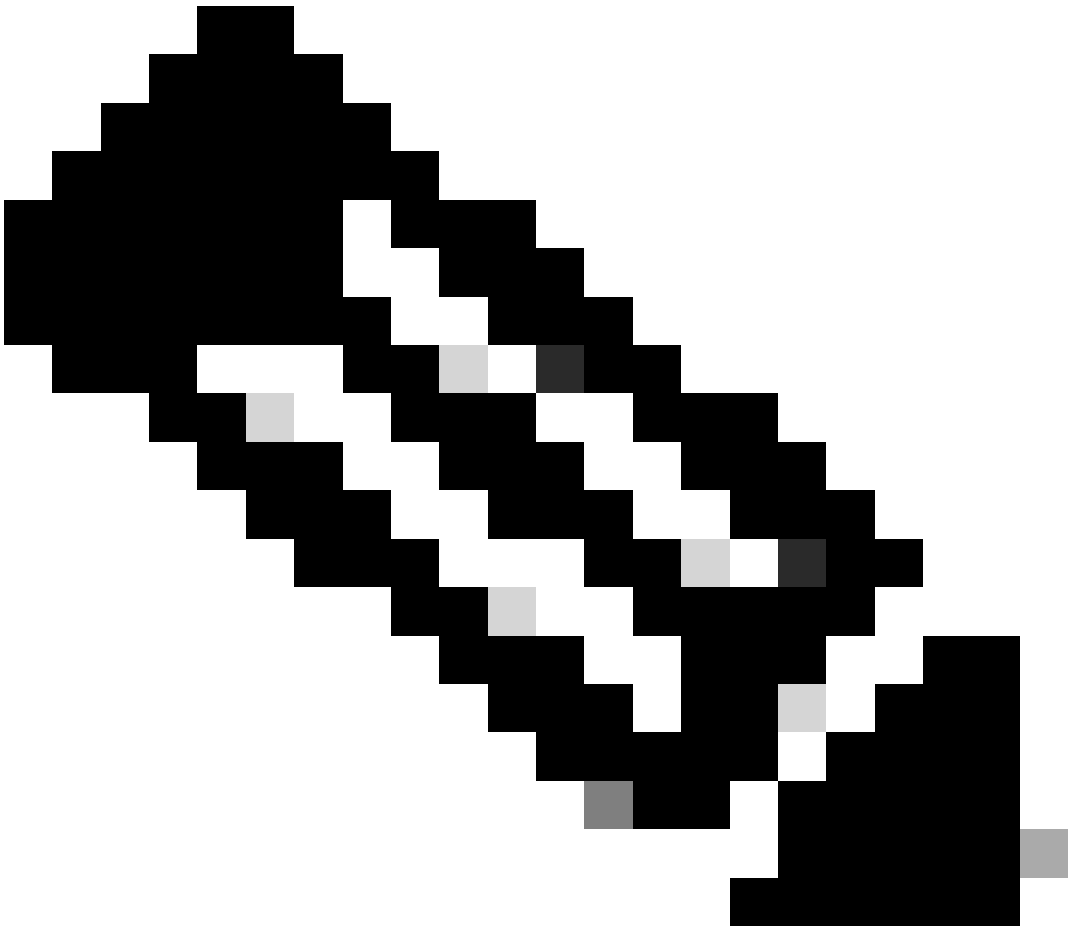
Opmerking: Signaleringspakketten bevatten bron- en bestemmings-IP-adressen, wat helpt bij de identificatie van de partijen die betrokken zijn bij het verzenden en ontvangen van de RTP-mediastroom.

media

Nadat de signalering is voltooid en de signaleringscomponenten (apparaten of servers) het mediatype zijn overeengekomen, wordt het Real Time Protocol (RTP) gebruikt om media (audio en/of video) naar alle betrokken partijen te verzenden.

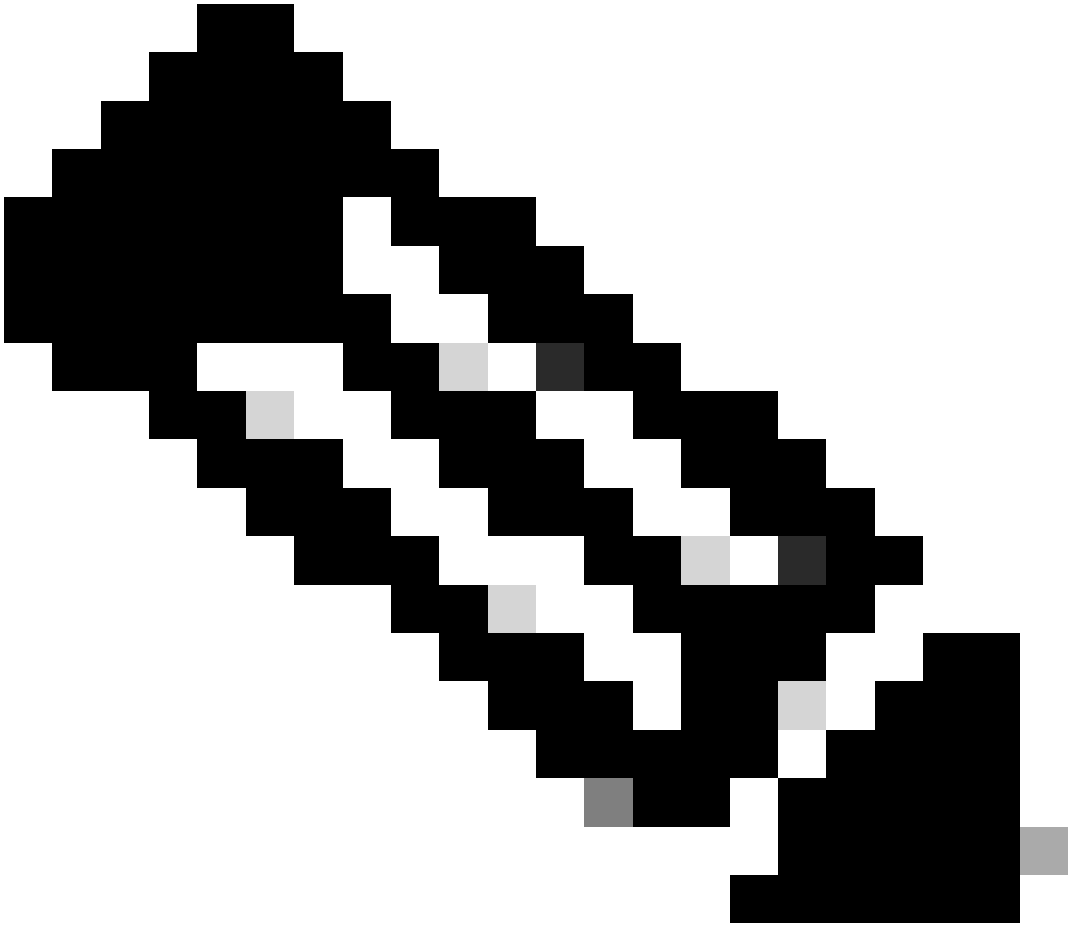
RTP is een internetprotocol dat wordt gebruikt voor het streamen van media en dat alleen wordt verzonden nadat de oproep is gemaakt en wordt uitgevoerd via het User Datagram Protocol (UDP).



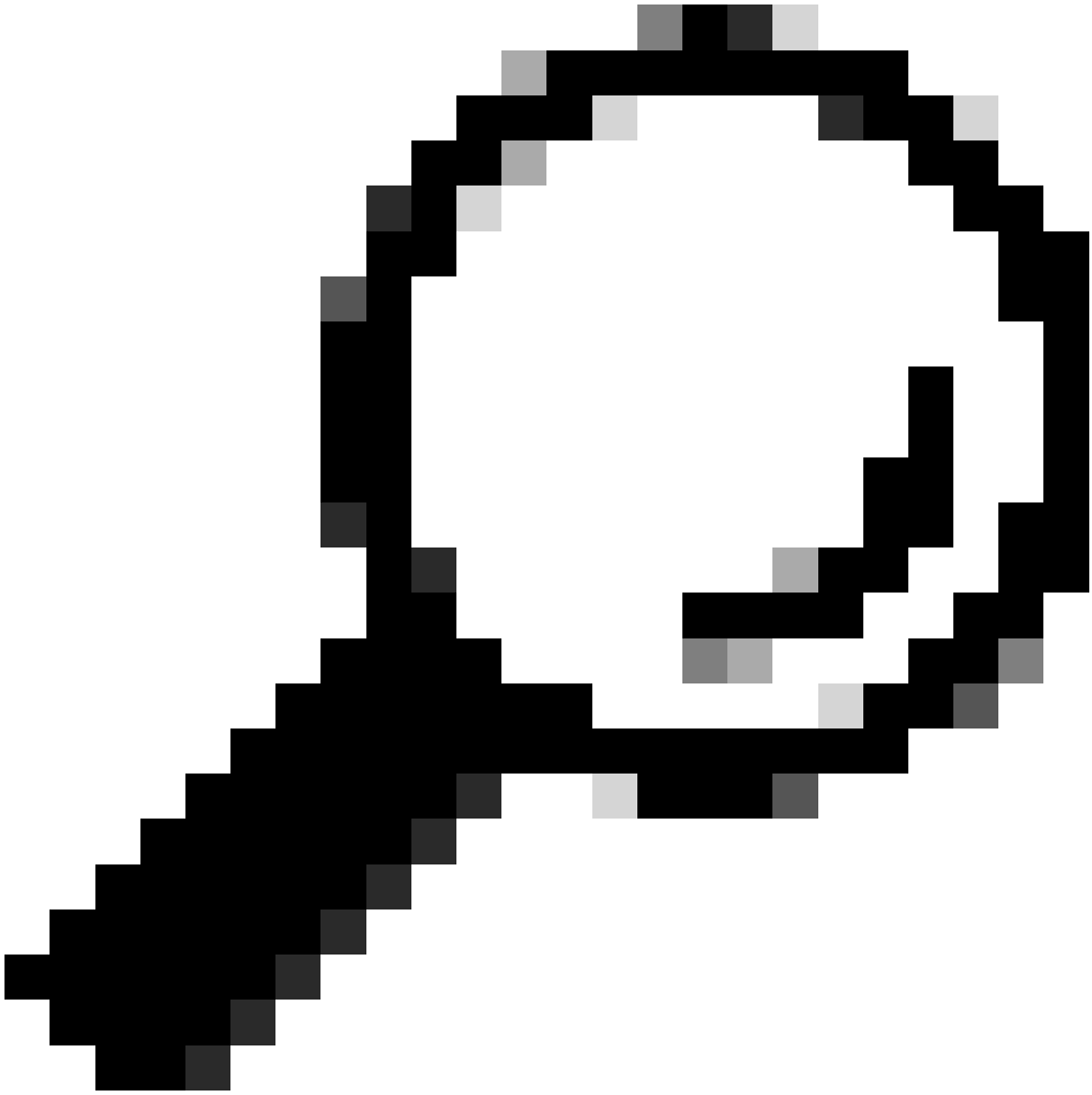


Opmerking: media kunnen spraak en/of video zijn en reizen op RTP-pakketten.

Signaleringscomponenten (apparaten of servers) bepalen welke poorten worden gebruikt voor het verzenden of ontvangen van media (audio en/of video). Het meest voorkomende poortbereik voor RTP is meestal tussen 16384 en 32767 voor de meeste apparaten.



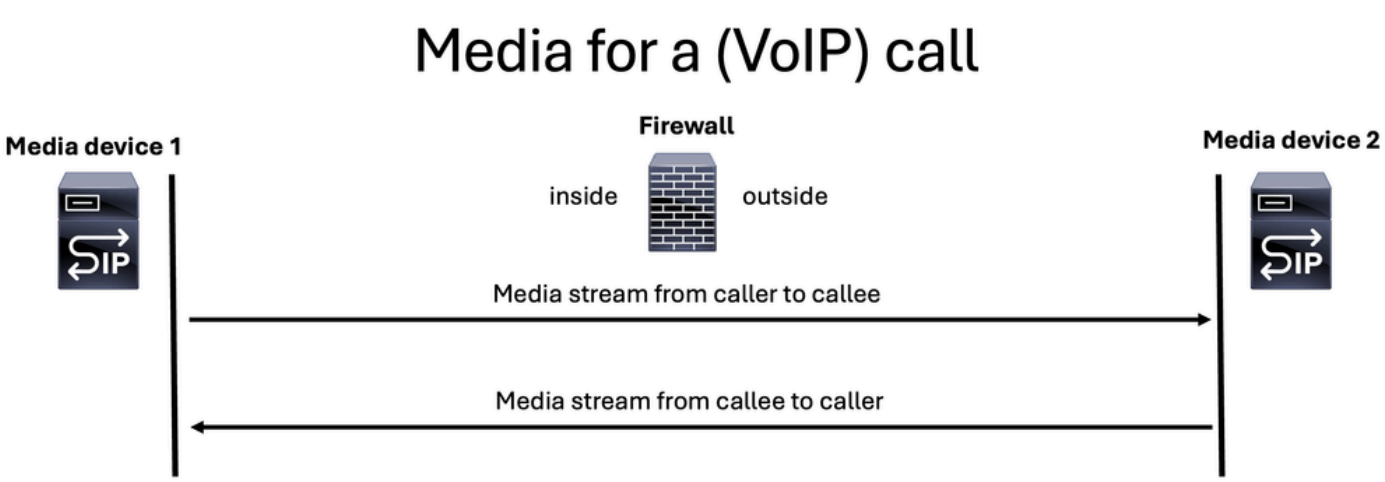
Opmerking: Bepaalde Cisco-apparaten, zoals de ASR- en ISR G3-platforms zoals het ISR4K-platform, maken gebruik van een gestandaardiseerd RTP-poortbereik van 8000 tot 48200. Het is van cruciaal belang om het specifieke RTP-poortbereik te controleren dat op uw apparaten is geconfigureerd, omdat het kan verschillen van deze gestandaardiseerde waarden en kan variëren tussen apparaten van derden.

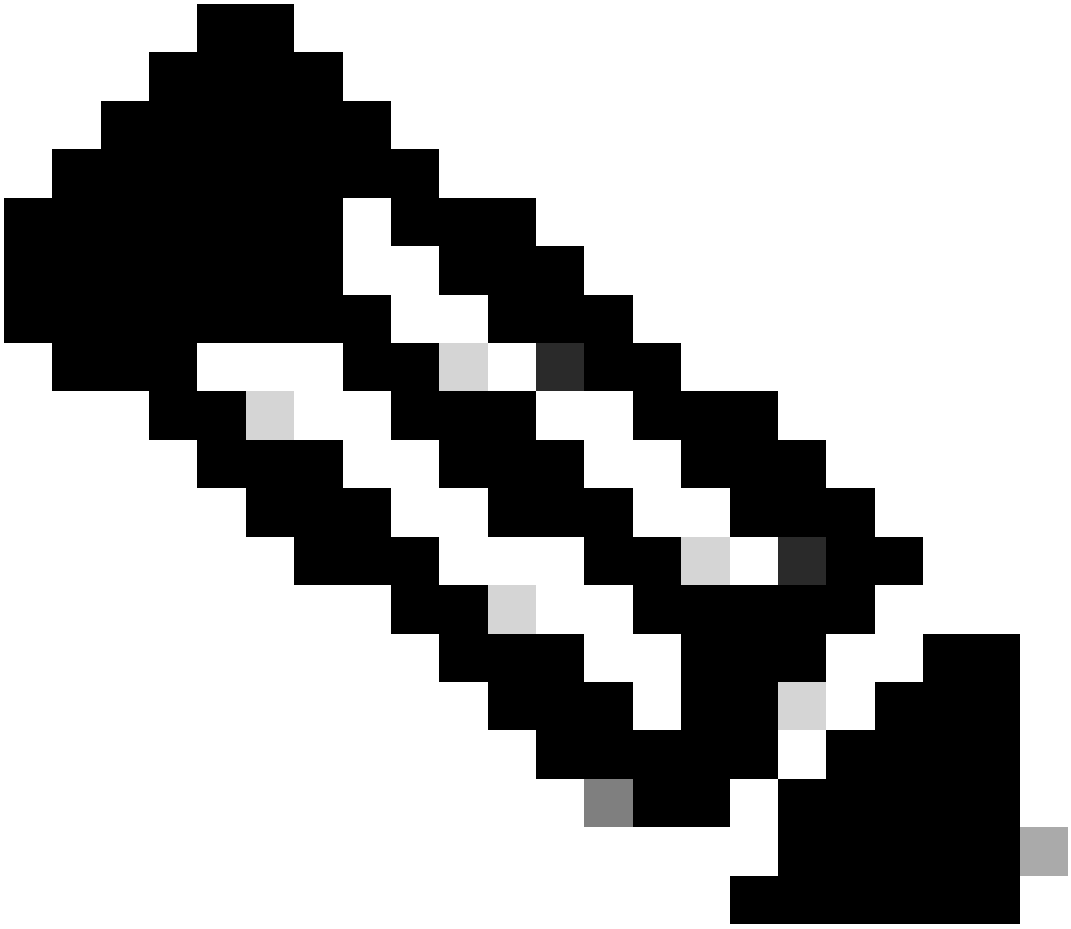


Tip: Soms verschilt het RTP-pad van het signaleringspad, waardoor het cruciaal is om de apparaten te identificeren die verantwoordelijk zijn voor het verzenden en ontvangen van RTP-spraakpakketten. Dit zorgt ervoor dat u UDP-verkeer tussen de apparaten die de ASA of FTD doorkruisen, kunt vastleggen.

Er zijn twee mediastromen of RTP-streams die worden gegenereerd op een normale spraakoproep:

1. Eén mediastroom van beller naar beller
2. Eén mediastroom van beller naar beller





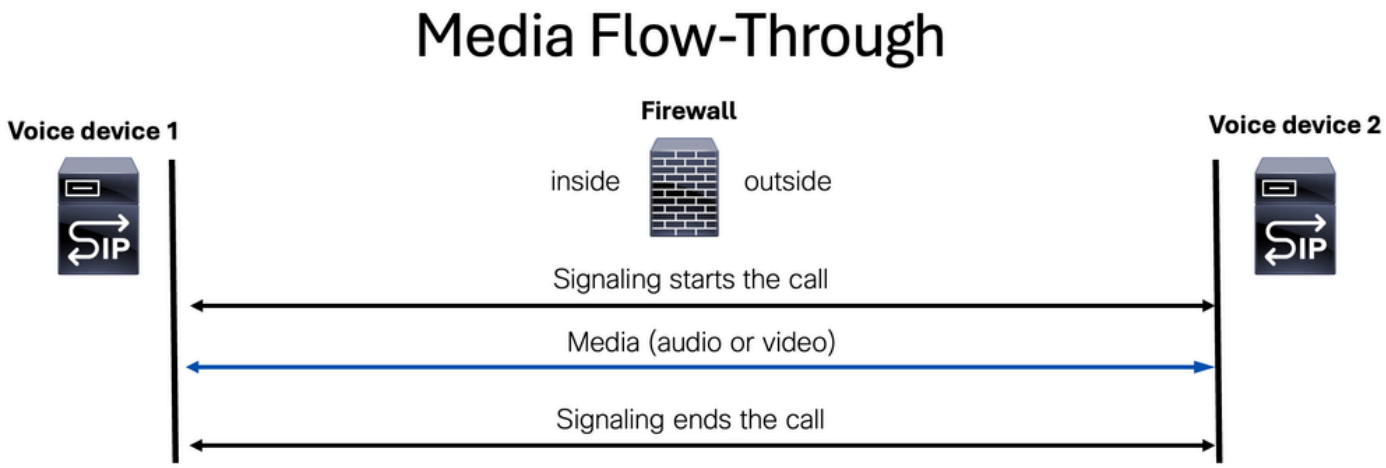
Opmerking: ter illustratie wordt het SIP-serverpictogram gebruikt om een signaleringsserver of een mediaserver in alle afbeeldingen weer te geven.

Bij het bespreken van mediastreaming in een spraakoproep is het belangrijk om twee belangrijke scenario's te benadrukken:

1. doorstroming van media
2. mediadoorstroming

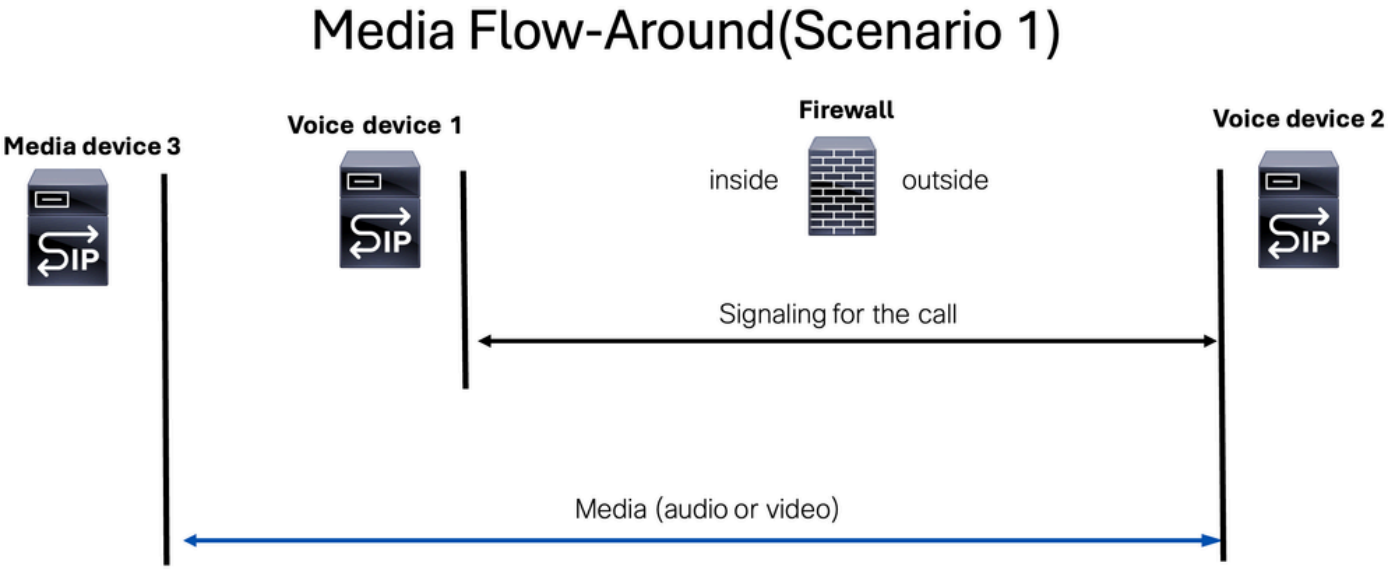
doorstroming van media

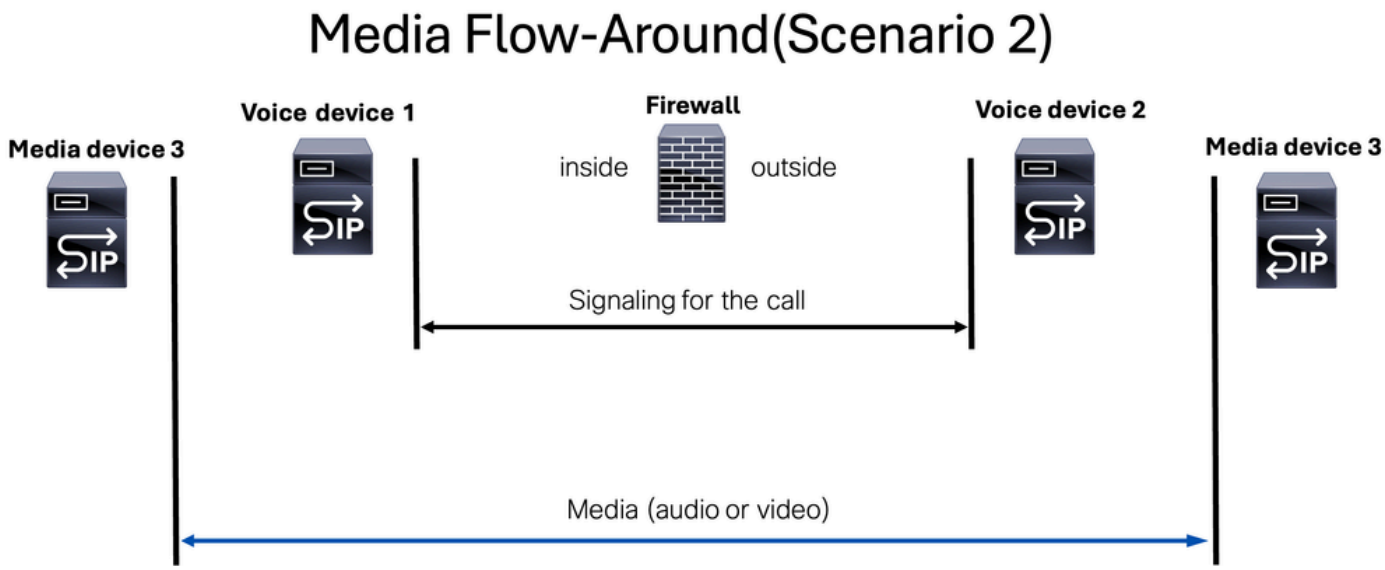
Media flow-through is een modus waarbij zowel media (spraak en/of video) als signaleringspakketten door hetzelfde apparaat worden verwerkt.



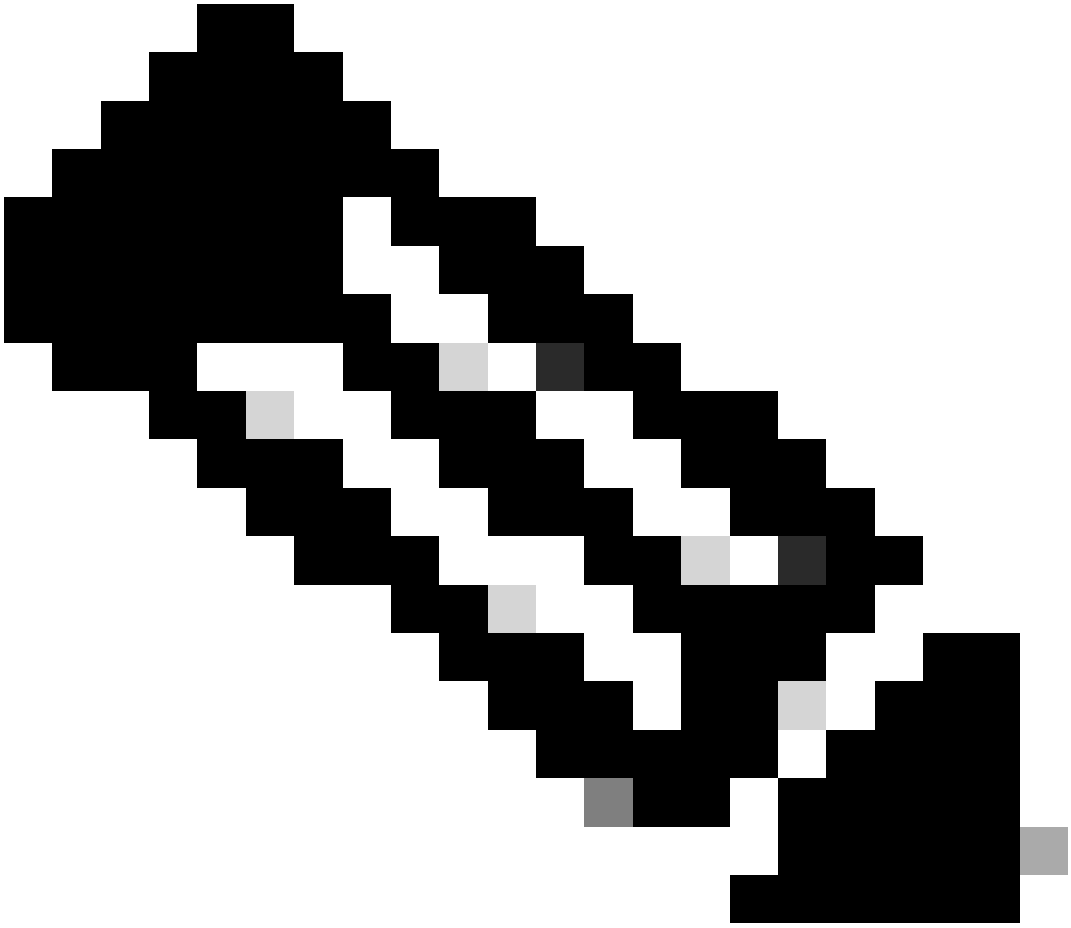
mediadoorstroming

Media stream flow-around is een modus waarbij signaalpakketten worden afgehandeld door twee afzonderlijke signaalcomponenten (apparaten of servers), terwijl de mediastroom (spraak of video) wordt beheerd door een derde apparaat dat bekend staat als het mediaapparaat.





Deze modus verduidelijkt de rollen van de betrokken apparaten en het onderscheid tussen signalering en mediastromen of apparaten.



Opmerking: Dit is vooral belangrijk om te vermelden wanneer het oplossen van problemen met de gemaakte toegangslijst de signaleringscomponenten (apparaten of servers) kan toestaan, maar als de mediastroom een ander mediaapparaat gebruikt, moeten we dit ook toestaan op de toegangslijst van ons FW-apparaat.

Session Initiation Protocol (SIP)

SIP is een application-layer control protocol dat is gedefinieerd door de Internet Engineering Task Force (IETF) in RFC 3261.

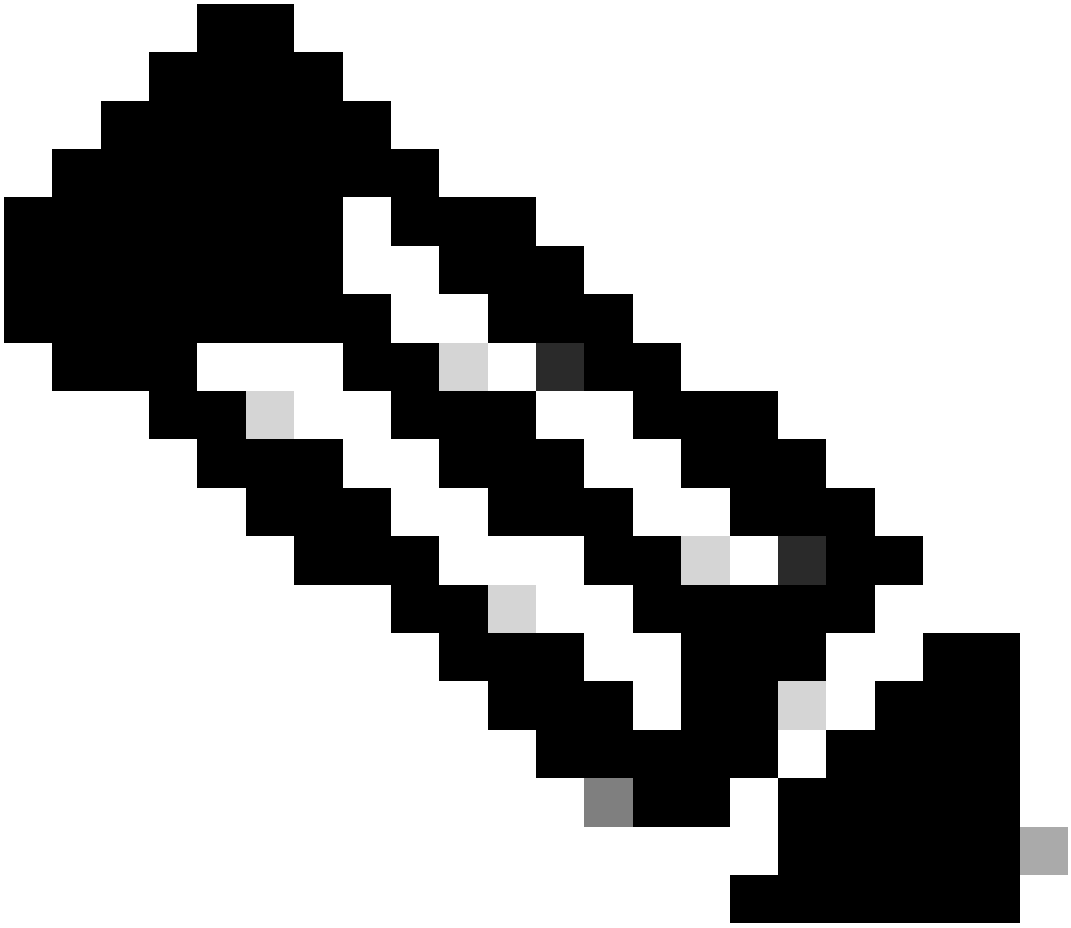
SIP is een op tekst gebaseerd protocol. Dit betekent dat SIP-berichten zijn samengesteld uit door mensen leesbare tekst, vergelijkbaar met hoe HTTP werkt.

SIP is ontworpen om de functies van signalering en sessiebeheer binnen een pakkettelefonienetwerk aan te pakken.

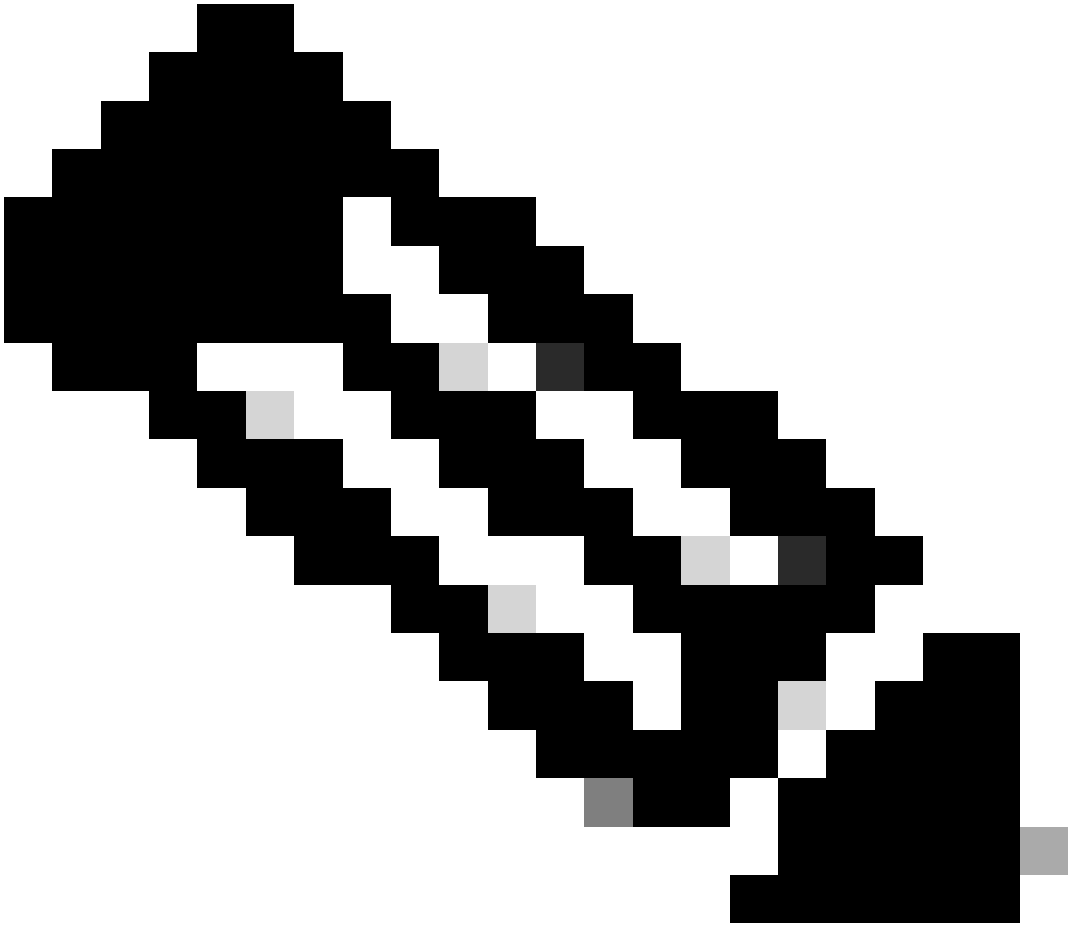
SIP kan:

- Een oproep maken
- Een oproep wijzigen
- een oproep beëindigen

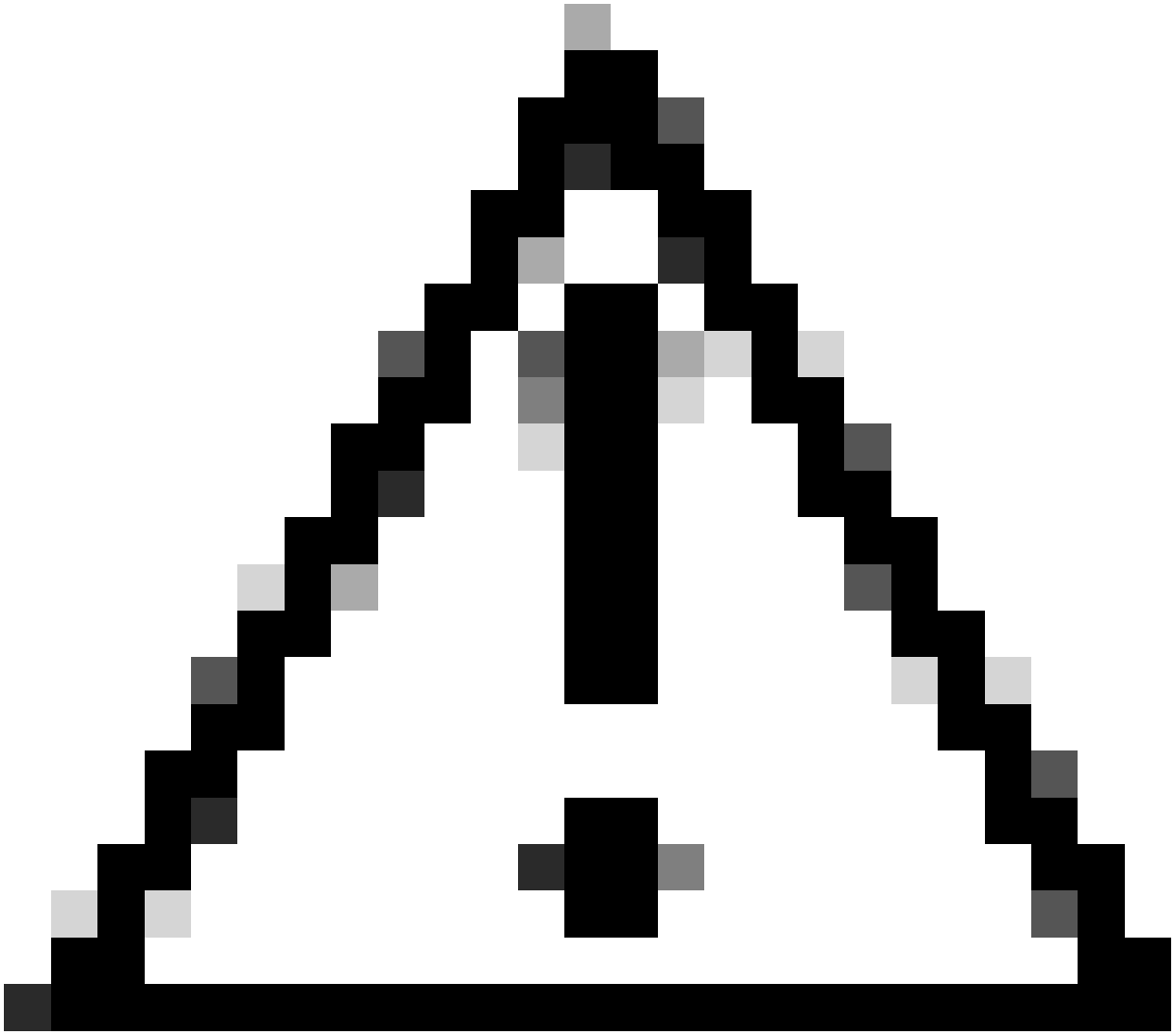
SIP kan zowel UDP als TCP worden gebruikt op gestandaardiseerde poort 5060. En als de SIP is gecodeerd met behulp van Transport Layer Security (TLS), kan deze de gestandaardiseerde poort 5061 gebruiken.



Opmerking: wanneer SIP-signalering wordt gecodeerd, zijn de werkelijke SIP-pakketten niet zichtbaar in pakketopnames op ASA- of FTD-apparaten. U kunt echter nog steeds de TCP-handshake waarnemen, gevolgd door de TLS-handshake tussen de SIP-clients en SIP-serverapparaten.



Opmerking: SIP-inspectie is standaard ingeschakeld voor Cisco Secure Firewall Threat Defense (FTD) en Secure Firewall Adaptive Security Appliance (ASA).



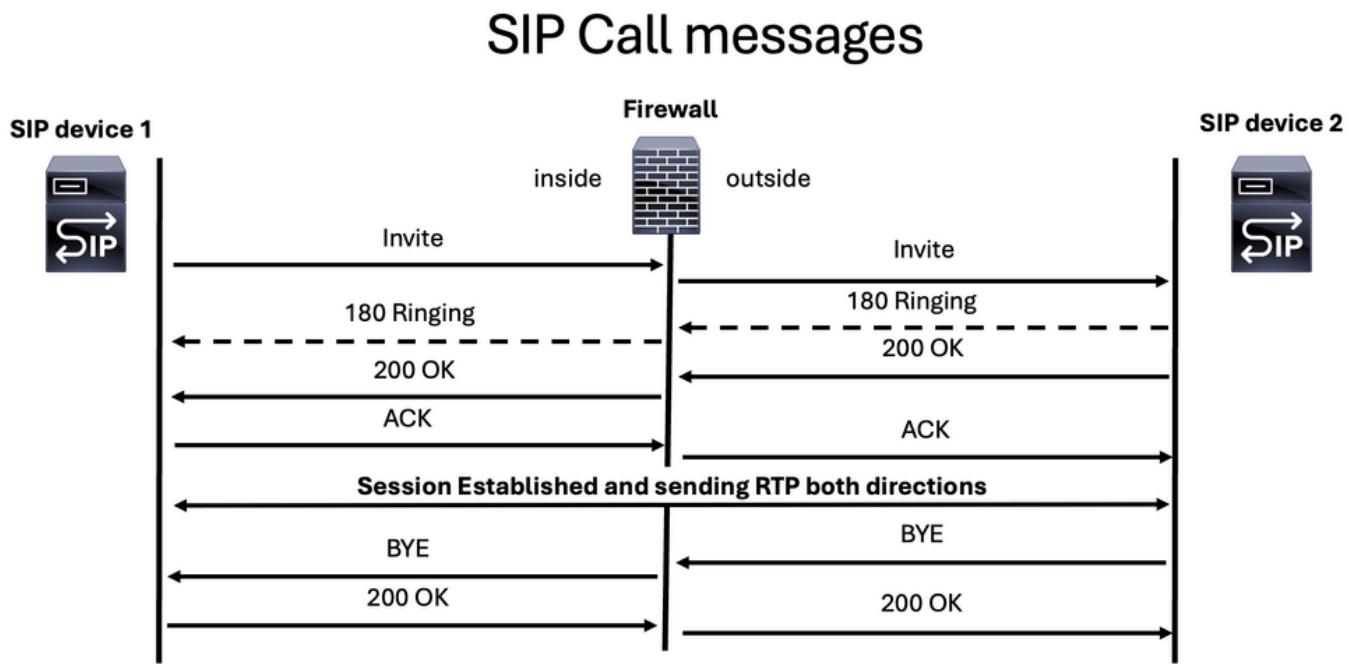
Let op: bevestig altijd welke poorten worden gebruikt voor signalering. Vergeet niet dat het SIP-protocol vaak poorten 5060 of 5061 gebruikt, maar sommige implementaties kunnen afwijken van deze standaarden en verschillende poorten gebruiken voor het SIP-protocol.

Er zijn drie scenario's die kunnen worden gevonden bij het oplossen van een SIP-signaleringsprobleem:

- SIP-oproepsignaleringsberichten
- SIP OPTION-berichten
- SIP REGISTER-berichten

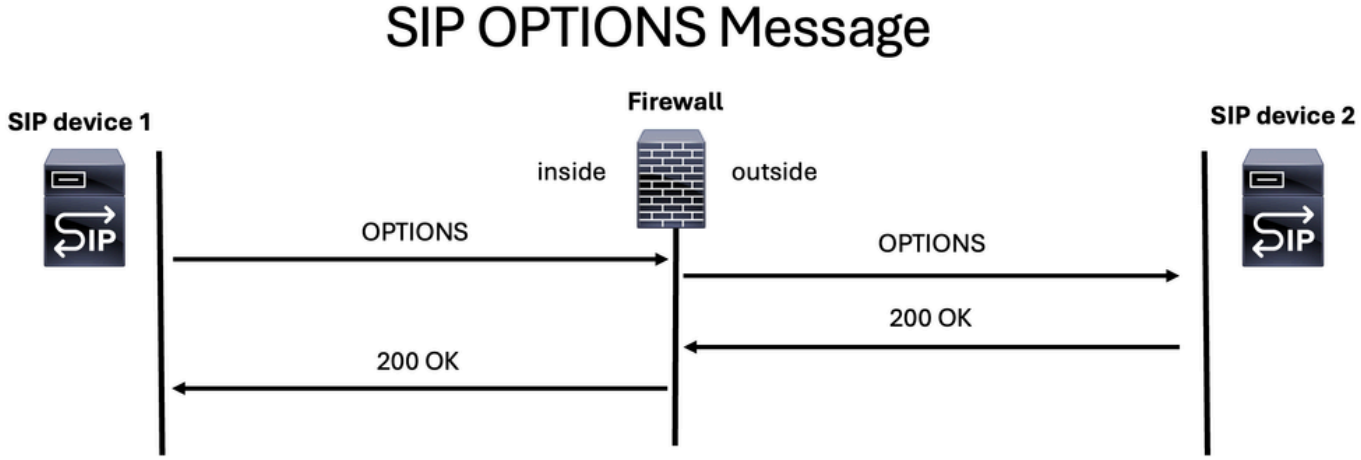
Berichten voor SIP-oproep

De belangrijkste SIP-berichten voor het instellen en beëindigen van een spraakoproep zijn:



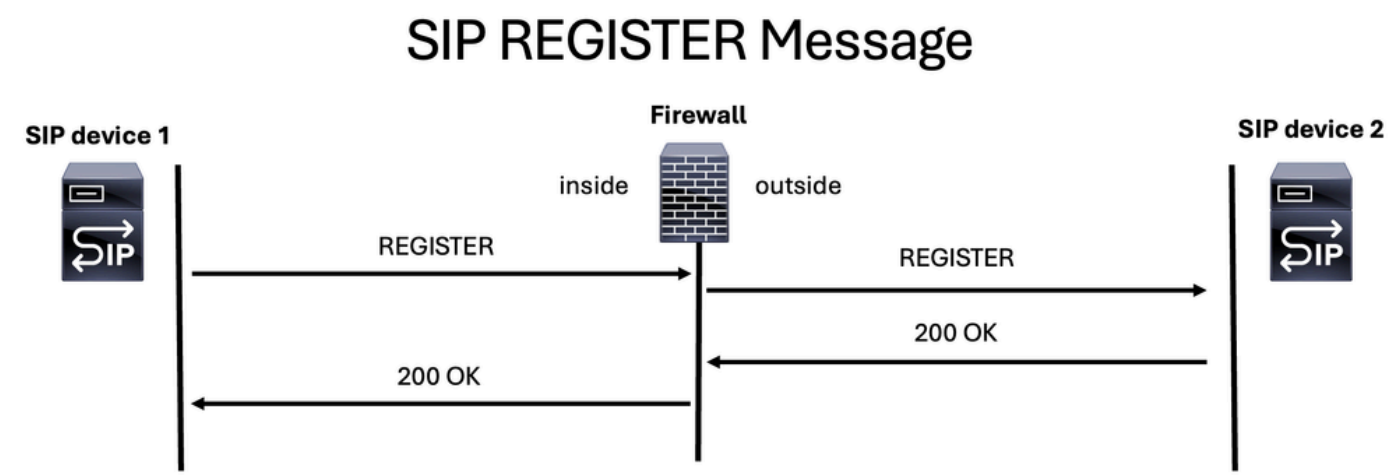
SIP OPTION-berichten

SIP OPTIONS-berichten zijn belangrijk om te bepalen of een SIP-apparaat online is en kan reageren. Het is als ping ICMP bericht, maar op SIP wereld.

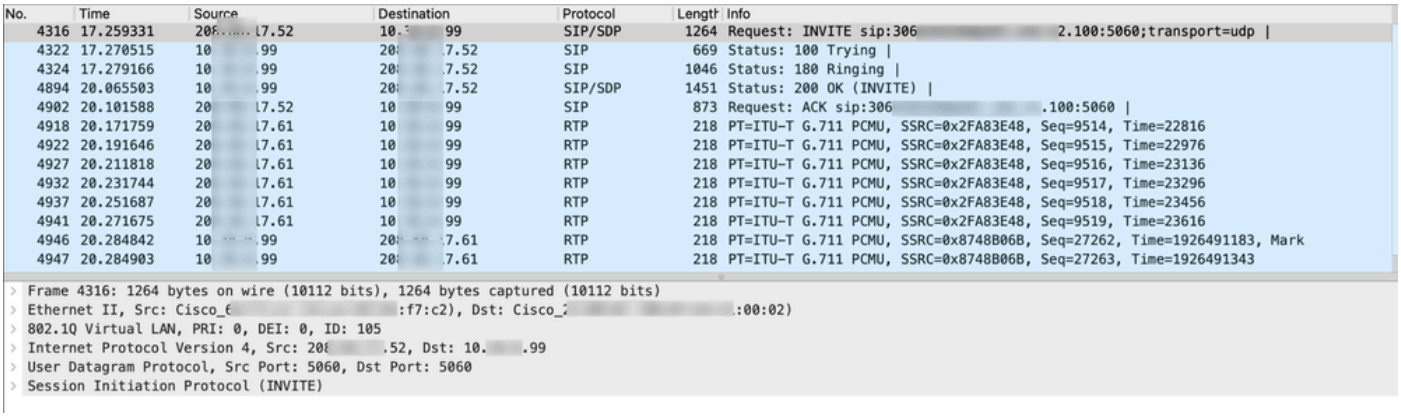


Bericht SIP-REGISTER

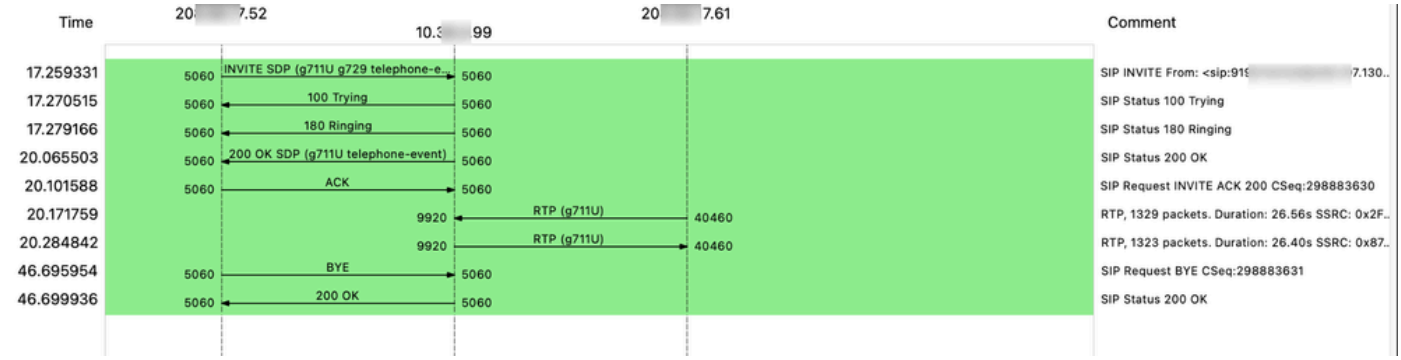
Een ander SIP-bericht dat u kunt vinden tijdens een probleemoplossingssessie voor firewalls, is het SIP REGISTER-bericht, waarmee een apparaat zich kan registreren bij een SIP-server.



Deze pakketopname toont verzoeken en antwoorden van twee SIP-apparaten en ook het media-(spraak)verkeer:

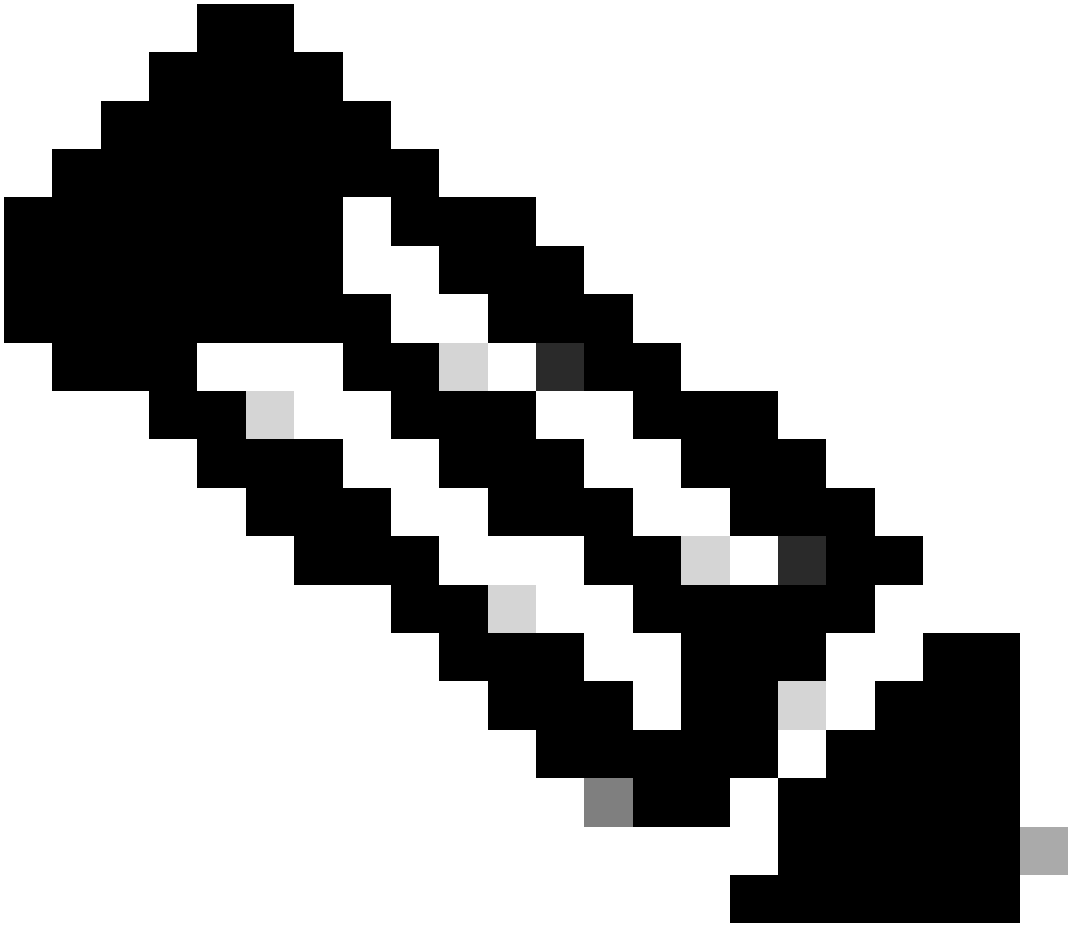


Dit is een voorbeeld van een stroom van zowel SIP-signalering als RTP-media (spraak):



Session Description Protocol (SDP)

Session Description Protocol (SDP) is een standaardweergave die wordt gebruikt om mediastromen voor multimediasessies te beschrijven. Het heeft geen media zelf, maar wordt gebruikt om te onderhandelen over het mediatype en het formaat tussen eindpunten. SDP wordt gebruikt in combinatie met het Session Initiation Protocol (SIP) om mediakarakteristieken voor een sessie te beheren en te onderhandelen.

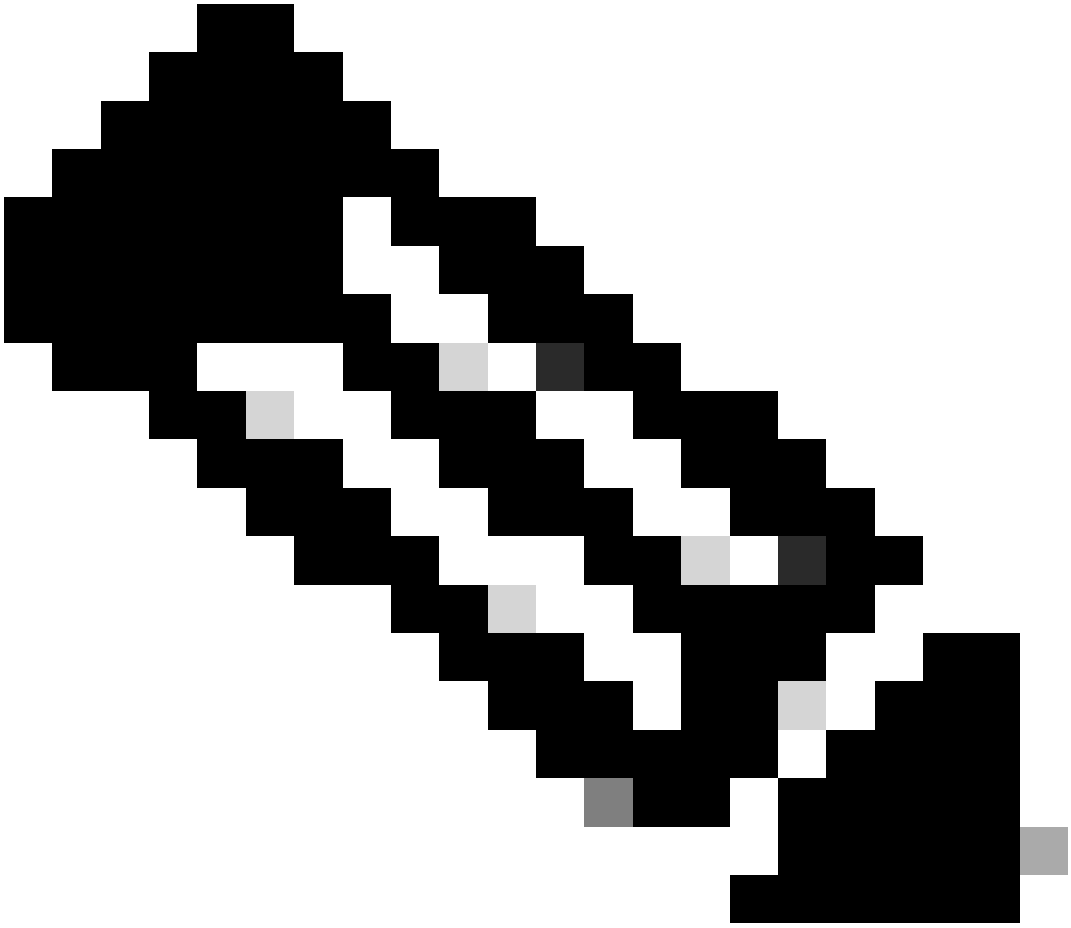


Opmerking: MGCP omvat het concept SDP, dat voor hetzelfde doel wordt gebruikt.

Dit is een voorbeeld van een SDP-bericht in een SIP-protocol:

```
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
```



Opmerking: Sommige SDP-berichten bevatten deze parameters in het voorbeeld:

++c-IN IP4: IP-adres van de mediaserver

++m=audio: Dit geeft aan dat het mediatype audio is.

++8266: Dit is het poortnummer waarop de audiostream wordt verzonden.

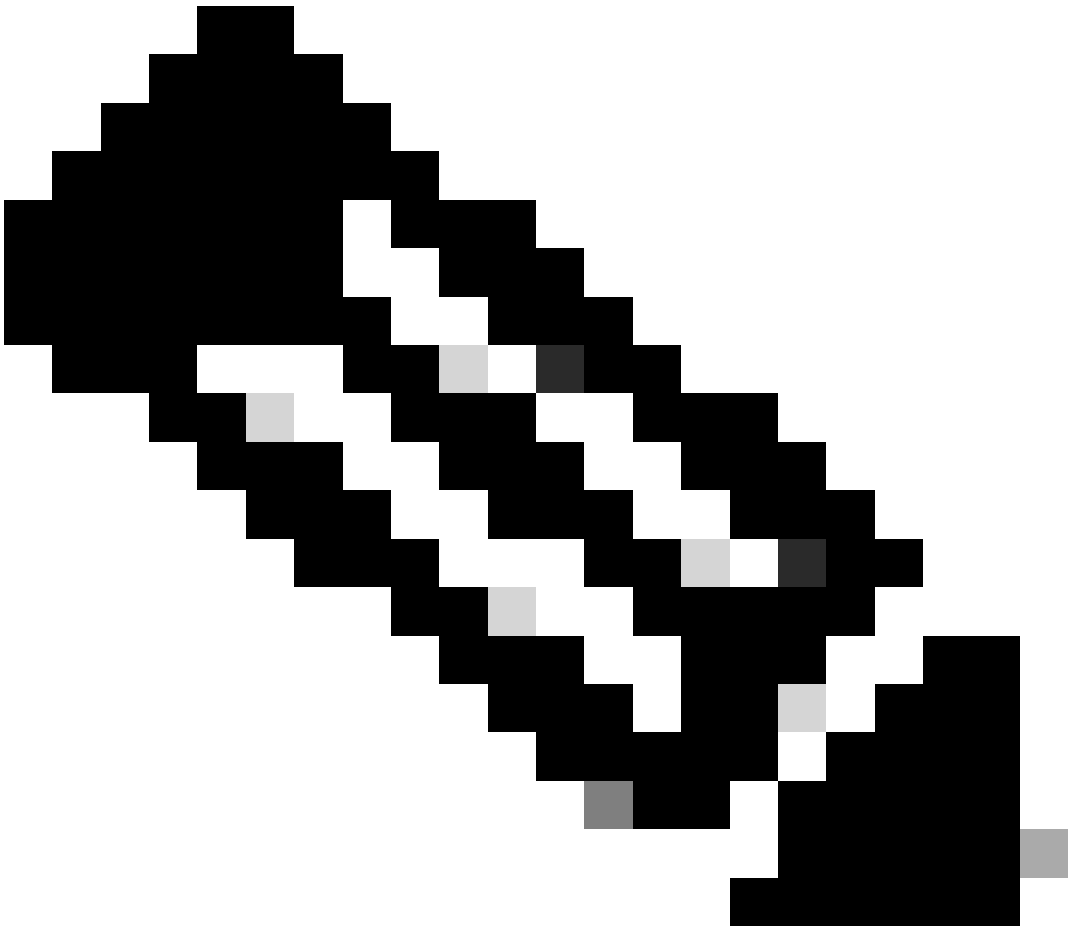
++RTP/AVP: Hiermee wordt het transportprotocol opgegeven, dat RTP is met behulp van het Audio/Video Profile (AVP).

++18 127: Dit zijn de payload types voor de audio codecs. Payload type 18 komt meestal overeen met de G.729 codec, en 127 is een dynamisch payload type dat kan worden toegewezen aan een codec als per de onderhandeling tussen de eindpunten.

Session Description Protocol (SDP) is te vinden in verschillende SIP-berichten zoals: INVITE, 183 Session in Progress, 200 OK, ACK, enzovoort. SDP dient als een antwoordmethode voor het uitwisselen van spraak- en/of videomogelijkheden tussen partijen. Bij het oplossen van problemen

met oproepen is het essentieel om drie hoofdconcepten te begrijpen:

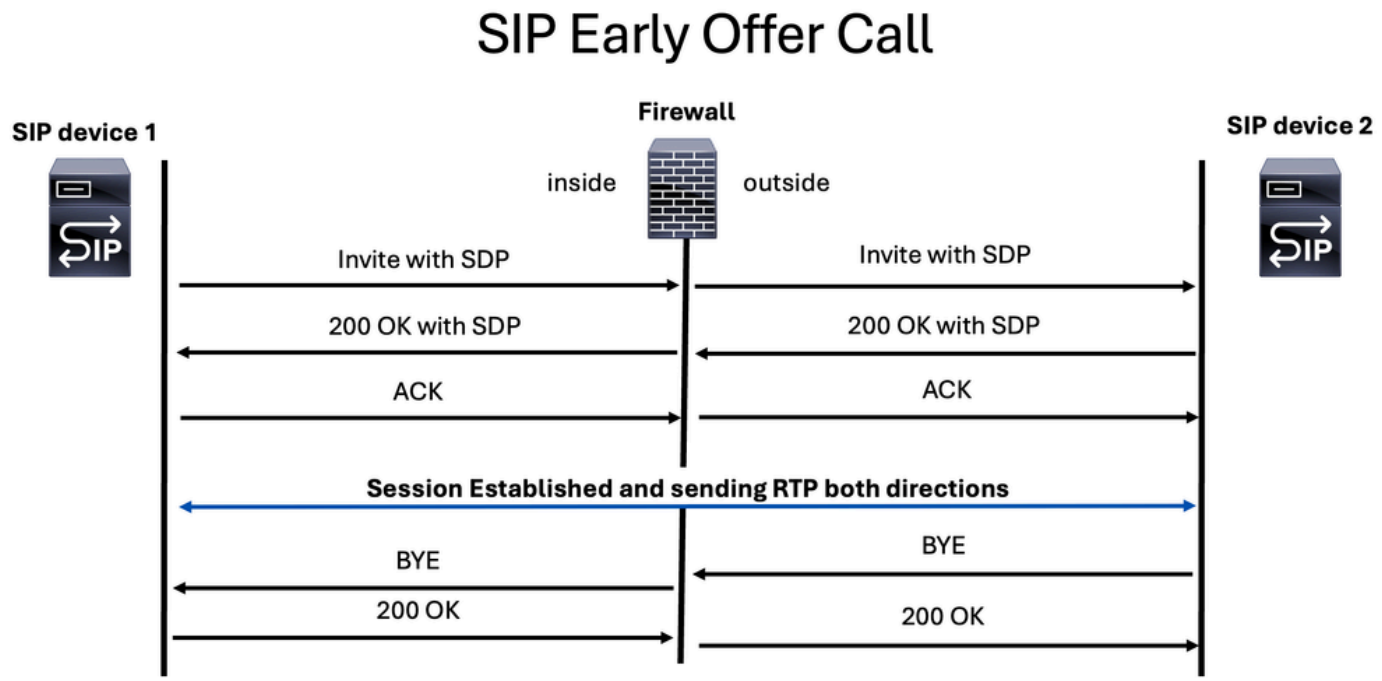
1. Vroege aanbieding
2. Aanbieding uitstellen
3. Vroege media



> Opmerking: Het is van cruciaal belang om de bestemming van SDP-berichten te begrijpen, omdat de inspectiefunctie op de firewall IP-adressen niet alleen in SIP-headers, maar ook in de SDP-sectie kan wijzigen.

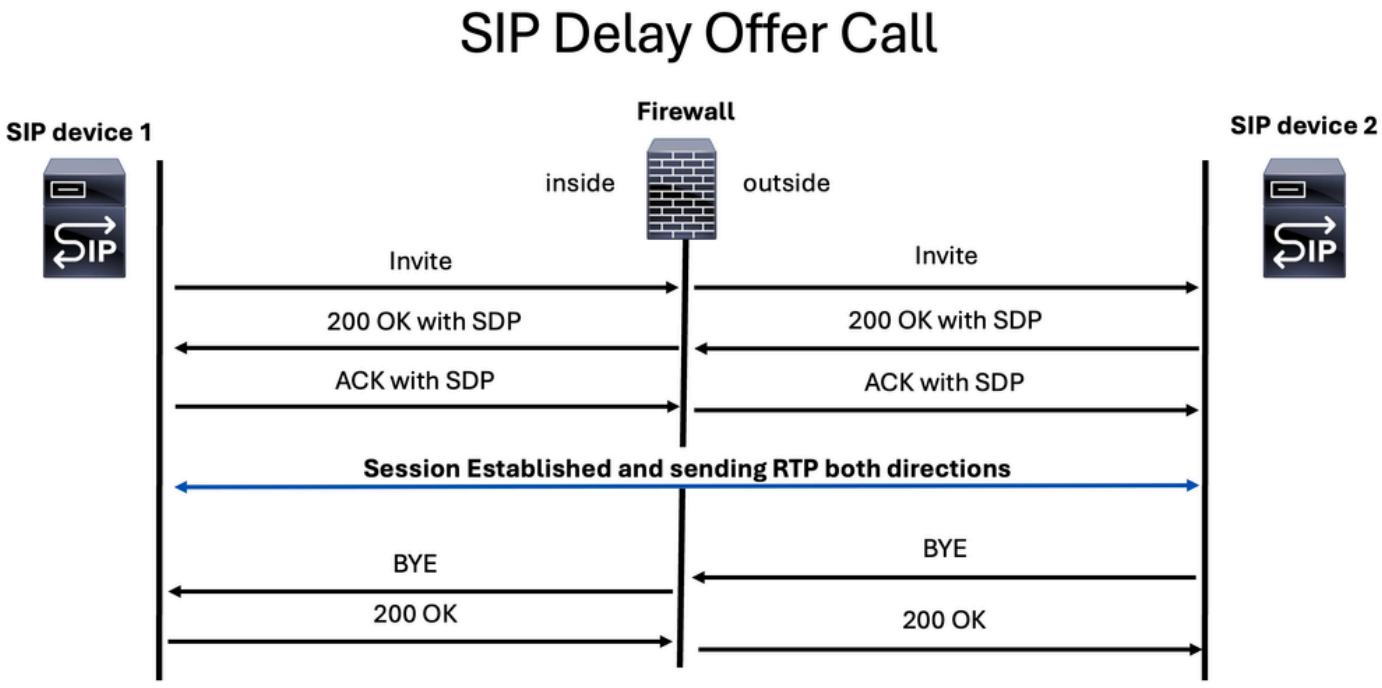
Vroege aanbieding

Hier zijn mediaparameters op SDP te vinden in de INVITE en 200 OK SIP-berichten.



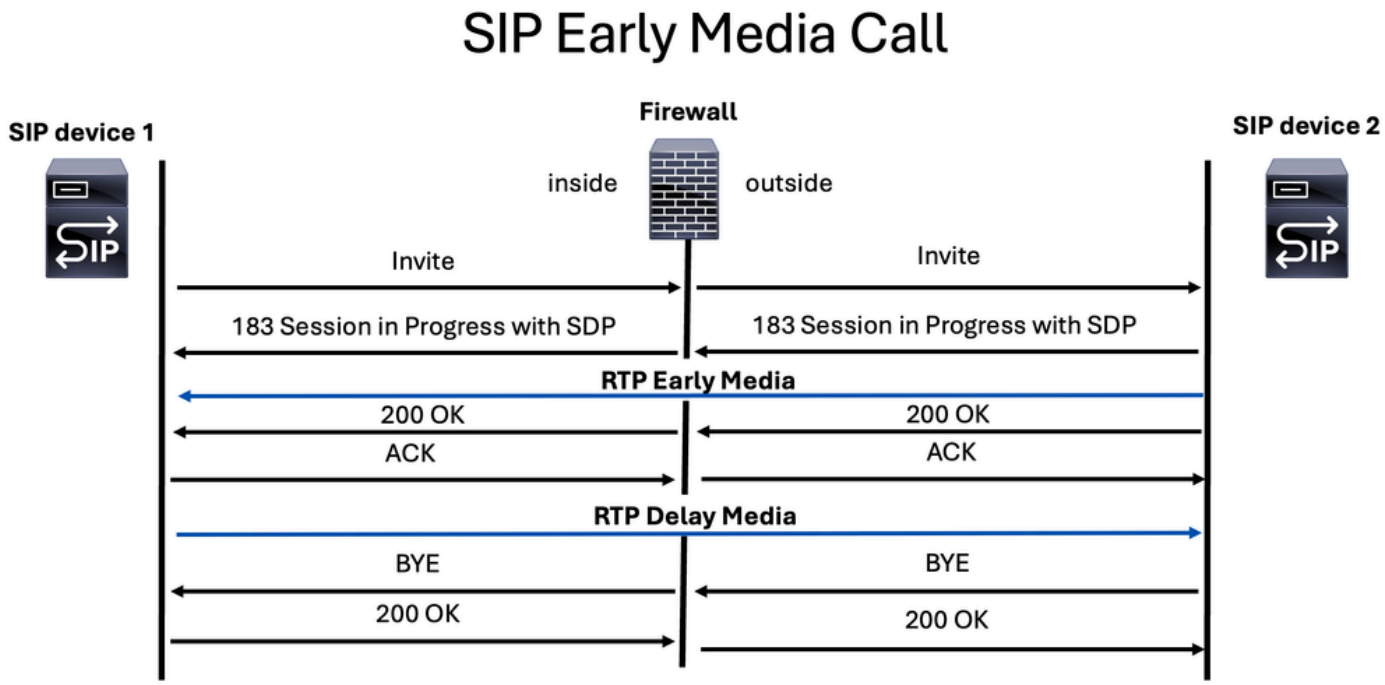
Aanbieding uitstellen

Bij deze methode wordt de SDP gevonden op 200 OK- en ACK SIP-berichten.



Vroege media

Vroege media worden verzonden via een specifiek SIP-bericht dat bekend staat als de 183 Session Progress-respons. Dit bericht bevat het Sessiebeschrijvingsprotocol (SDP) met mediaparameters voor de aangeroepen partij. Het wordt vaak gebruikt door providers en SIP-providers om geautomatiseerde spraakberichten of andere media naar de beller te sturen voordat het gesprek officieel is verbonden.

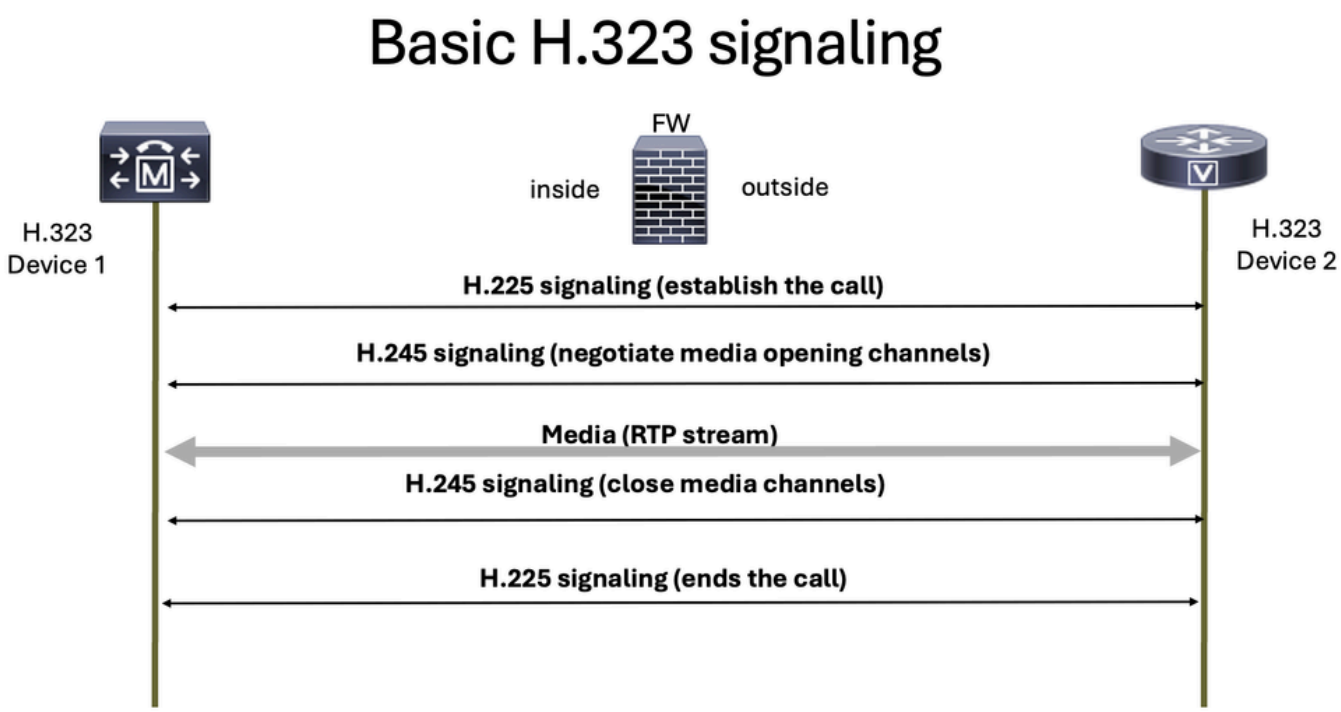


H.323

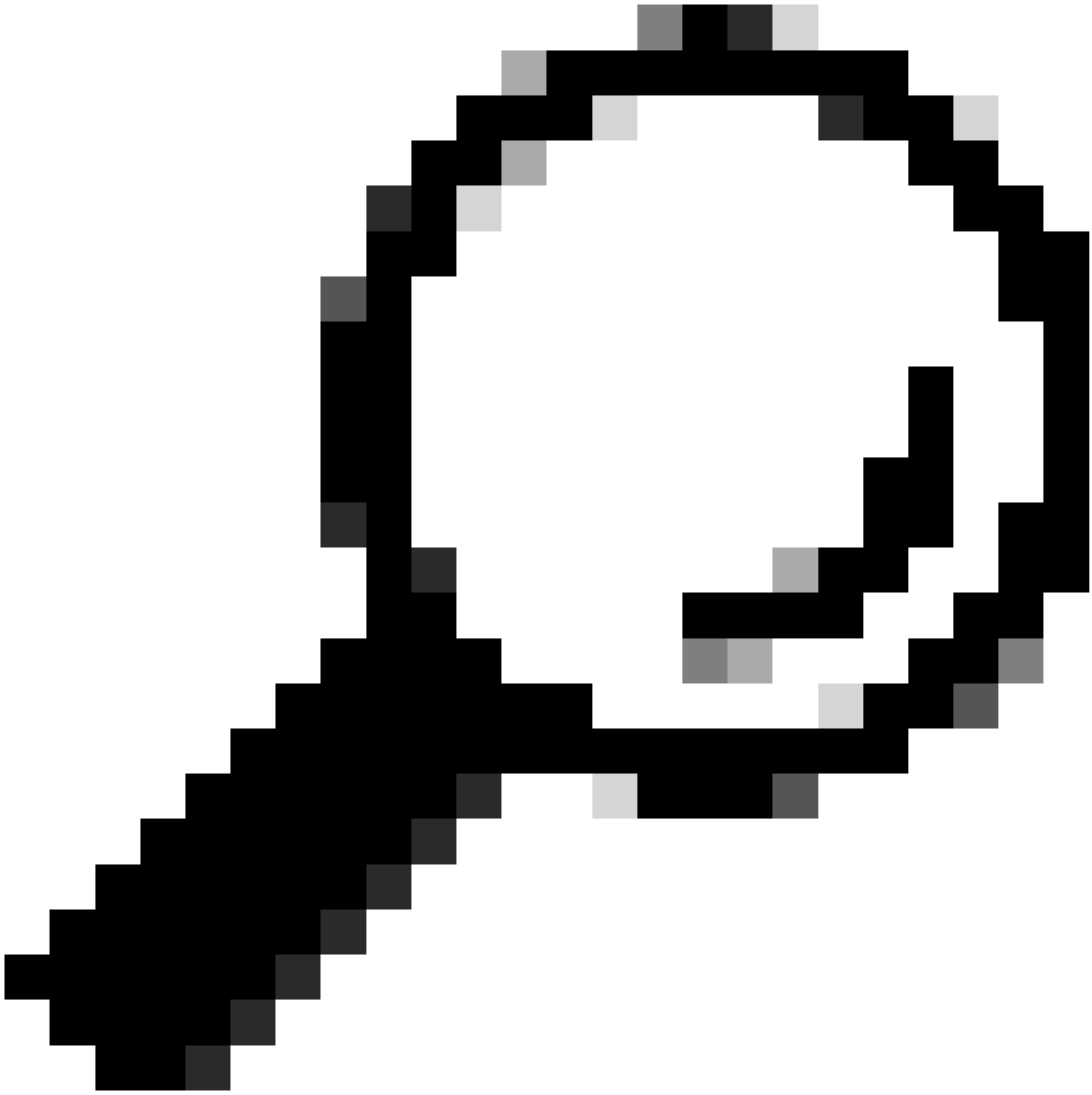
H.323 is een reeks protocollen die door de Internationale Telecommunicatie Unie (ITU) zijn gedefinieerd voor spraak-, video- en datacommunicatie via pakketgeschakelde netwerken, zoals het internet.

Het H.323-protocol bestaat uit twee hoofdcomponenten:

1. H.225: Deze regelt de oproepsignalering, inclusief de installatie en beëindiging van oproepen.
2. H.245: Dit is verantwoordelijk voor de uitwisseling van mogelijkheden en het openen en sluiten van kanalen voor audio en video.



De poorten die worden gebruikt door het H.323-signaleringsprotocol zijn 1718, 1719 en 1720.

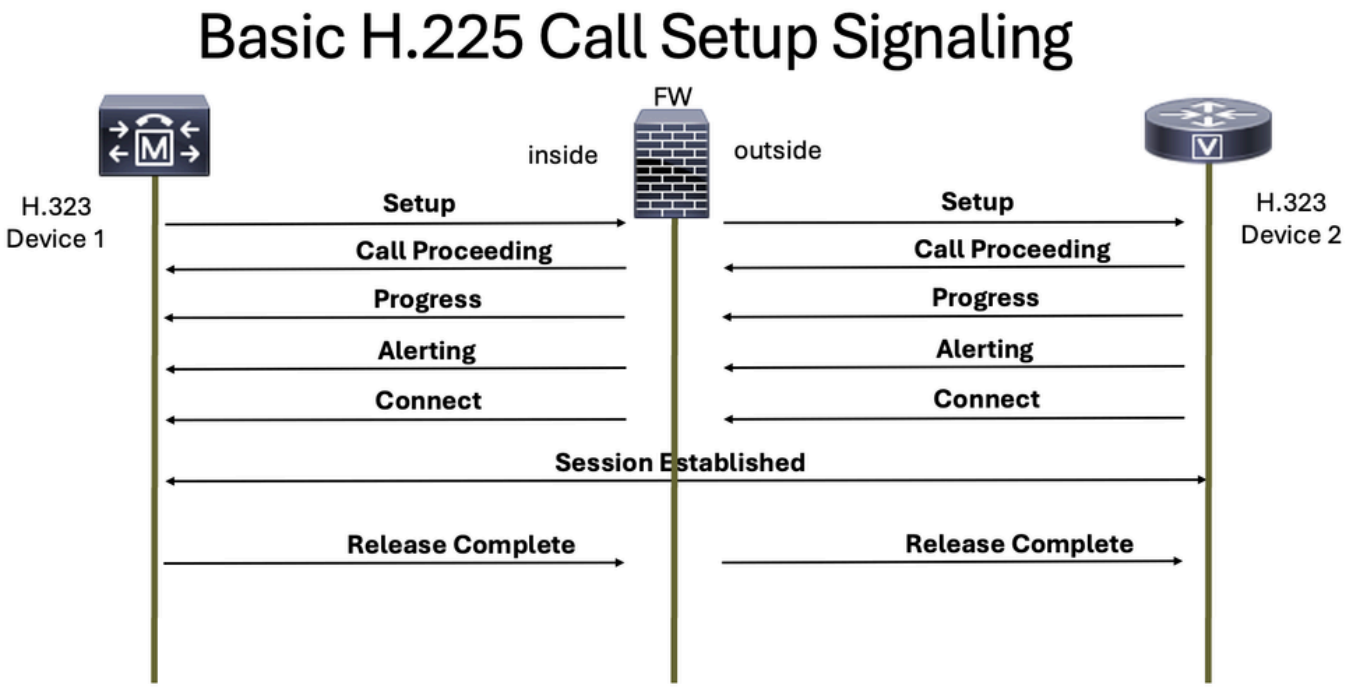


Tip: beveiligde H.323-protocolcommunicatie kan problemen ondervinden bij het overschakelen van UDP naar TCP vanwege het gebruik van TLS voor codering, waardoor een firewall de verbinding per ongeluk kan blokkeren als verdachte activiteit, dus het is cruciaal om de firewall te configureren om zowel UDP- als TCP-verkeer voor H.323-eindpunten of servers mogelijk te maken.

H.323 is een protocol dat twee werkingsmodi heeft: slow start en fast start.

H.225

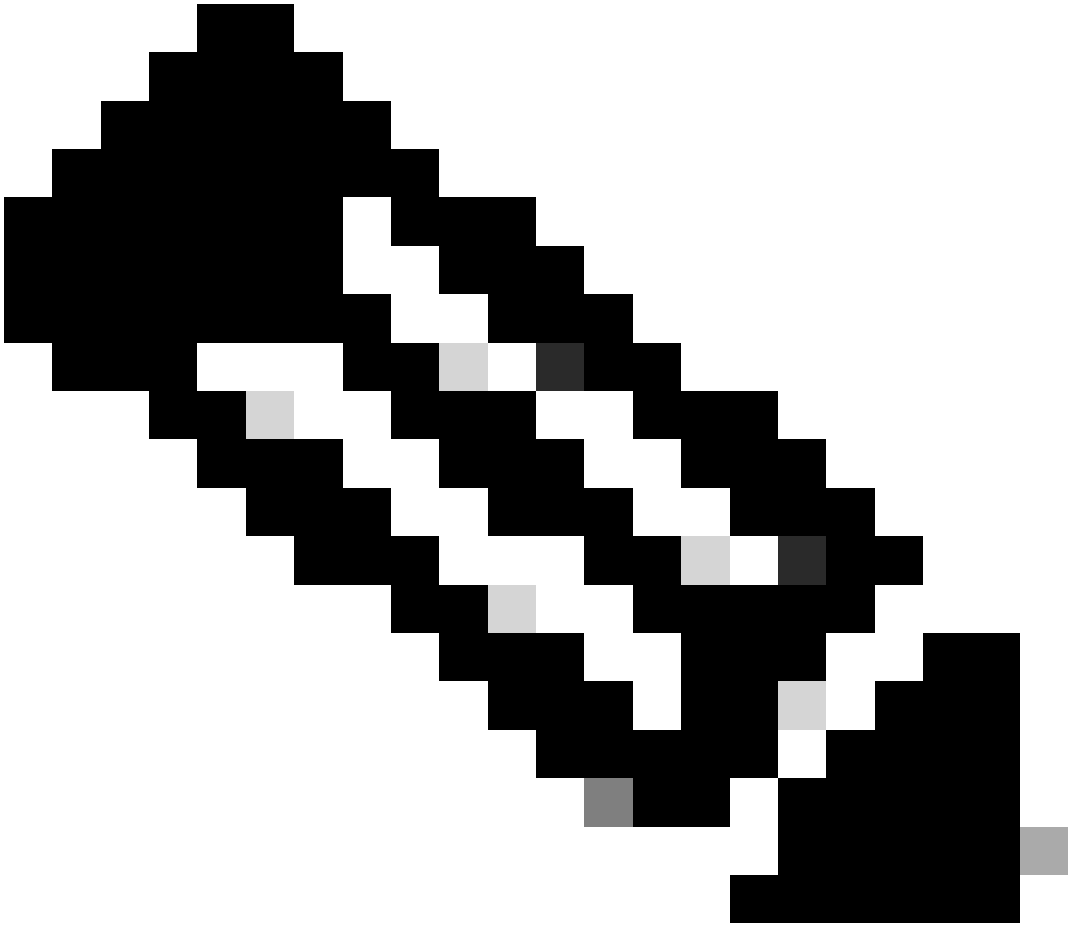
Dit protocol is verantwoordelijk voor het instellen van de oproep en het beëindigen van een spraakoproep wanneer een van de partijen ophangt.



H,245

H.245 biedt de volgende functionaliteiten:

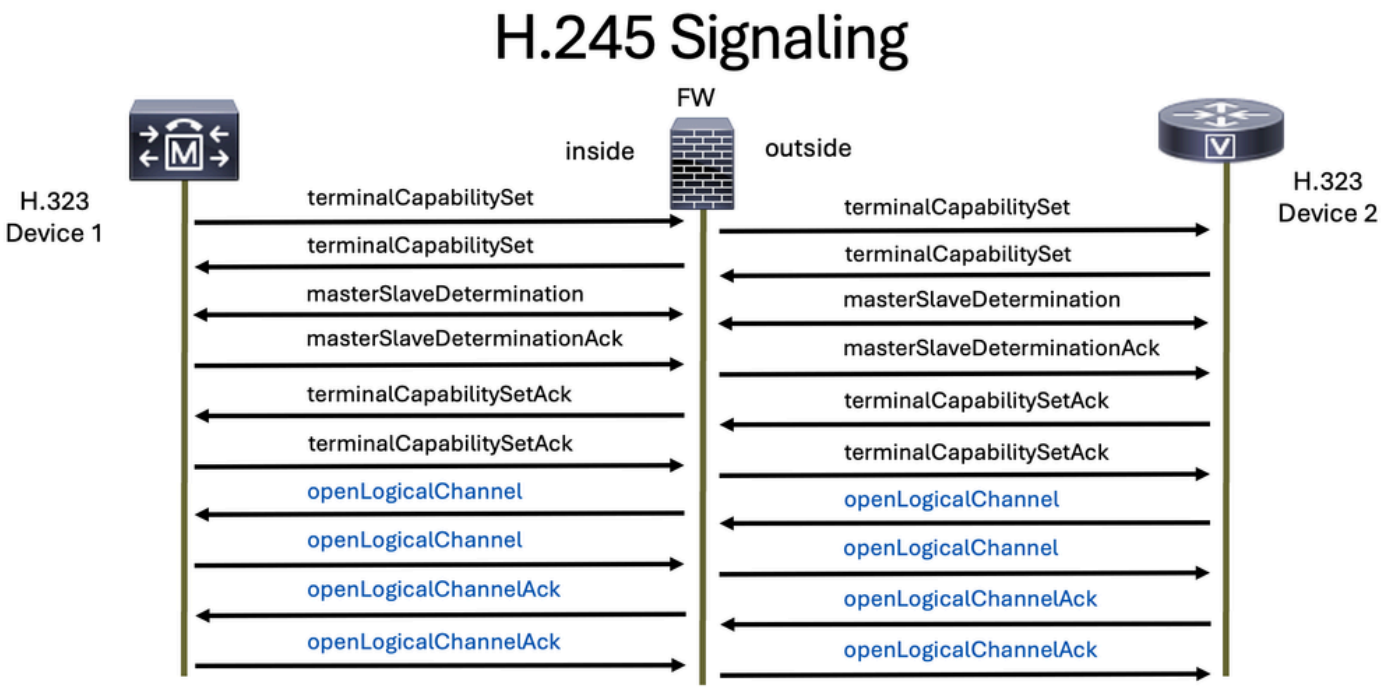
- uitwisseling van terminalcapaciteit
- Bepalingen voor meester/slaaf
- logisch-kanaalsignalering



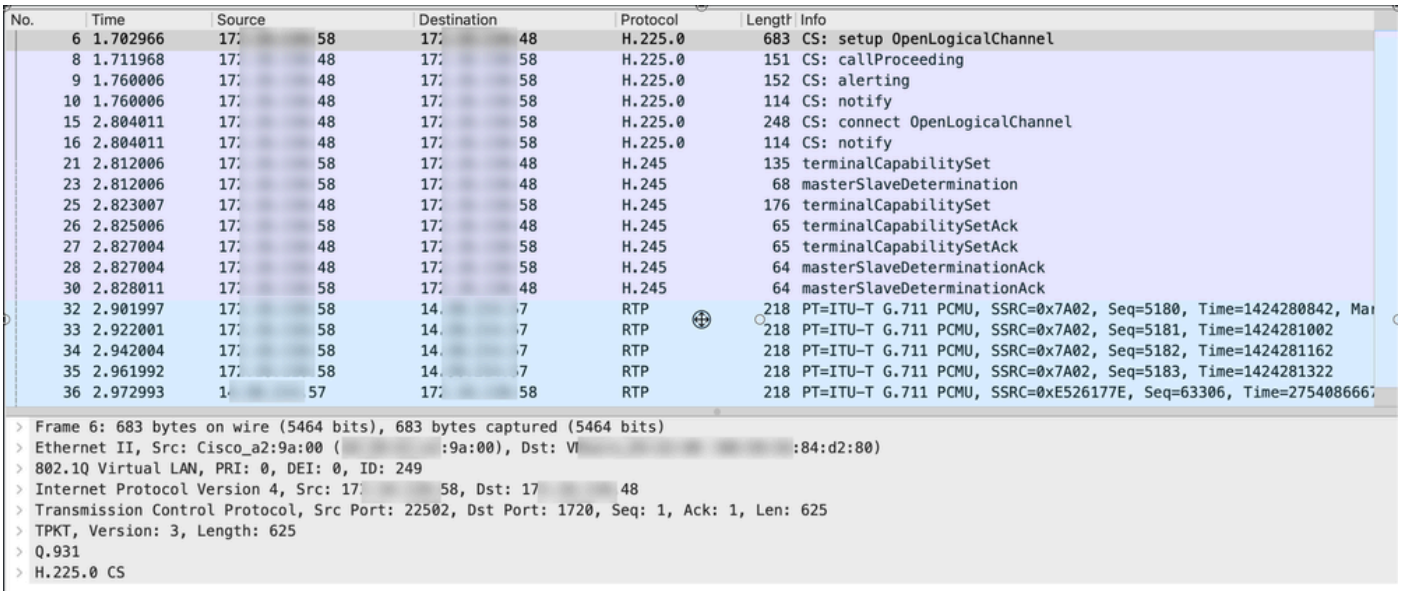
Opmerking: De termen Master en Slave die in dit document worden gebruikt, zijn hardcoded in het oorspronkelijke H.323-protocol en weerspiegelen niet het beleid of de waarden van ons bedrijf. We zetten ons in voor het bevorderen van inclusieve en respectvolle taal.

Het H.245-protocol wordt verzonden na ontvangst van het H.225-verbindingsbericht.

Dit protocol helpt bij het bepalen welk stemprotocol wordt gebruikt voor RTP, en het is gespecificeerd op het openen van het logische kanaal en het sluiten van logische kanaalberichten ervoor.



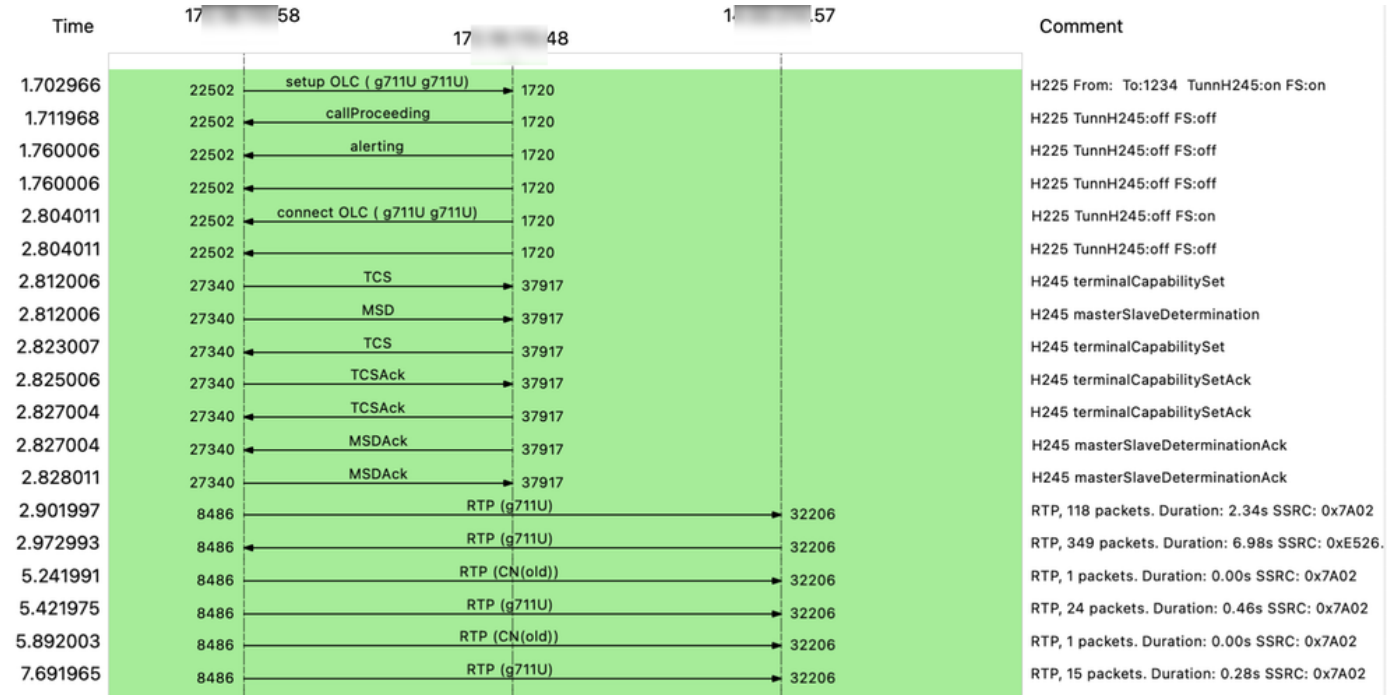
Deze pakketopname toont verzoeken en antwoorden van twee H.323-apparaten met H.225 en H.245 en ook het media(spraak)verkeer:

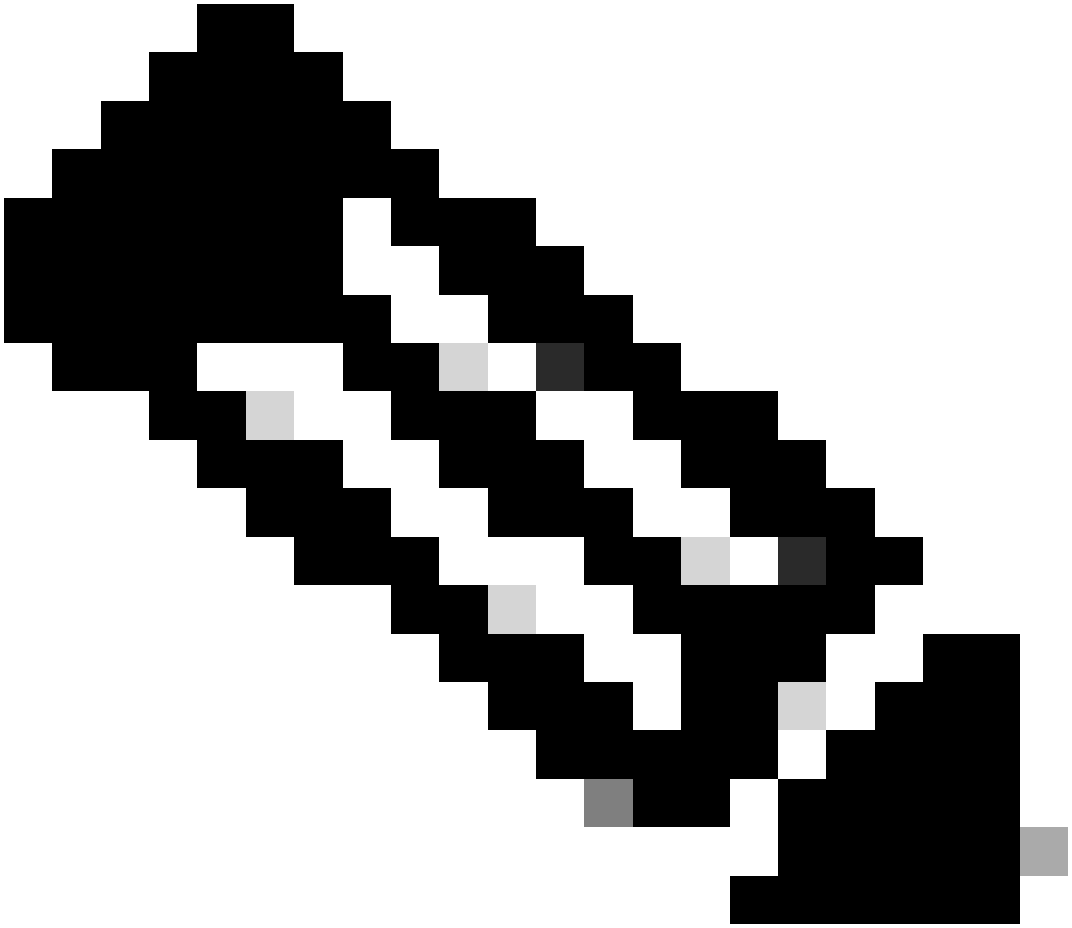


No.	Time	Source	Destination	Protocol	Length	Info
6	1.702966	17 58	17 48	H.225.0	683	CS: setup OpenLogicalChannel
8	1.711968	17 48	17 58	H.225.0	151	CS: callProceeding
9	1.760006	17 48	17 58	H.225.0	152	CS: alerting
10	1.760006	17 48	17 58	H.225.0	114	CS: notify
15	2.804011	17 48	17 58	H.225.0	248	CS: connect OpenLogicalChannel
16	2.804011	17 48	17 58	H.225.0	114	CS: notify
21	2.812006	17 58	17 48	H.245	135	terminalCapabilitySet
23	2.812006	17 58	17 48	H.245	68	masterSlaveDetermination
25	2.823007	17 48	17 58	H.245	176	terminalCapabilitySet
26	2.825006	17 58	17 48	H.245	65	terminalCapabilitySetAck
27	2.827004	17 48	17 58	H.245	65	terminalCapabilitySetAck
28	2.827004	17 48	17 58	H.245	64	masterSlaveDeterminationAck
30	2.828011	17 58	17 48	H.245	64	masterSlaveDeterminationAck
32	2.901997	17 58	14 7	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7A02, Seq=5180, Time=1424280842, Ma
33	2.922001	17 58	14 7	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7A02, Seq=5181, Time=1424281002
34	2.942004	17 58	14 7	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7A02, Seq=5182, Time=1424281162
35	2.961992	17 58	14 7	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7A02, Seq=5183, Time=1424281322
36	2.972993	1 57	17 58	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0xE526177E, Seq=63306, Time=2754086667

```
> Frame 6: 683 bytes on wire (5464 bits), 683 bytes captured (5464 bits)
> Ethernet II, Src: Cisco_a2:9a:00 ( :9a:00), Dst: V :84:d2:80)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 249
> Internet Protocol Version 4, Src: 17 58, Dst: 17 48
> Transmission Control Protocol, Src Port: 22502, Dst Port: 1720, Seq: 1, Ack: 1, Len: 625
> TPKT, Version: 3, Length: 625
> Q.931
> H.225.0 CS
```

Dit is een voorbeeld van een stroom van zowel H.323-signalering met H.225 en H.245 als RTP-media (spraak):

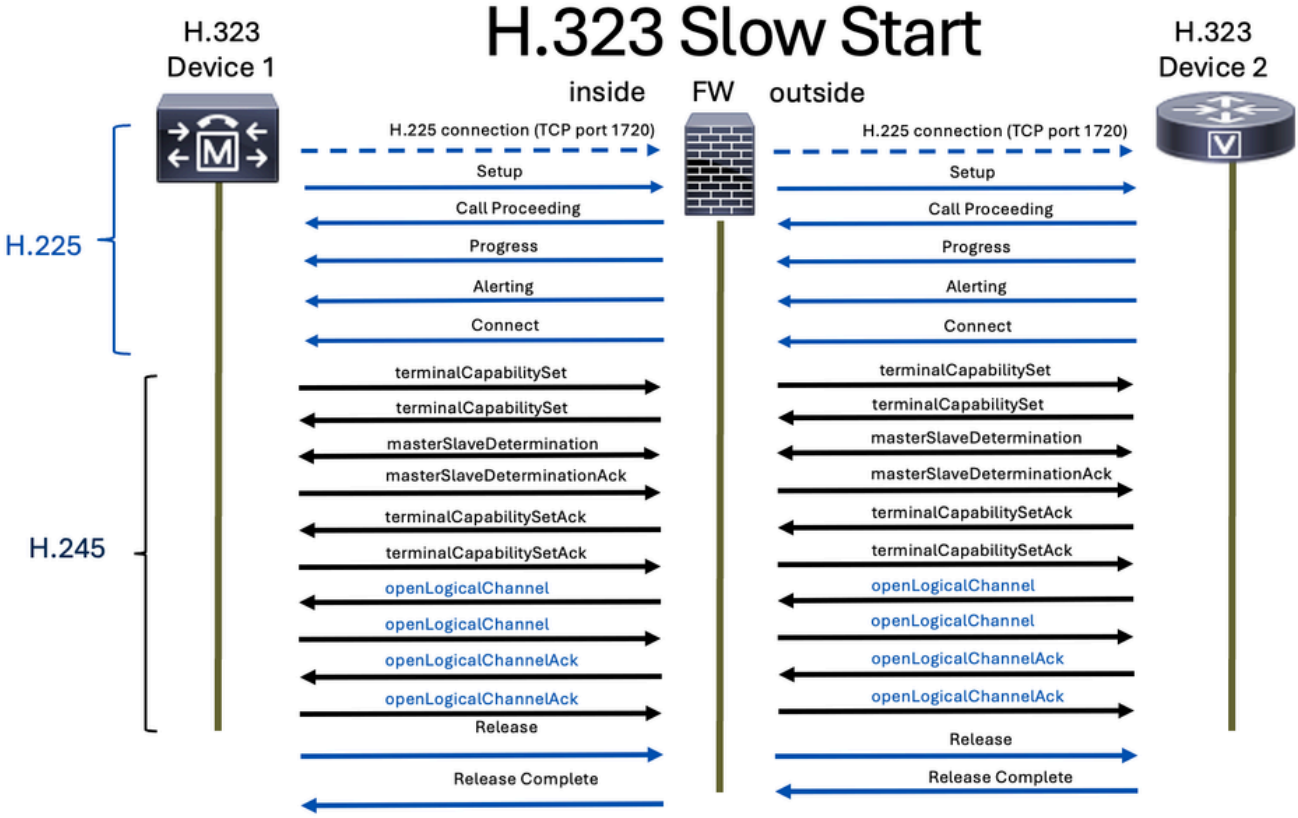

Time
Comment
1.702966 22502 setup OLC (g711U g711U) 1720 H225 From: To:1234 TunnH245:on FS:on
1.711968 22502 callProceeding 1720 H225 TunnH245:off FS:off
1.760006 22502 alerting 1720 H225 TunnH245:off FS:off
1.760006 22502 1720 H225 TunnH245:off FS:off
2.804011 22502 connect OLC (g711U g711U) 1720 H225 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



Opmerking: H.323-inspectie is standaard ingeschakeld voor Cisco Secure Firewall Threat Defense (FTD) en Secure Firewall Adaptive Security Appliance (ASA).

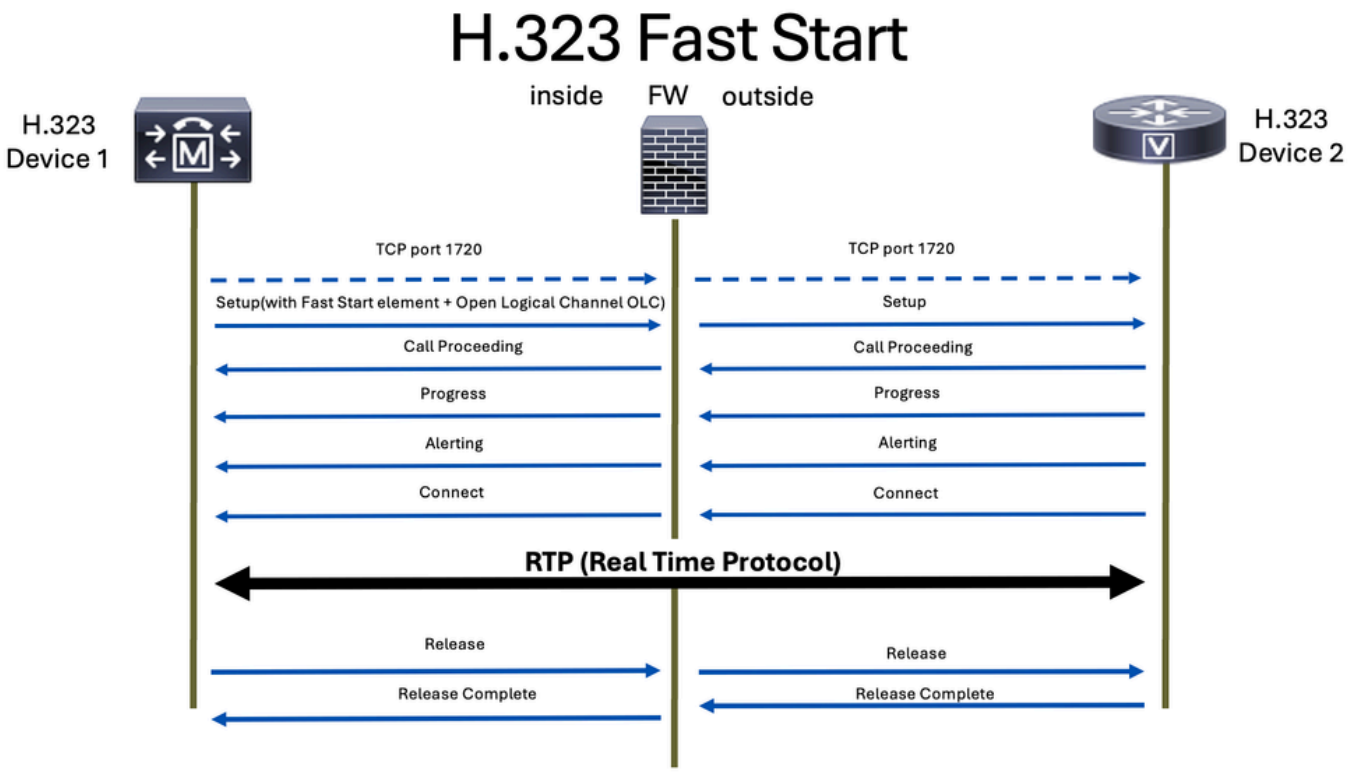
Trage start

In de slow start-modus omvat het instellingsproces van de oproep verschillende signaalstappen voordat mediakanalen worden ingesteld. De stappen omvatten Instellen, Doorgaan van oproepen, Waarschuwing en Verbinding maken. Na deze stappen wordt de H.245-mediumonderhandeling afzonderlijk uitgevoerd. Dit betekent dat de mediakanalen pas worden ingesteld nadat de eerste oproepsignalering is voltooid, wat kan resulteren in een langere installatietijd.



Snelle start

In tegenstelling hiermee zorgt de snelle startmodus ervoor dat de mediumonderhandeling kan plaatsvinden binnen het eerste Setup-bericht. Dit betekent dat de mediakanalen sneller kunnen worden ingesteld, omdat de onderhandeling wordt uitgevoerd als onderdeel van de eerste oproepinstallatie. Snelle start stroomlijnt het proces door het aantal uitgewisselde berichten en de hoeveelheid verwerking die nodig is voordat de mediakanalen worden ingesteld, te verminderen.

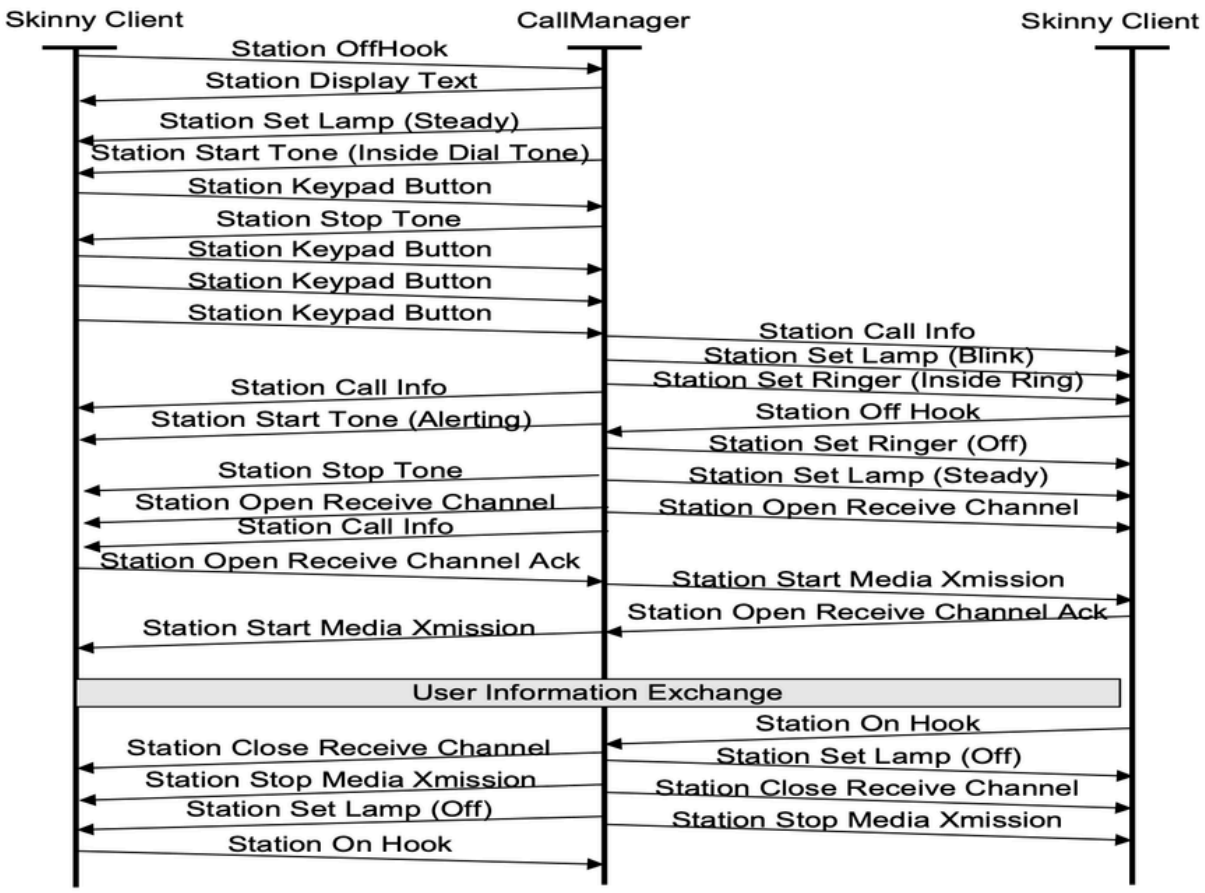


SCCP

Skinny Client Control Protocol (SCCP), vaak simpelweg Skinny genoemd, is een Cisco-protocol voor bedrijfseigen signalering. Het wordt voornamelijk gebruikt door Cisco Unified Communications Manager (CUCM), Cisco Unified Communications Manager Express (CME) routers en Cisco IP Phones om het instellen en beheren van oproepen te vergemakkelijken.

Het SCCP-protocol gebruikt TCP op poort 2000 voor niet-beveiligde SCCP en poort 2443 voor beveiligde SCCP.

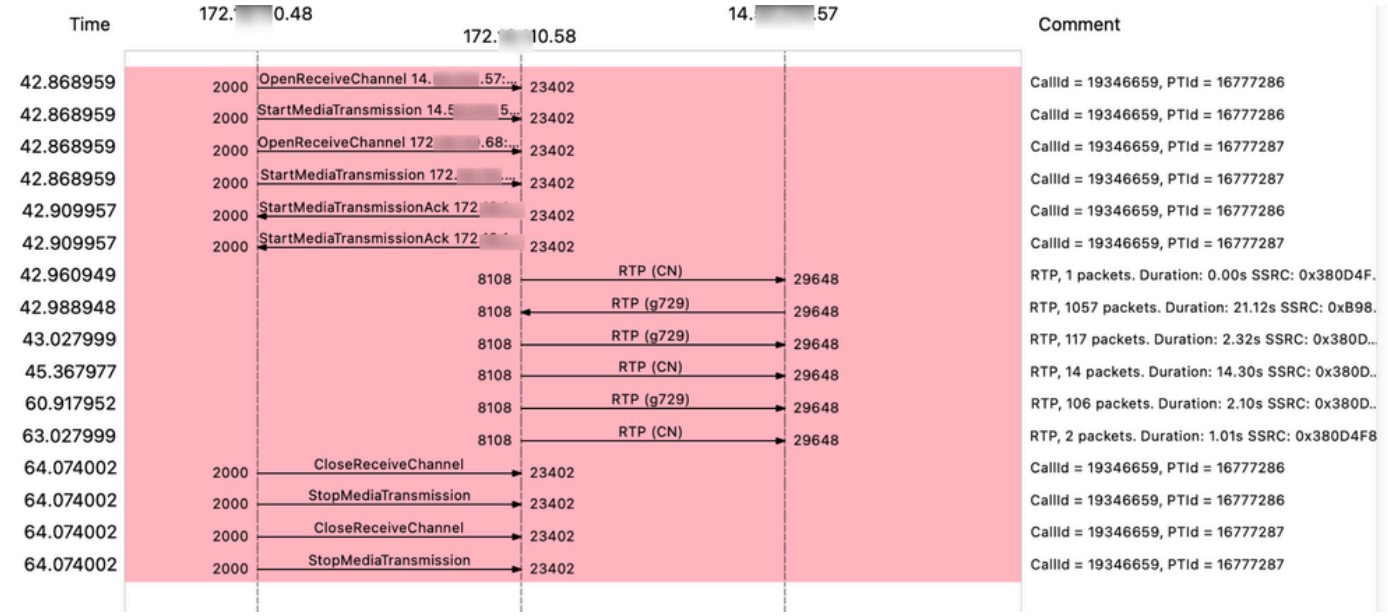
Dit zijn de gebruikelijke SCCP-berichten die u kunt vinden op een SCCP-oproep:

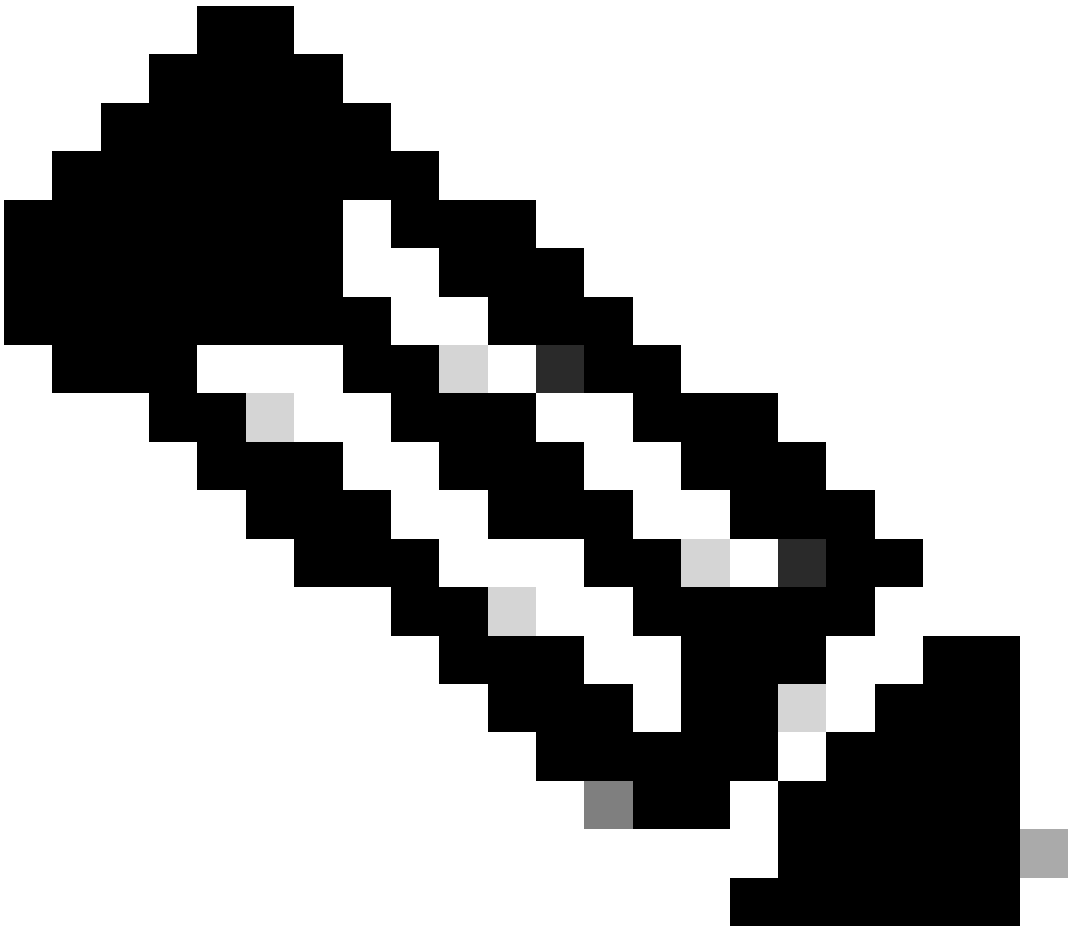


Deze pakketopname toont verzoeken en antwoorden van twee SCCP-apparaten en ook het media- (spraak)verkeer:

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

Dit is een voorbeeld van een stroom van zowel SCCP-signalering als RTP-media (spraak):





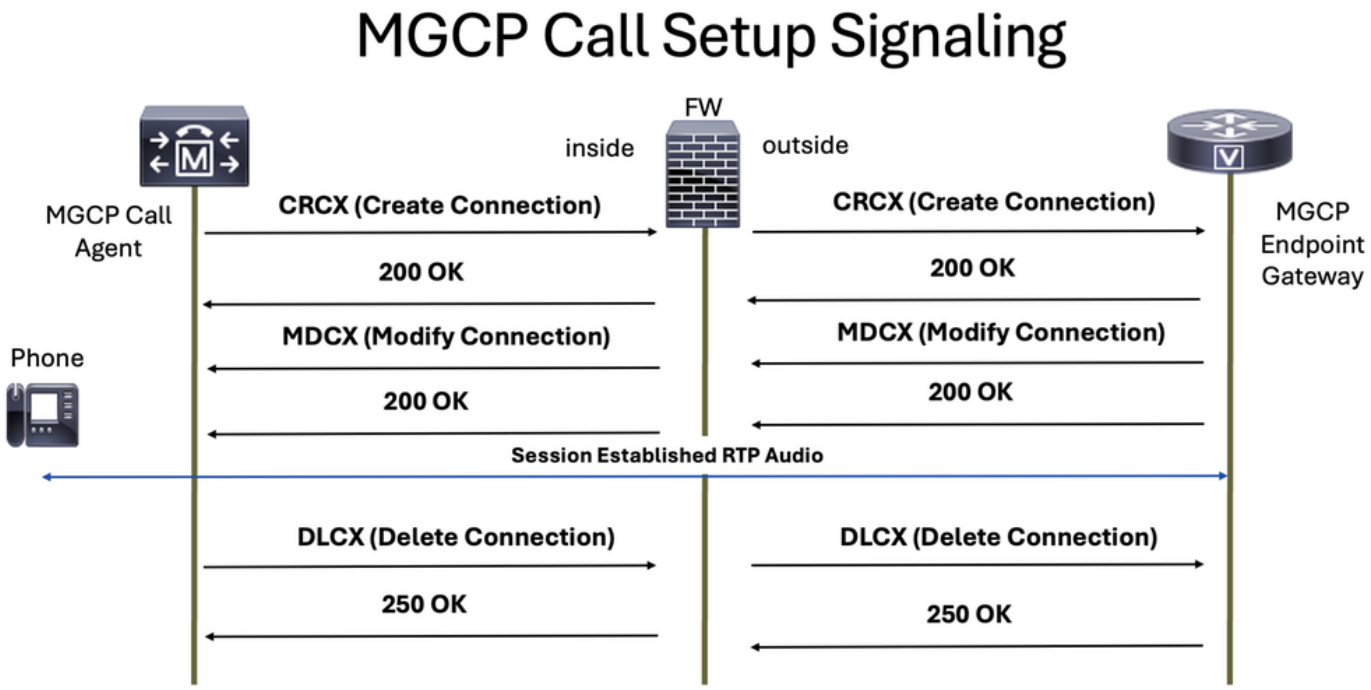
Opmerking: SCCP-inspectie is standaard ingeschakeld voor Cisco Secure Firewall Threat Defense (FTD) en Secure Firewall Adaptive Security Appliance (ASA).

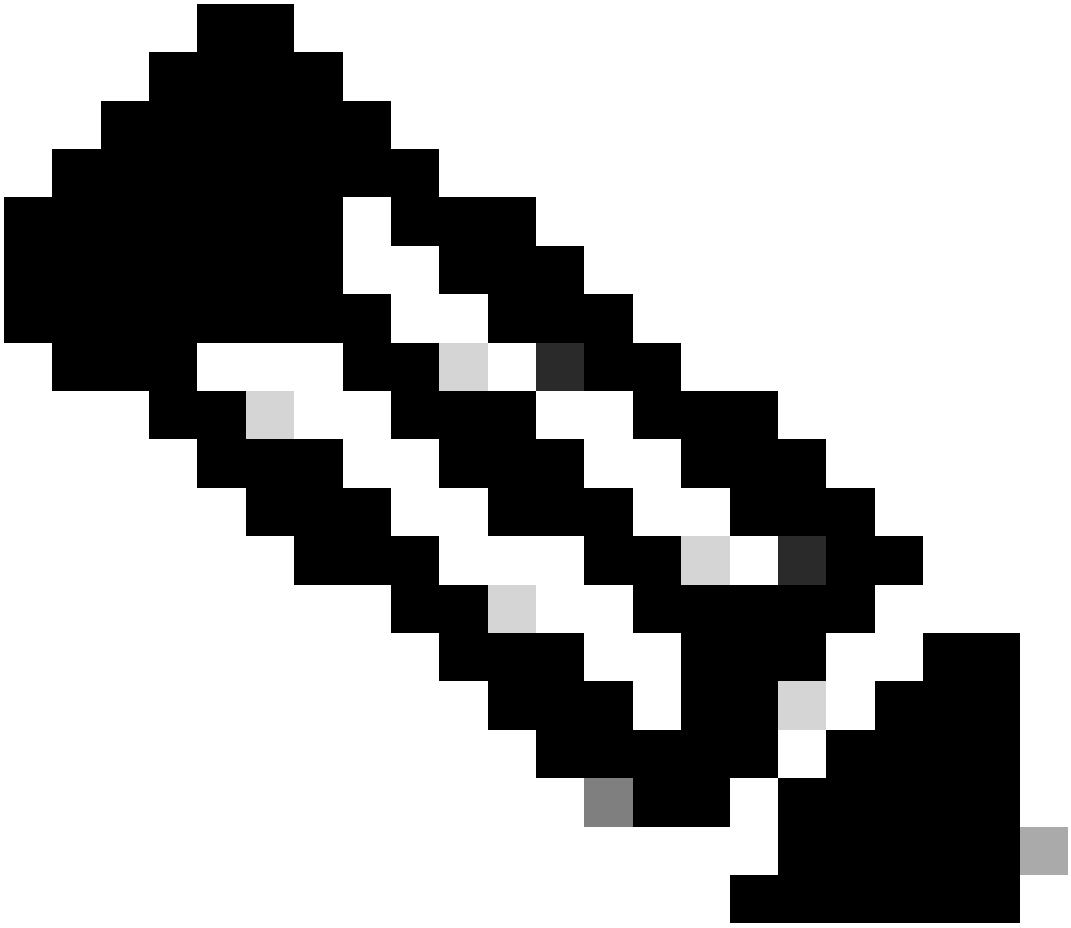
MGCP

Media Gateway Control Protocol (MGCP) is een protocol dat wordt gebruikt voor de besturing van VoIP-oproepen door een oproepbesturingsapparaat, bijvoorbeeld CUCM.

Het MGCP-signaleringsprotocol is gedefinieerd op RFC 2705 en gebruikt TCP-poort 2428 en UDP-poort 2427 voor communicatie.

De MGCP normale pakketten die u verwacht voor een oproep communicatie zijn:



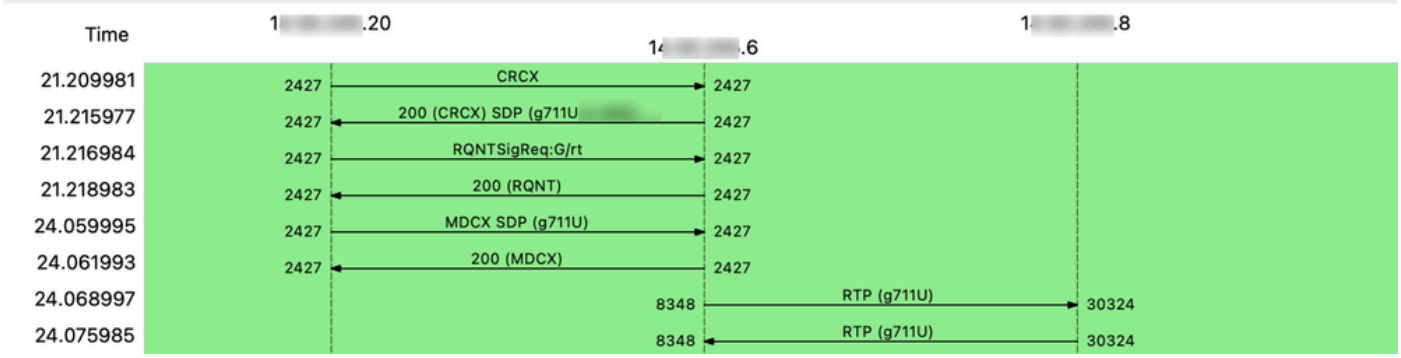


> Opmerking: MGCP-inspectie is niet ingeschakeld in het standaard inspectiebeleid voor Cisco Secure Firewall Threat Defense (FTD) en Secure Firewall Adaptive Security Appliance (ASA), dus u moet deze inspectie inschakelen als u deze inspectie nodig hebt.

Deze pakketopname toont verzoeken en antwoorden van twee MGCP-apparaten en ook het media- (spraak)verkeer:

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

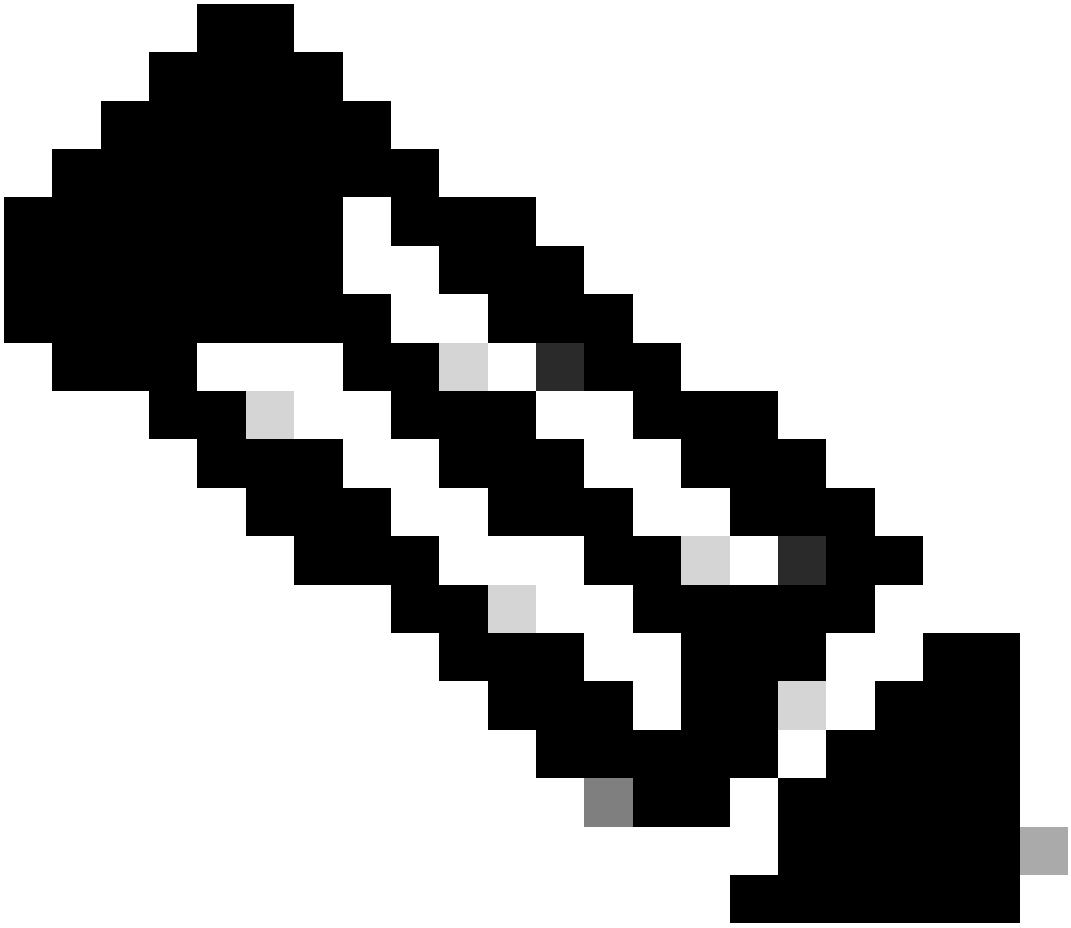
Dit is een voorbeeld van een stroom van zowel MGCP-signalering als RTP-media (spraak):



beste praktijken

Voor ASA:

- Gebruik een vergunningsregel die het verkeer van en naar de twee signaleringscomponenten (apparaten of servers) mogelijk maakt. Dit kan worden beperkt door de poorten die worden gebruikt op het opgegeven VoIP-signaleringsprotocol.
- Sta het RTP-poortbereik toe tussen de media-apparaten die audio- en/of videostreams kunnen verzenden en/of ontvangen.



Opmerking: houd er rekening mee dat deze audio- of mediaapparaten kunnen verschillen van de signaleringscomponenten (apparaten of servers).

Voor FTD:

- Definieer voorfilterregels voor signaleringsonderdelen (apparaten of servers) en definieer de specifieke poort om alleen het verkeer voor het opgegeven signaleringsprotocol te beperken.
- Configureer het voorfilter voor het RTP-protocol voor audio en/of video.

Problemen oplossen

Bij het oplossen van spraakproblemen moet u weten of het probleem signalering of media (spraak of video) of beide is, hier zijn enkele voorbeelden die u kunnen helpen om dit te onderscheiden:

Voorbeelden van signaleringsproblemen:

++De gebruiker meldt dat de oproep niet tot stand is gebracht.

++De gebruiker kan geen andere gebruikers of nummers bellen.

++De SIP Trunk verschijnt niet, omdat het OPTIONS-bericht geen reactie krijgt.

++Mijn apparaat kan zich niet registreren.

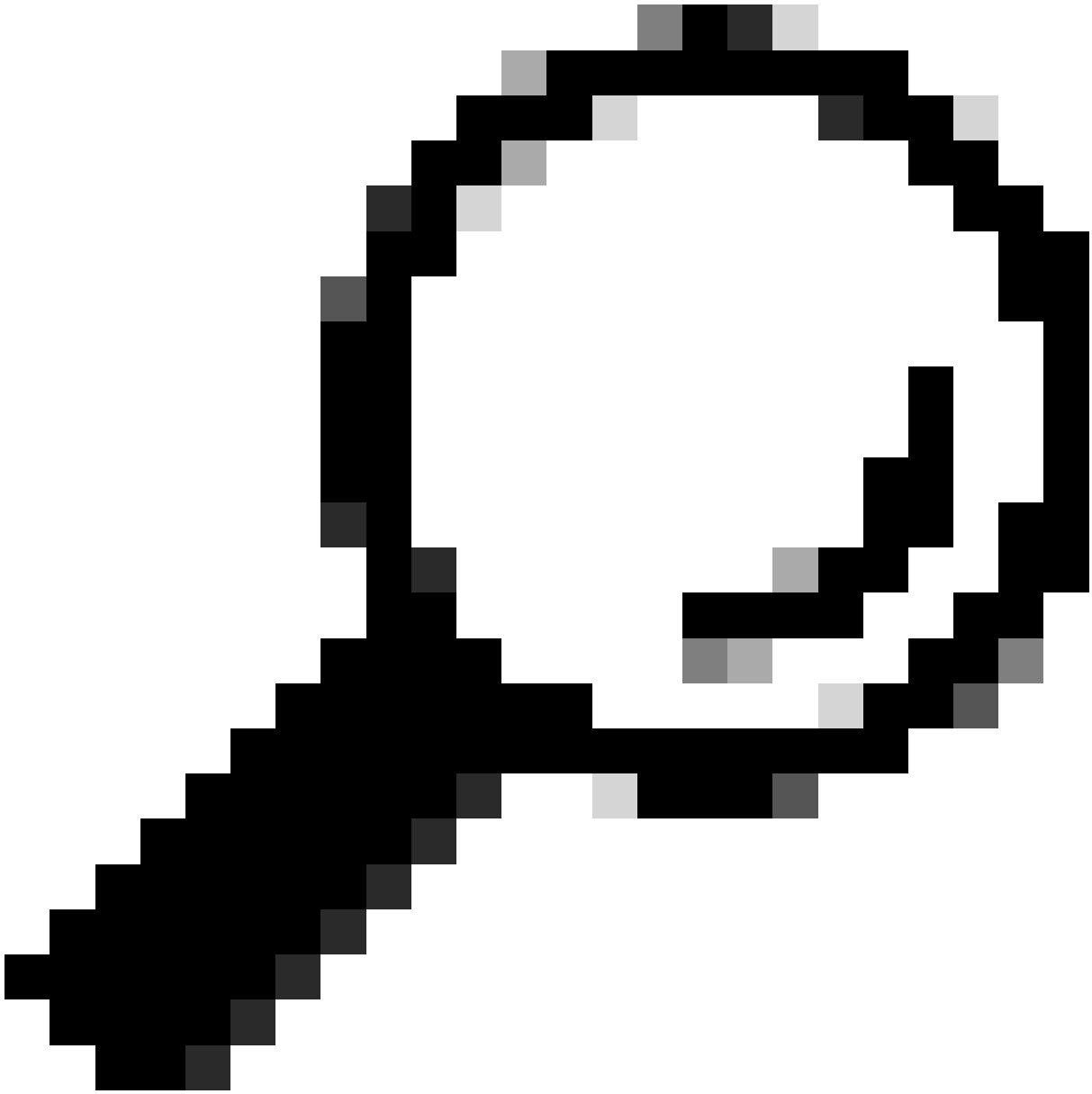
Voorbeelden van media (spraak of video) problemen:

++Er is een eenrichtingsaudioprobleem.

++Er is geen audio aanwezig.

++ Er is helemaal geen video.

++De oproep wordt stil.



Tip: tijdens een videogesprek kan de SDP onderhandelen over maximaal drie medialijnen (m-lijnen): audio, video en beeld. Elke m-lijn komt overeen met een afzonderlijke Real-Time Transport Protocol (RTP) stroom per call leg, wat betekent dat er maximaal drie verschillende RTP-stromen kunnen zijn - één voor elk mediatype - op elk onderdeel van het gesprek.

Problemen met signalering in firewall oplossen

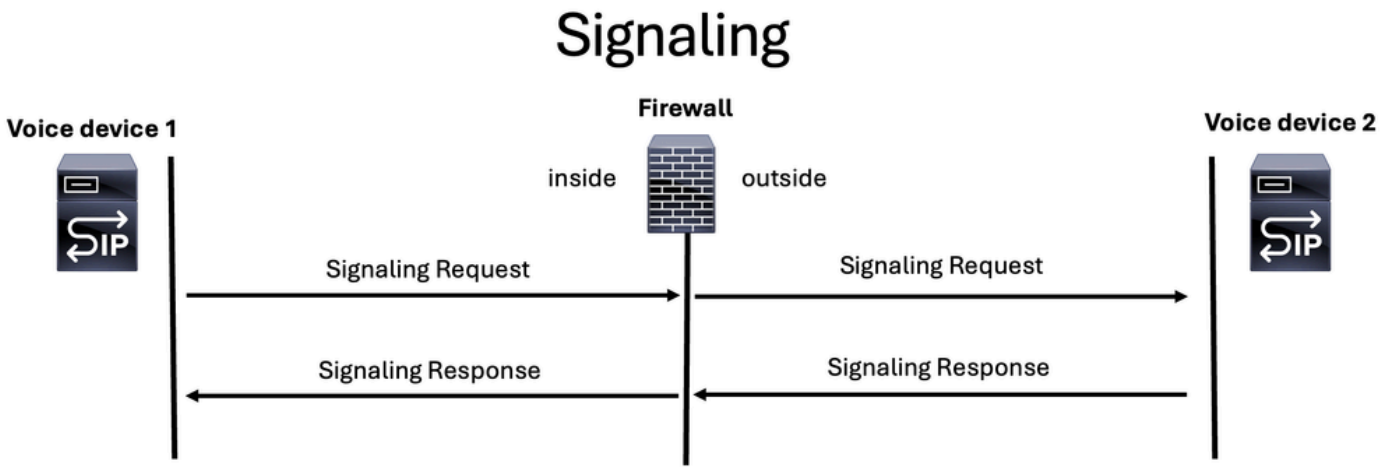
Voor het oplossen van problemen met het signaleringsonderdeel moet u ervoor zorgen dat:

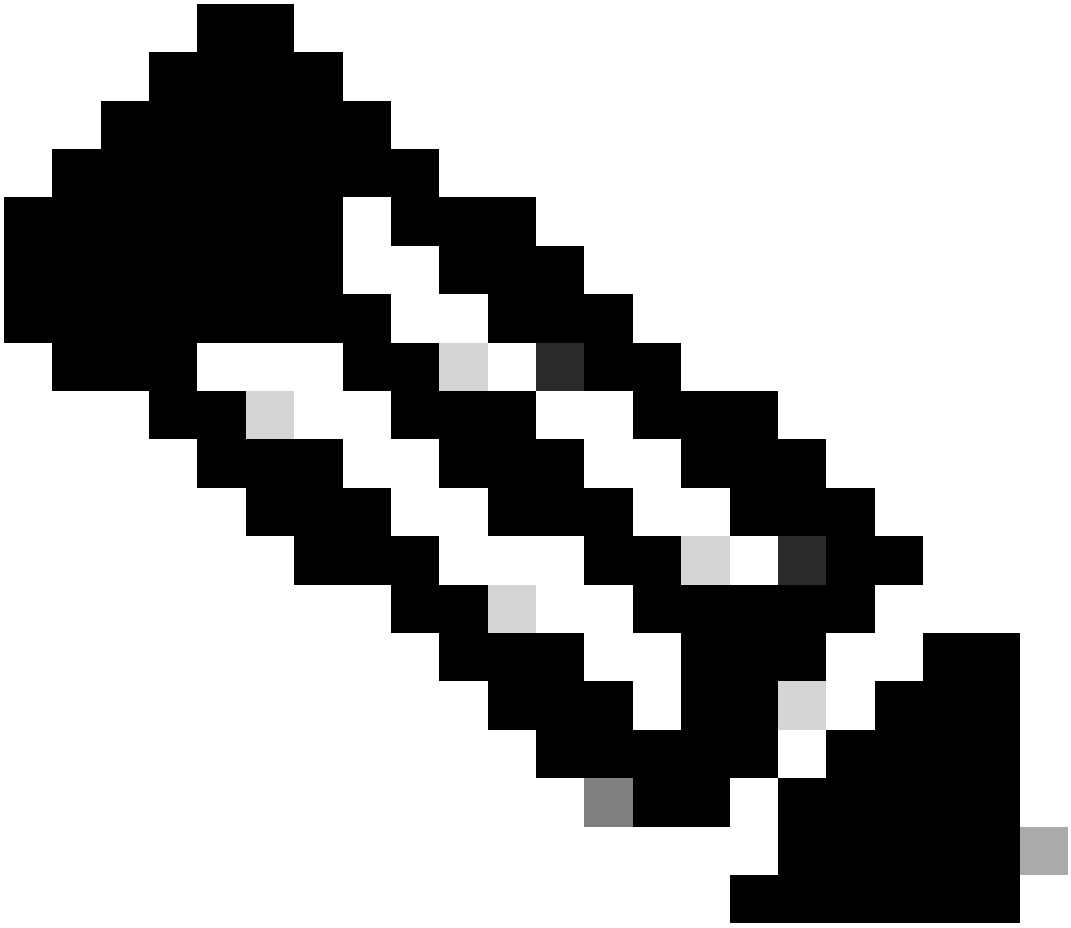
++Identificeer alle signaleringscomponenten (apparaten of servers) die betrokken zijn bij de oproep vanuit zowel de ingangen- als de uitgang-interface en configureer passende matchingcriteria op de pakketopnames op CLI van beide Secure FW.

++Vergeet niet dat het aantal signaleringsberichten op de ingangsinterface moet overeenkomen met de uitgang-interface.

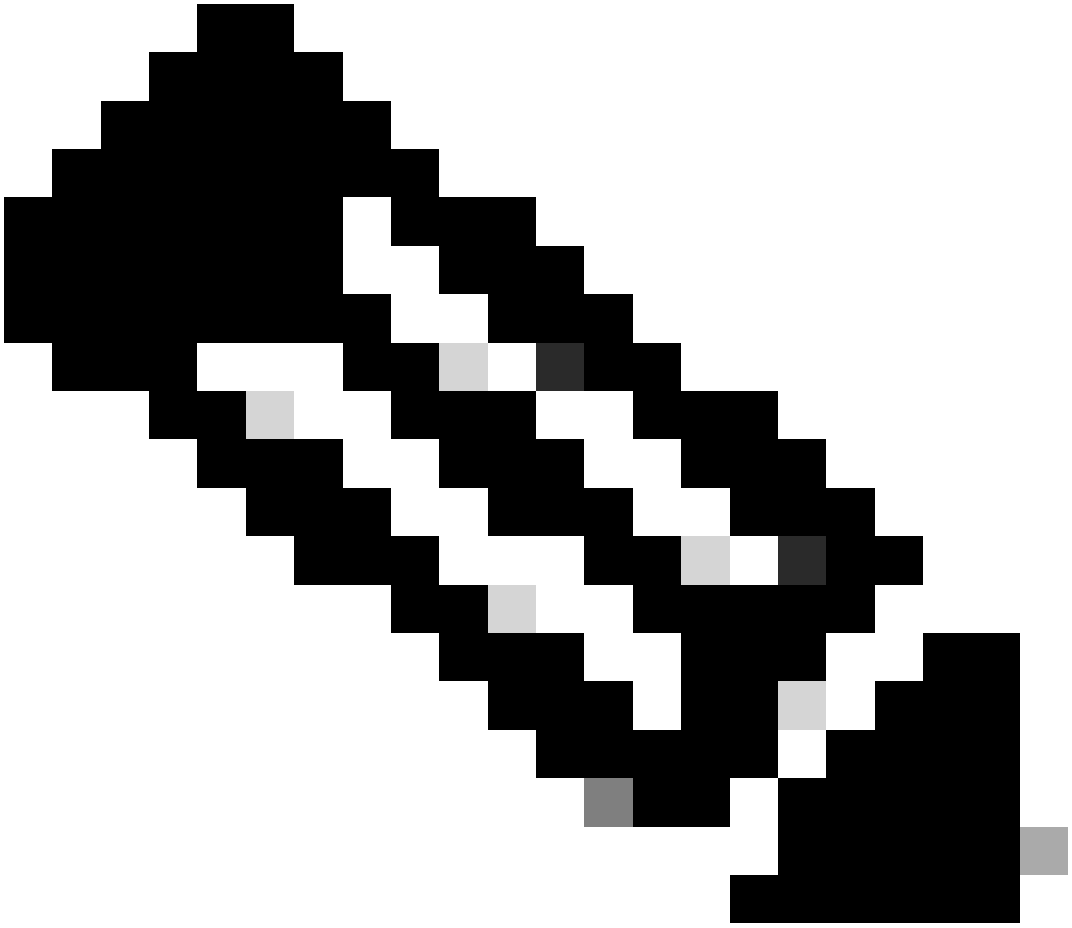
++Packet capture kan efficiënter worden gemaakt door aan te geven of het signaleringsprotocol gebruikmaakt van TCP of UDP en door te filteren op het verwachte poortnummer. Aangezien alle signaleringsprotocollen via IP werken, helpt het toepassen van deze filters op de CLI de hoeveelheid verkeer die u in uw opnamen ziet, te beperken.

++Alleen voor uitgang-interfaces moet u ervoor zorgen dat het NAT IP-adres dat is toegewezen aan uitgaand verkeer, wordt opgegeven in het pakketopnamefilter. Dit zorgt ervoor dat u het juiste verkeer vastlegt zoals het op de uitgang-interface wordt weergegeven.





Opmerking: Onthoud dat, ongeacht welk signaleringsprotocol wordt gebruikt voor spraak, er altijd een verzoek en een antwoord moet zijn en consistent moet zijn op zowel de ingangen als de ingangen.

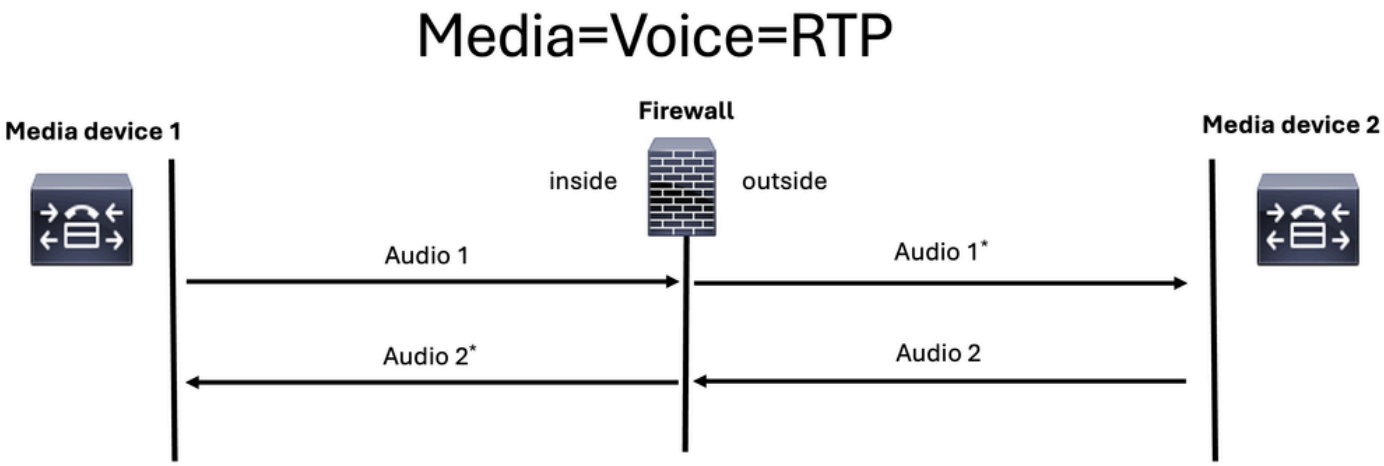


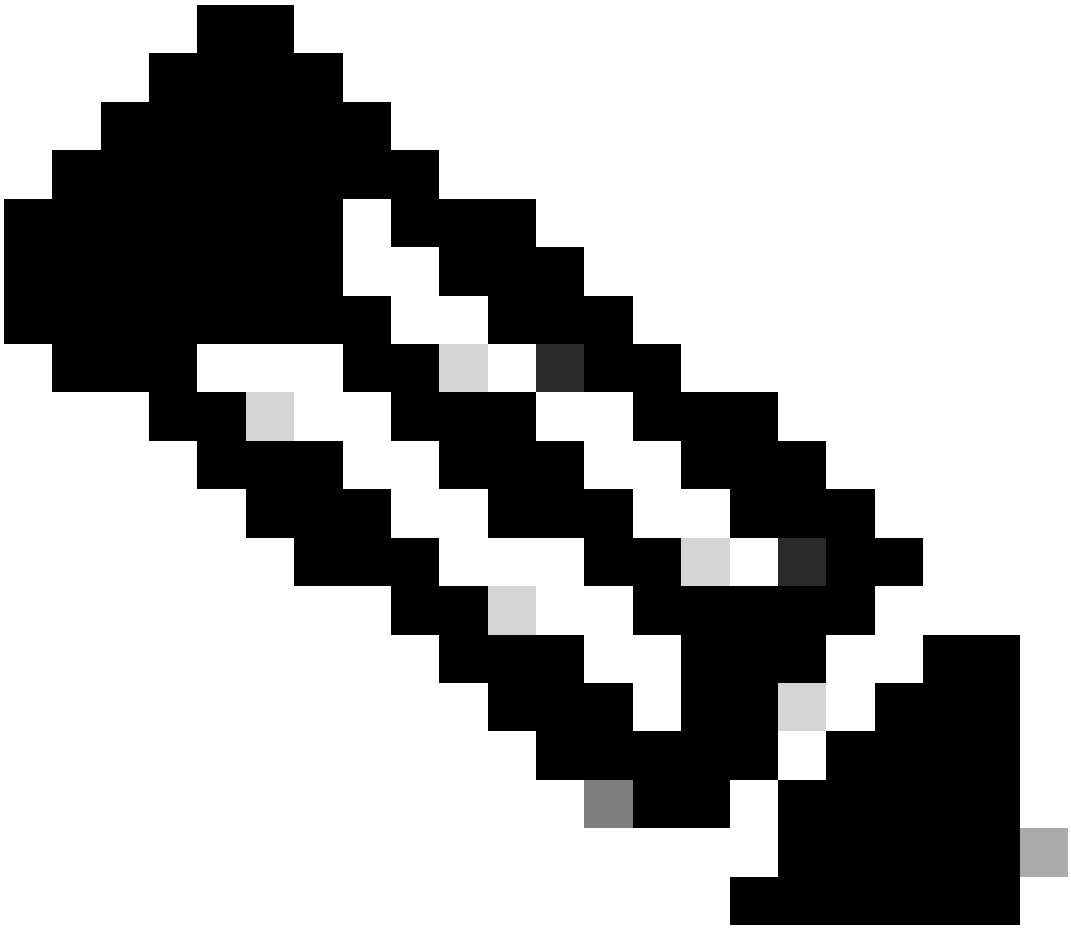
Opmerking: zorg er waar mogelijk voor dat er slechts één firewall is betrokken bij het communicatiepad. In sommige implementaties kunnen spraaksignalering en mediastromen afzonderlijke firewalls doorkruisen. Zorg er in deze gevallen voor dat u alle relevante firewalls in uw probleemoplossingsproces opneemt

Problemen met media oplossen in Firewall

Vanuit FW-perspectief zullen er 4 streams zijn die moeten worden geanalyseerd bij het oplossen van eenrichtingsaudio, tweewegaudio-problemen of geen audio:

1. RTP Stream van beller naar beller (Ingress Interface).
2. RTP-stream van beller naar beller (Eress-interface).
3. RTP-stream van gebeld naar beller (Egress-interface).
4. RTP-stream van oproep naar beller (Ingress-interface).



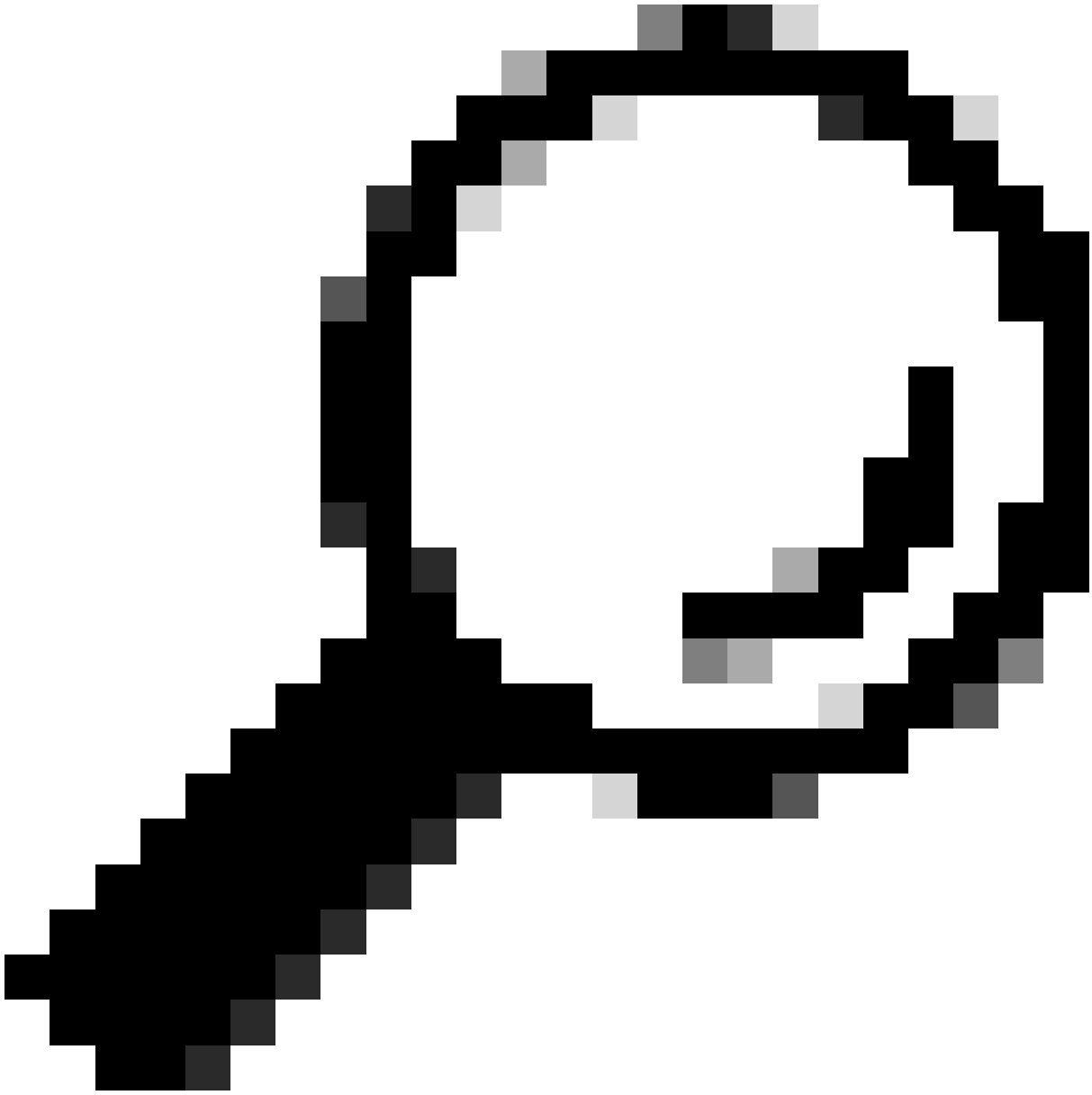


Opmerking: zorg ervoor dat u problemen oplost met behulp van CLI-pakketopnames in de ASA- of LINA-modus op de FTD, omdat dit meer flexibiliteit biedt om meerdere matches toe te passen binnen één pakketopname.

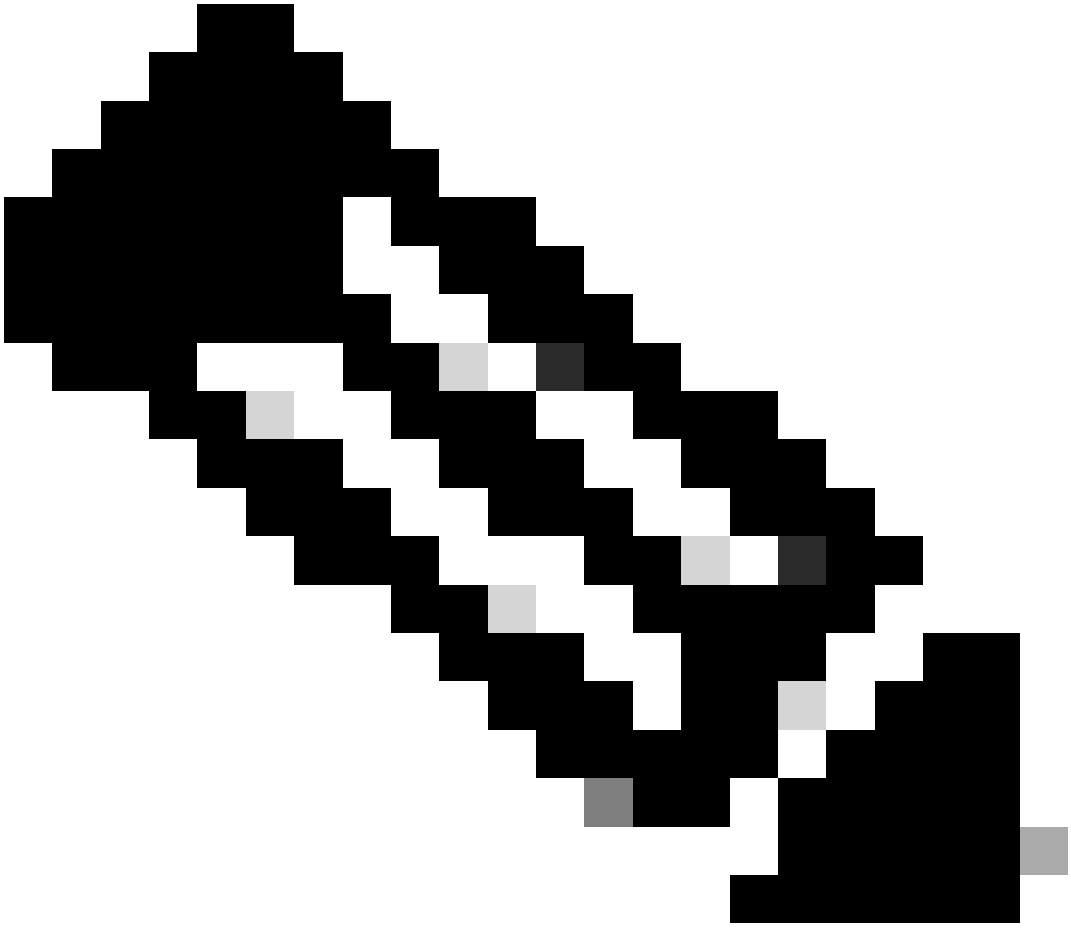
Problemen oplossen met SIP-oproepen

Bij het oplossen van spraakproblemen op Secure FW (ASA of FTD) moet u de volgende stappen uitvoeren:

1. Zorg ervoor dat u de oproepstroom en het topologiediagram hebt.
2. Zorg ervoor dat u het probleem begrijpt vanuit het perspectief van de gebruiker.
3. Begrijp het pad voor het signaleringsprotocol.
4. Begrijp het pad van het RTP-protocol.
5. Neem pakketopnames op zowel de ingress- als de egress-interfaces.
6. Controleer de configuratie-ACL-regels en NAT-regels.
7. Controleer of het SIP-signaleringsverkeer niet wordt geblokkeerd door de firewall. Vergelijk daarnaast de ingangen- en uitgangen-interfaces om de spraakverkeersstroom te analyseren.
8. Controleer of het RTP-mediaverkeer niet wordt geblokkeerd door de firewall door de verkeersstroom op de in- en uitgangen te vergelijken.
9. Zorg ervoor dat de signaleringsapparatuur ondersteuning biedt voor inspectie en, indien niet, schakel deze uit.



Tip: De SIP-signaleringsberichten die de FW binnenkomen, moeten ook hetzelfde zijn als het verlaten van de FW.



Opmerking: de tips voor probleemoplossing voor SIP kunnen ook worden toegepast op H.323-, MGCP- en SCCP-protocollen.

Gerelateerde informatie

- ASA-pakketopnamen configureren met CLI
- Firepower Threat Defence Captures gebruiken

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.