Grundlegende Informationen zu Voice-over-IP-Protokollen für eine sichere Firewall

Inhalt

Einleitung

In diesem Dokument werden die Grundlagen der verschiedenen VoIP-Protokolle beschrieben, die den Technikern bei der effektiven Fehlerbehebung in sicheren Firewalls helfen.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist für die Verwendung in Fehlerbehebungsszenarien mit folgenden Geräten vorgesehen:

- Sichere Firewall-Bedrohungsabwehr (FTD)
- Secure Firewall Adaptive Security Appliance (ASA)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

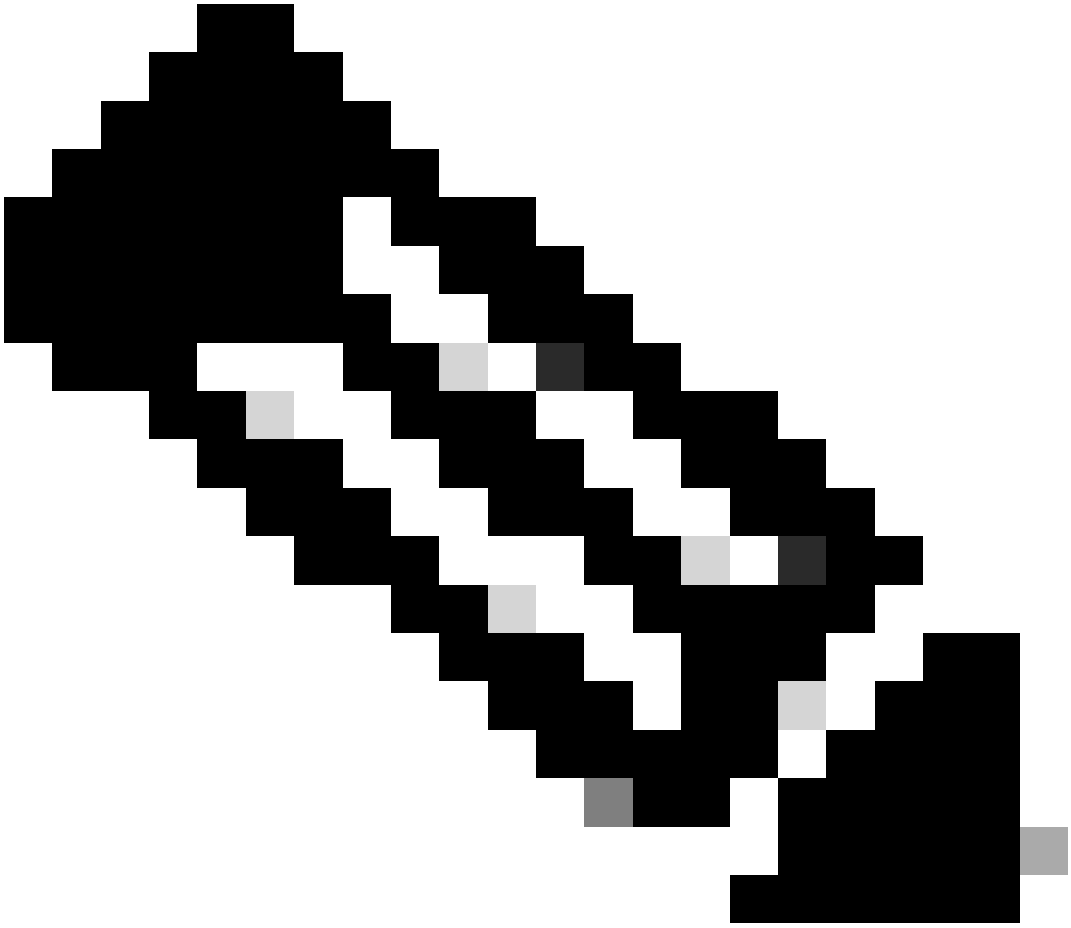
Grundlagen von VoIP

Kommunikation ist für menschliche Interaktionen von grundlegender Bedeutung, und VoIP-Protokolle (Voice over IP) sind für die menschliche Kommunikation unverzichtbar geworden. Aus diesem Grund ist es wichtig, ihre Teile zu kennen, wenn Sie ein Szenario mit einer Firewall (FW) beheben.

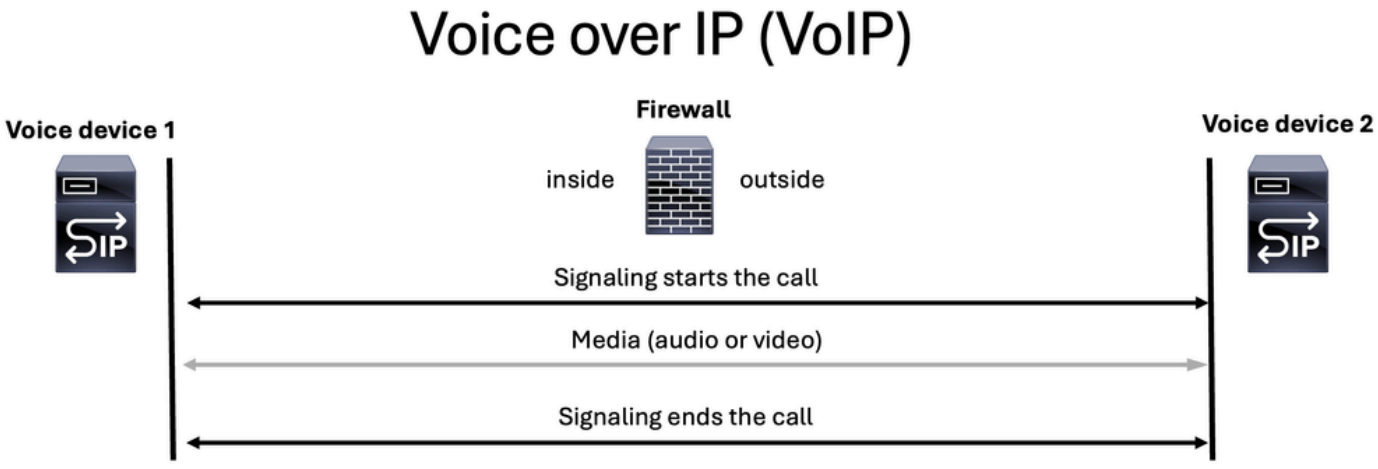
Das VoIP besteht aus zwei Teilen:

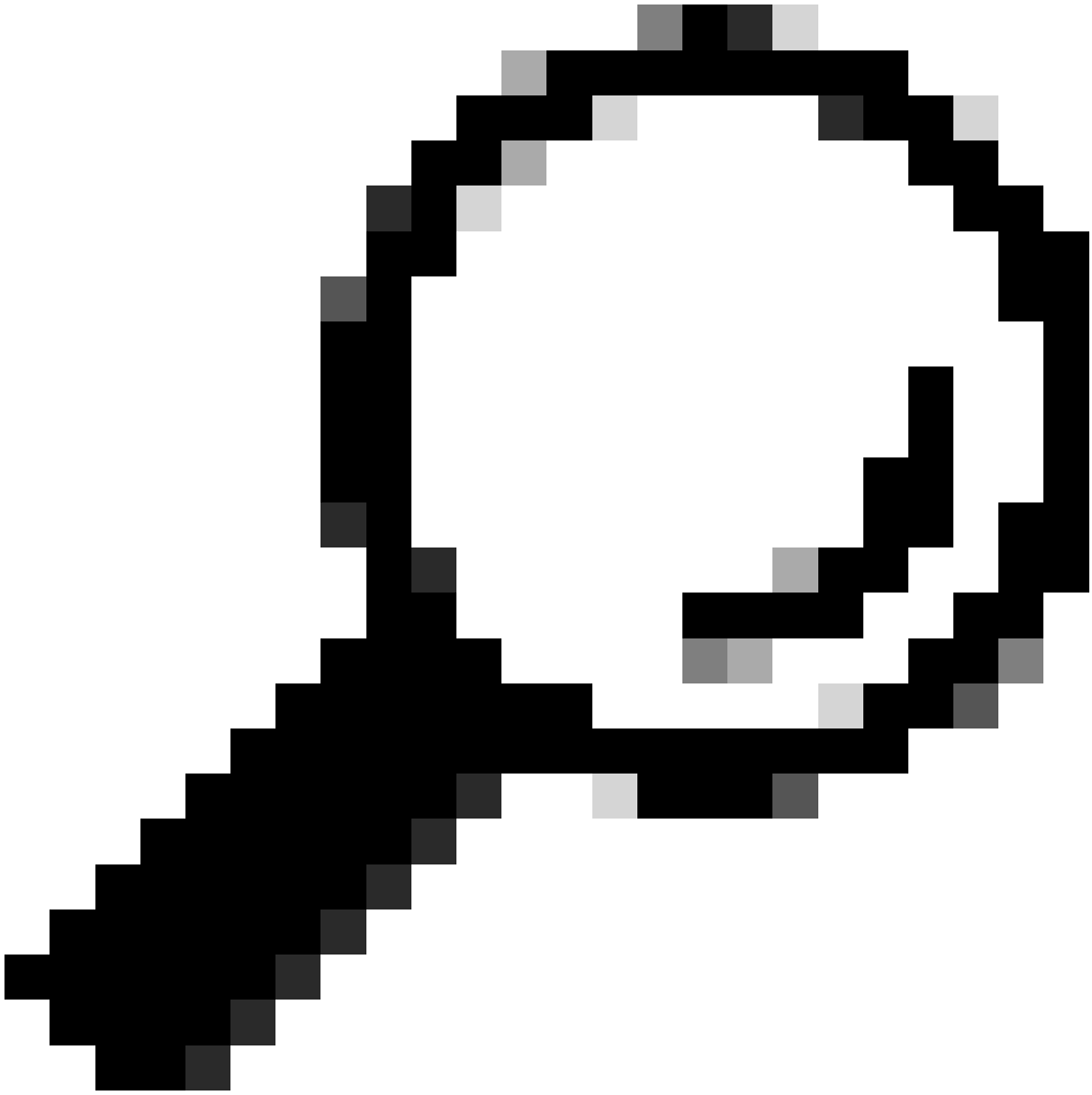
- Signalisierung
- Medien (Sprache oder Video)

Die VoIP-Kommunikation beginnt immer mit einem Signalisierungsteil, um einen Anruf zu starten. Anschließend wird das Medium (Sprache oder Video) gestreamt, und schließlich wird der Anruf durch die Signalisierung beendet.

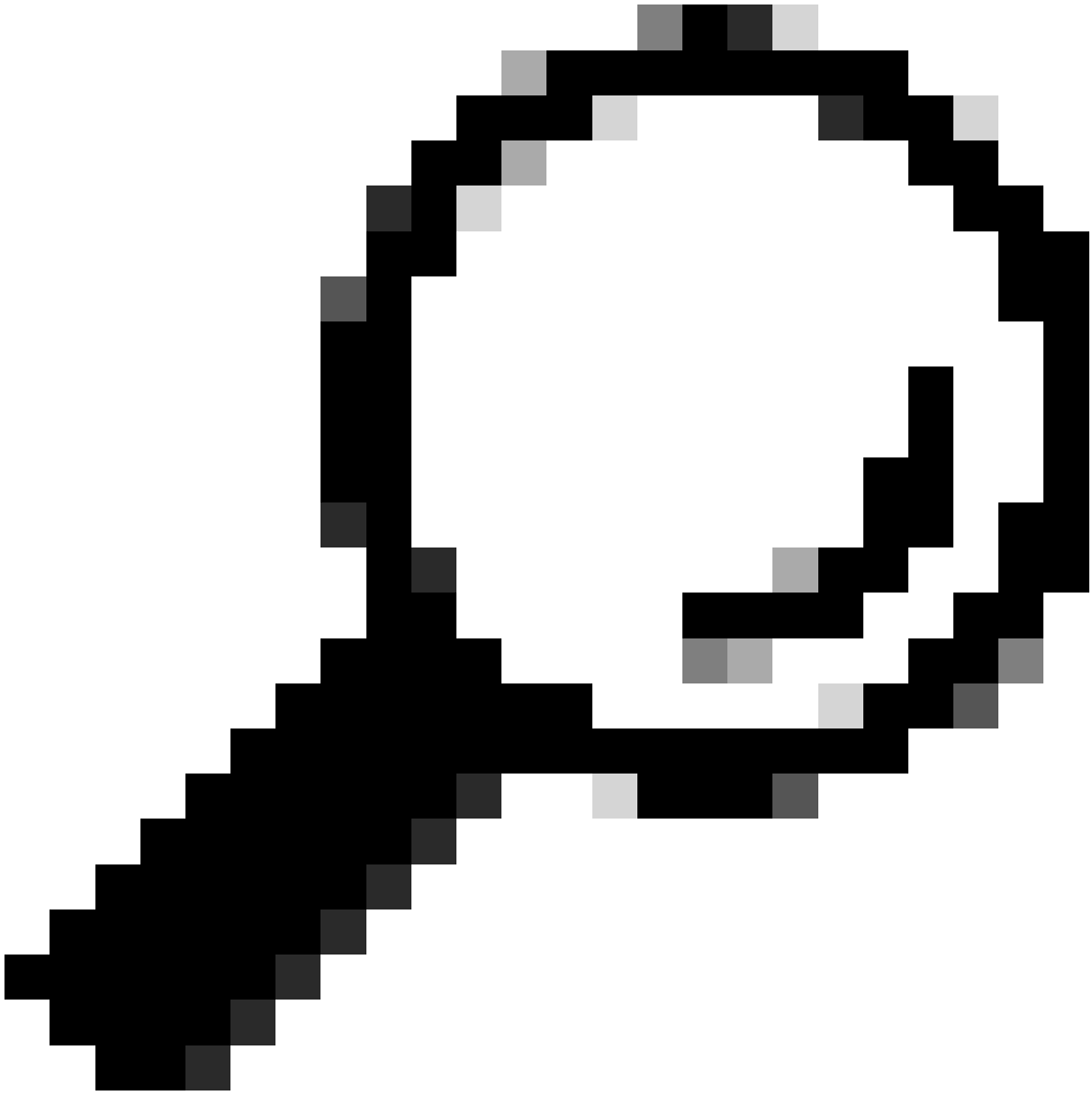


Anmerkung: SIP ist das am häufigsten verwendete Protokoll und wird daher in vielen Diagrammen durchgängig als SIP-Sprachserversymbol dargestellt.





Tipp: Bei der Behebung eines Sprachproblems für ASA oder FTD ist es wichtig, das Szenario aus der Perspektive des Benutzers zu betrachten. Sie müssen feststellen, ob der Anruf angenommen wurde oder ob es kein Audio oder unidirektionales Audio gibt. Diese Informationen liefern wertvolle Hinweise darauf, ob das Problem beim Signalisierungsprotokoll oder beim Medienprotokoll (Sprache oder Video) liegt.



Tipp: Ein Sprachgerät kann den RTP-Verkehr (Real-time Transport Protocol), den Signalisierungsverkehr oder beide gleichzeitig verwalten. Bei der Behebung von Sprachproblemen müssen folgende Hauptkonzepte beachtet werden:

++Signalisierungsserver: Diese Server sind ausschließlich für die Verarbeitung des Signalisierungsverkehrs zuständig.

++Medienserver: Diese Server verarbeiten ausschließlich den Sprach-RTP-Verkehr.

++ Einige Geräte können beide Aufgaben ausführen.

Signalisierung

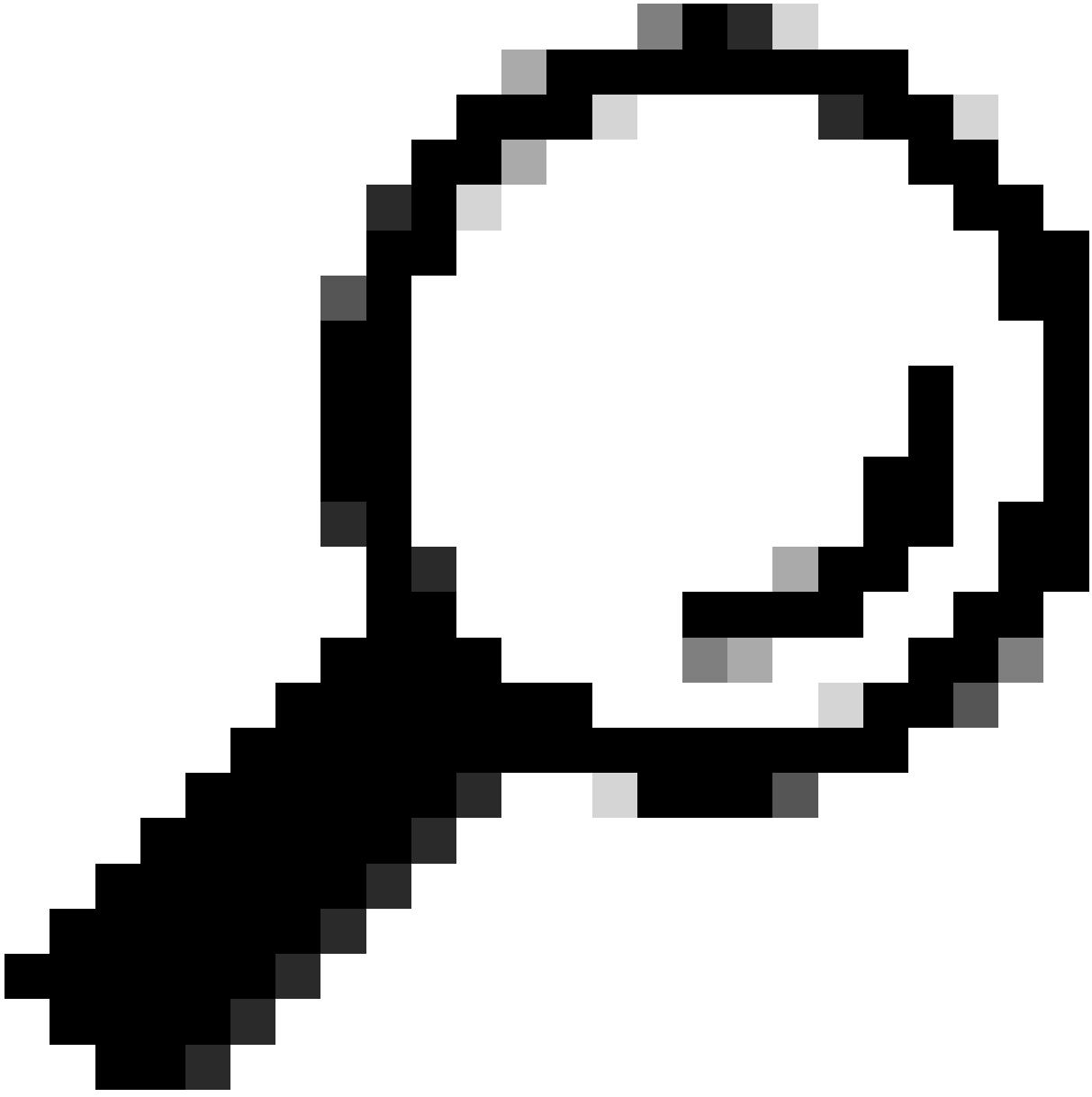
Das Signalisierungsprotokoll ist der Teil eines Anrufs, der die Sprachkommunikation startet. Es

führt jedoch nicht nur diese Funktionen aus:

- Hält die Kommunikation aufrecht.
- Ändert die Kommunikation.
- Beendet die Kommunikation.

Verschiedene Signalisierungsprotokolle helfen bei der Herstellung eines Anrufs. Zu den gängigsten gehören:

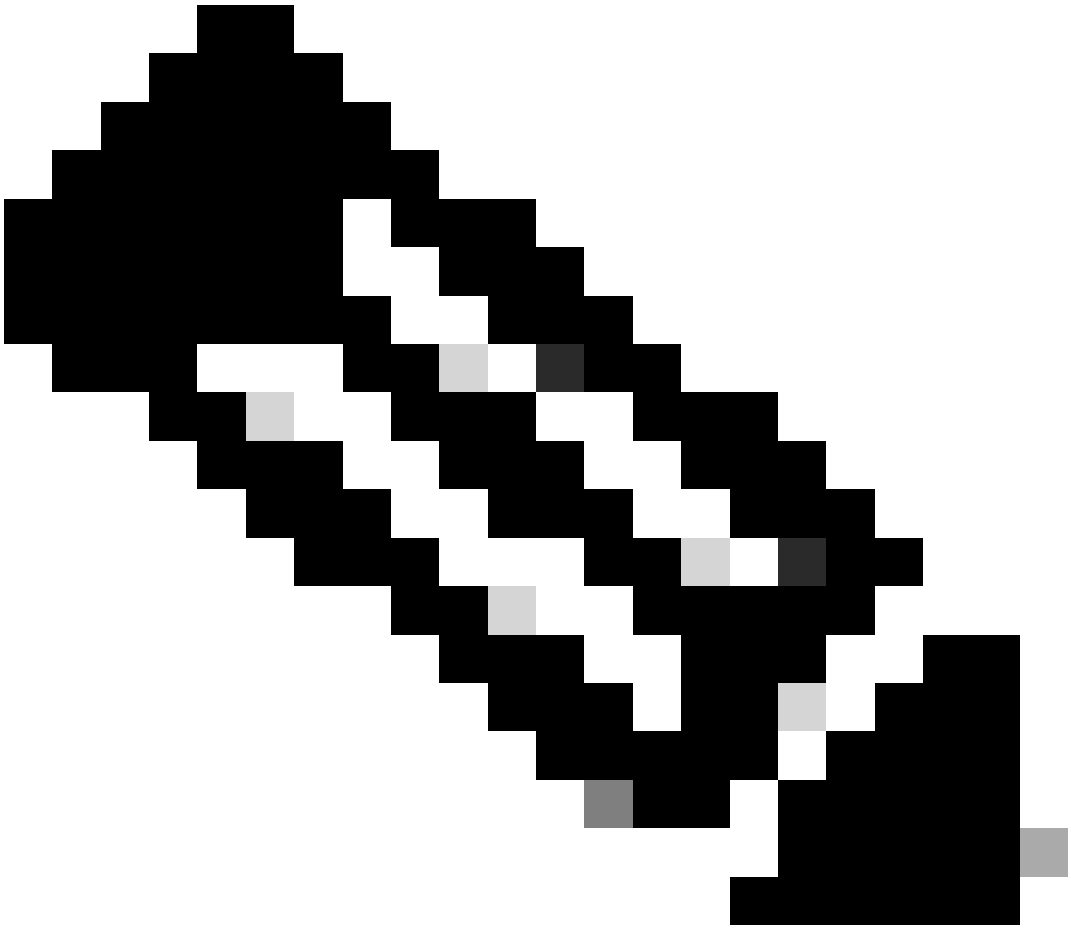
- Session Initiation Protocol (SIP)
- H,323
- Media Gateway Control Protocol (MGCP)
- SCCP (Skinny Call Control Protocol)



Tipp: Es ist wichtig, das verwendete Signalisierungsprotokoll zu identifizieren, um die

---

entsprechenden Ports für die Paketerfassung auf ASA oder FTD zu bestimmen. Darüber hinaus sind ein Anruffluss und eine Netzwerktopologie hilfreich, um den Signalisierungspfad zu verstehen.

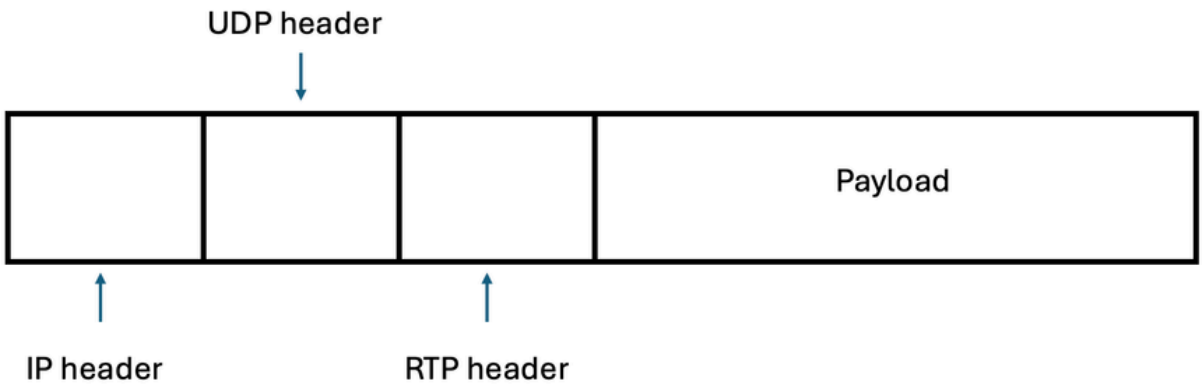


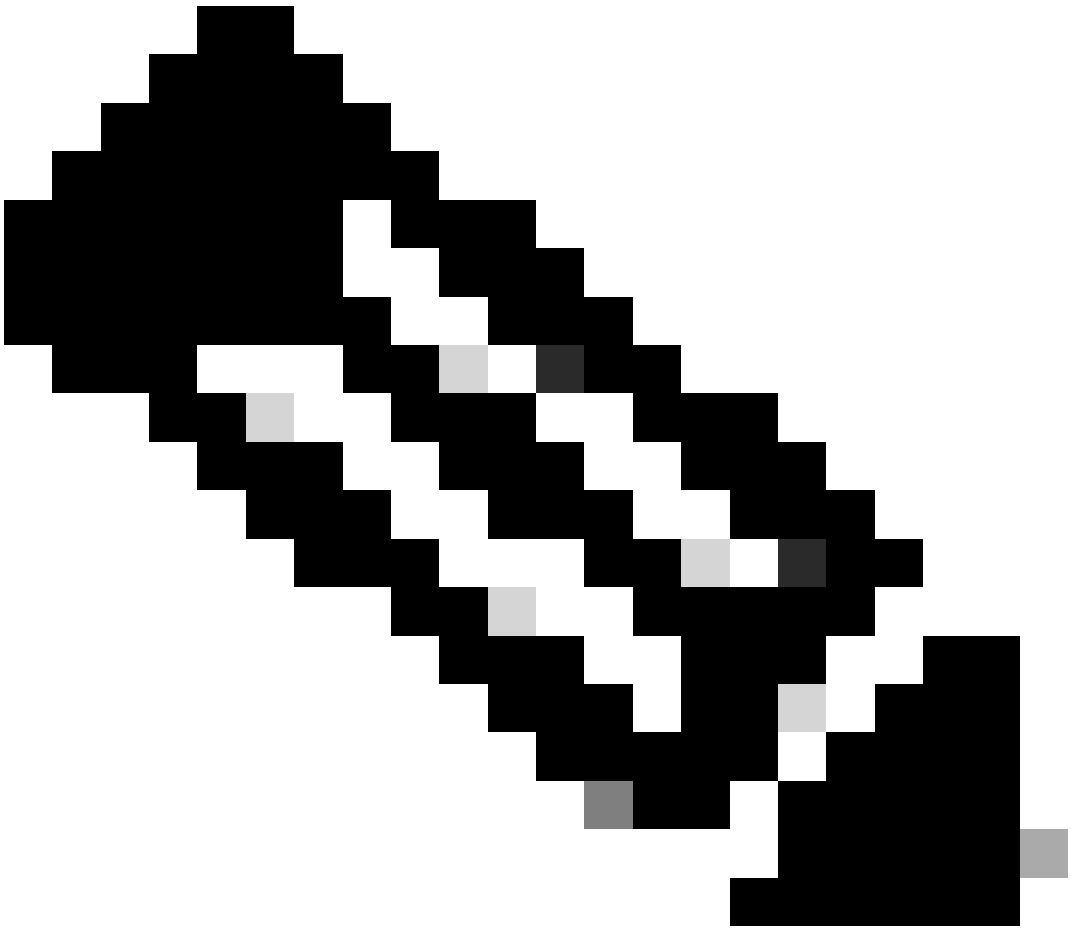
Anmerkung: Signalisierungspakete enthalten Quell- und Ziel-IP-Adressen und tragen so zur Identifizierung der Parteien bei, die am Senden und Empfangen des RTP-Medien-Streams beteiligt sind.

Medien

Nachdem die Signalisierung abgeschlossen ist und sich die Signalisierungskomponenten (Geräte oder Server) auf den Medientyp geeinigt haben, kommt das Real Time Protocol (RTP) zum Einsatz, um Medien (Audio und/oder Video) an alle Beteiligten zu senden.

RTP ist ein Internetprotokoll für Streaming-Medien, das erst nach Herstellung des Anrufs gesendet wird und über das User Datagram Protocol (UDP) ausgeführt wird.

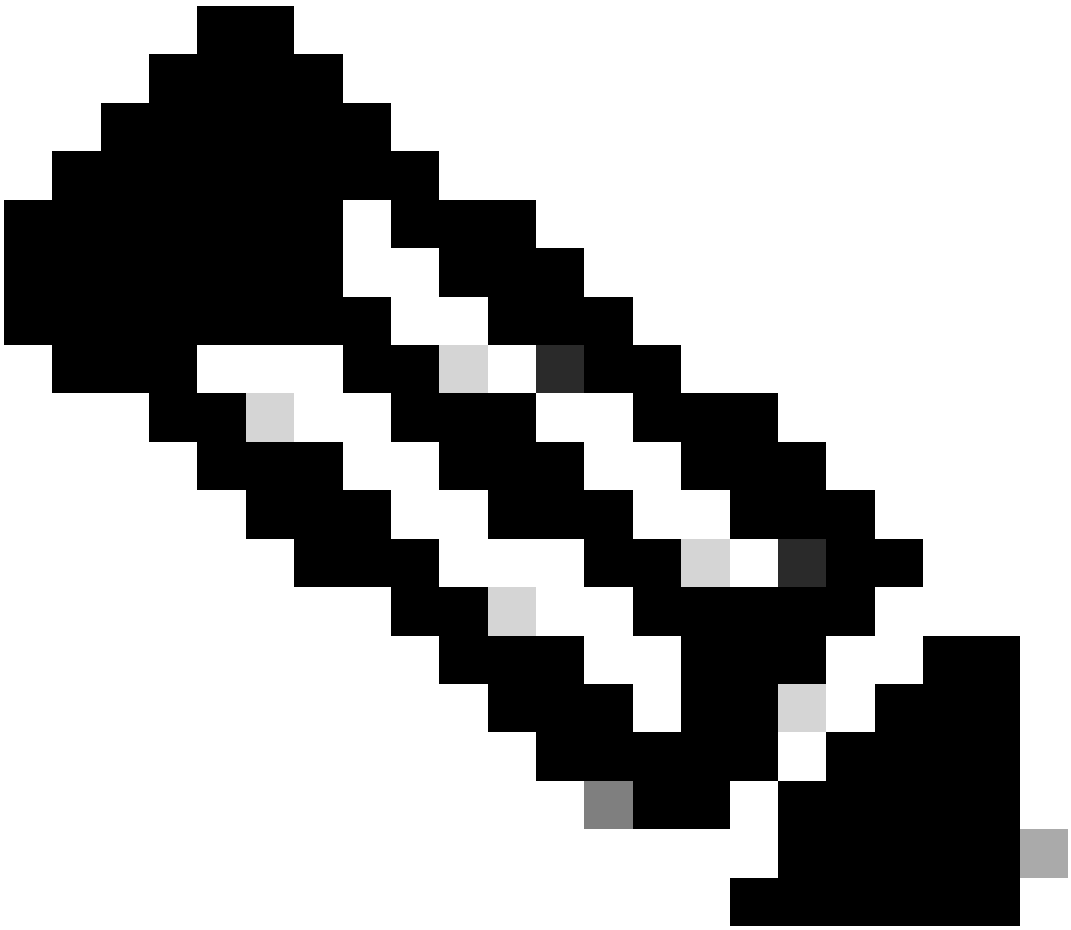




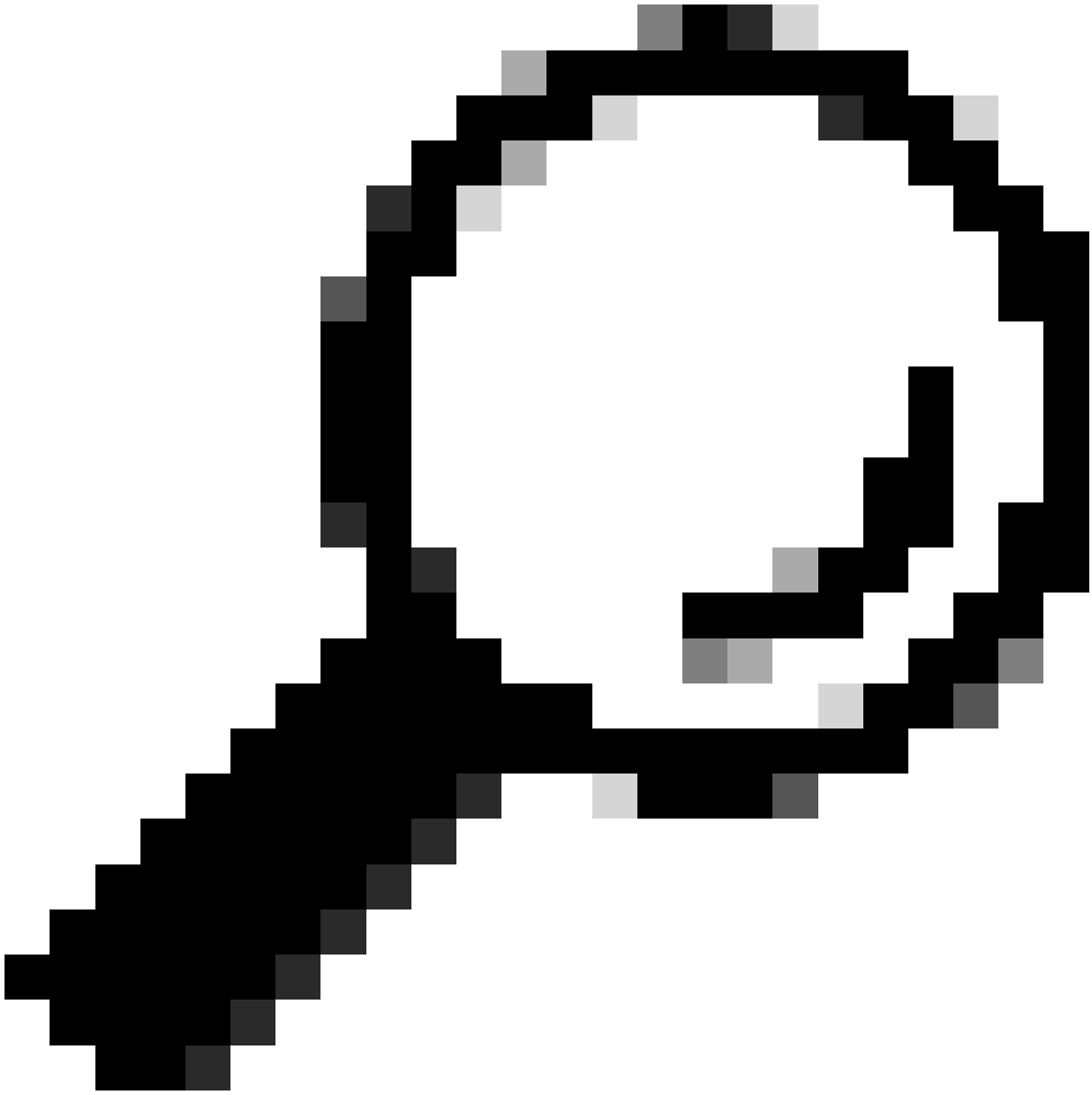
Anmerkung: Medien können Sprache und/oder Video sein und werden über RTP-Pakete übertragen.

Signalisierungskomponenten (Geräte oder Server) bestimmen, welche Ports zum Senden oder Empfangen von Medien (Audio und/oder Video) verwendet werden. Der gängigste Port-Bereich

für RTP liegt bei den meisten Geräten in der Regel zwischen 16384 und 32767.



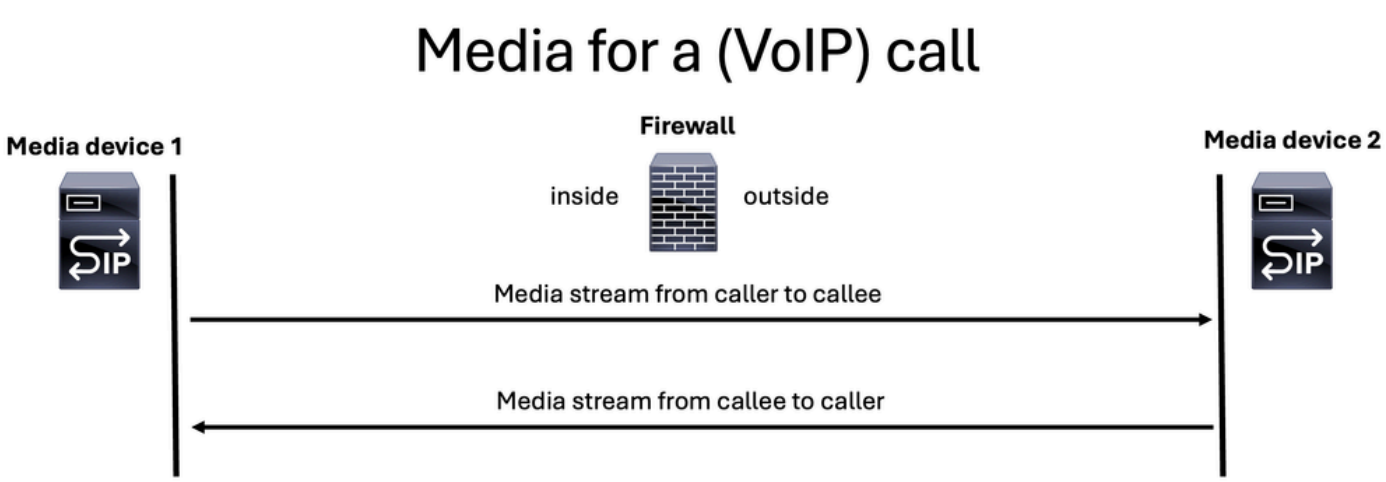
Anmerkung: Bestimmte Cisco Geräte, wie die ASR- und ISR G3-Plattformen wie die ISR4K-Plattform, verwenden einen standardisierten RTP-Port-Bereich von 8000 bis 48200. Es ist wichtig, den spezifischen RTP-Port-Bereich zu überprüfen, der auf Ihren Geräten konfiguriert ist, da er von diesen standardisierten Werten abweichen kann und von Drittanbietergeräten abweichen kann.

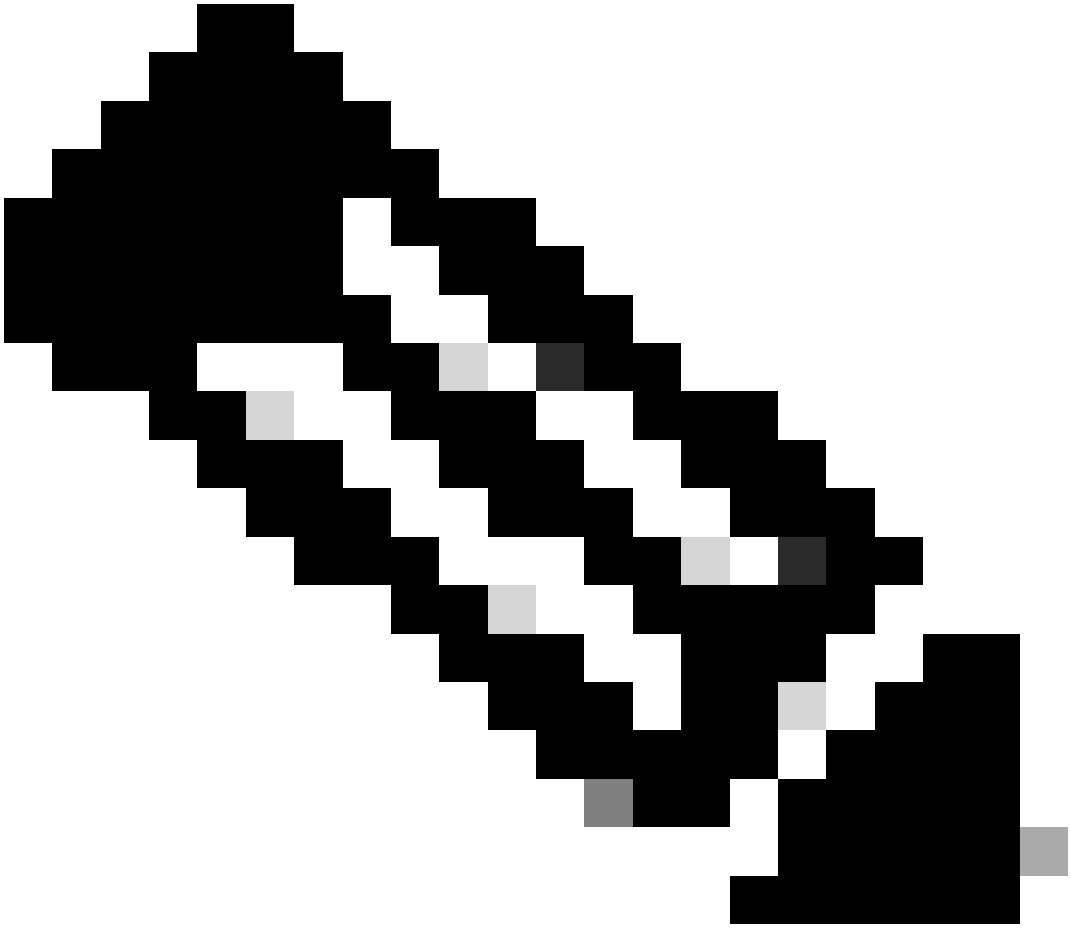


Tipp: Manchmal unterscheidet sich der RTP-Pfad vom Signalisierungspfad, weshalb es wichtig ist, die Geräte zu identifizieren, die für das Senden und Empfangen von Sprach-RTP-Paketen verantwortlich sind. Auf diese Weise wird sichergestellt, dass Sie den UDP-Datenverkehr zwischen den Geräten erfassen, die die ASA oder FTD passieren.

Es gibt zwei Medien-Streams oder RTP-Streams, die bei einem normalen Sprachanruf generiert werden:

1. Ein Medien-Stream vom Anrufer zum Angerufenen
2. Ein Medien-Stream vom Angerufenen zum Anrufer





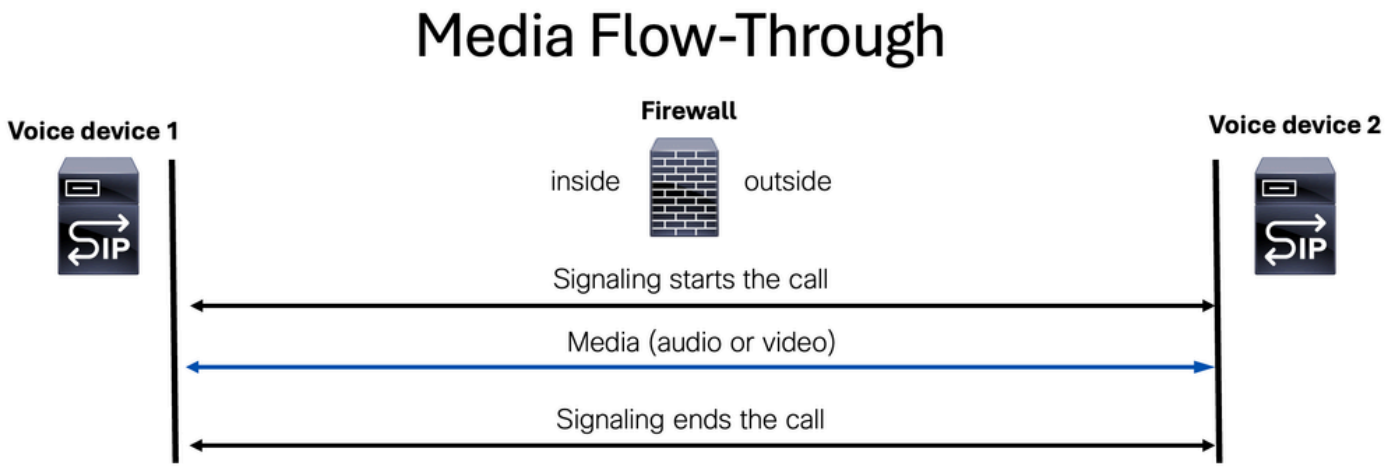
Anmerkung: Zur Veranschaulichung wird das SIP-Serversymbol verwendet, um in allen Bildern entweder einen Signalisierungs- oder einen Medienserver darzustellen.

Wenn Sie das Streaming von Medien während eines Sprachanrufs besprechen, müssen Sie zwei wichtige Szenarien hervorheben:

1. Durchfluss der Medien
2. Umgehung von Medien

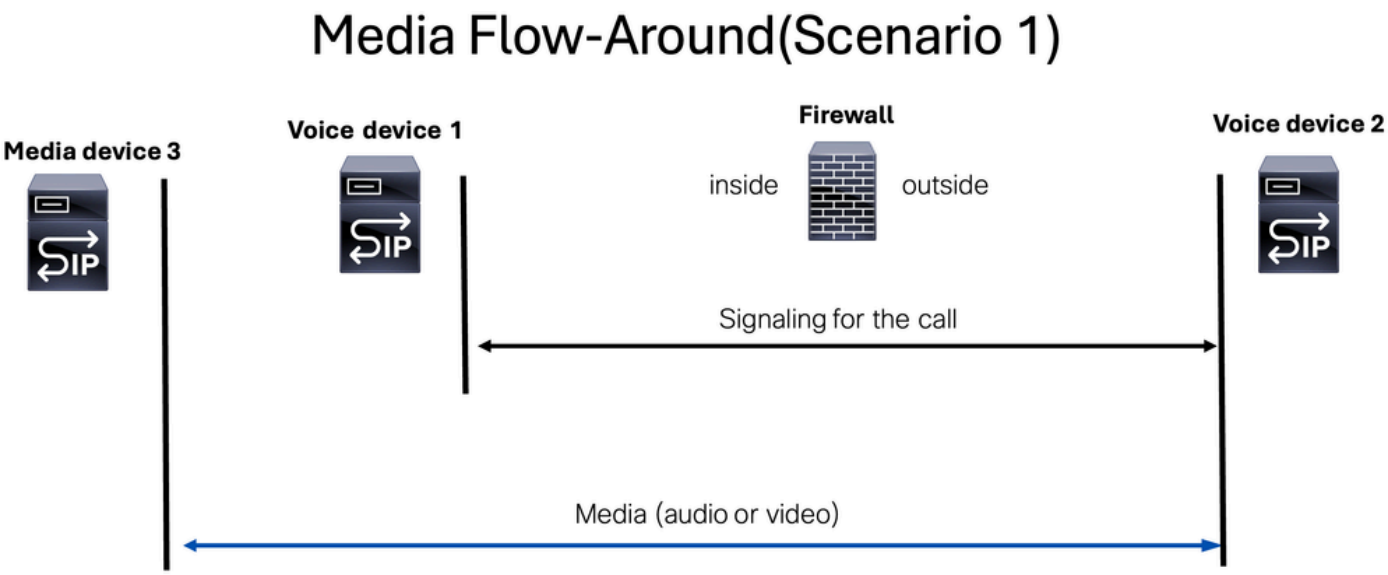
Durchfluss der Medien

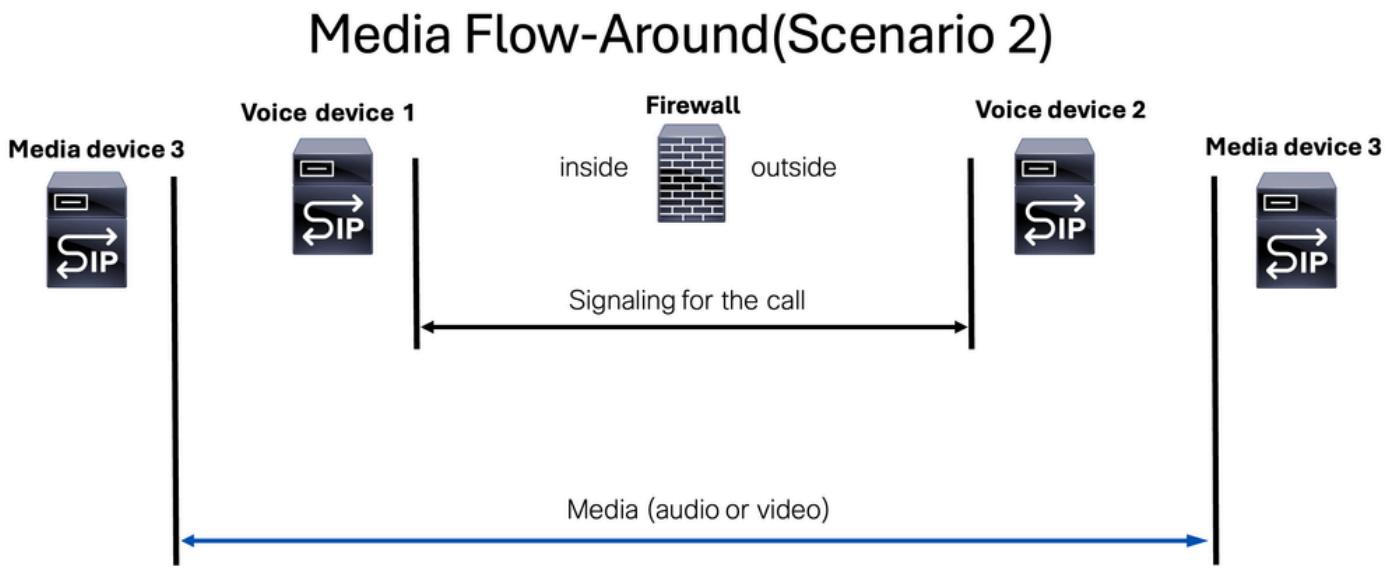
Media Flow-Through ist ein Modus, in dem sowohl Medien (Sprache und/oder Video) als auch Signalisierungspakete vom gleichen Gerät verarbeitet werden.



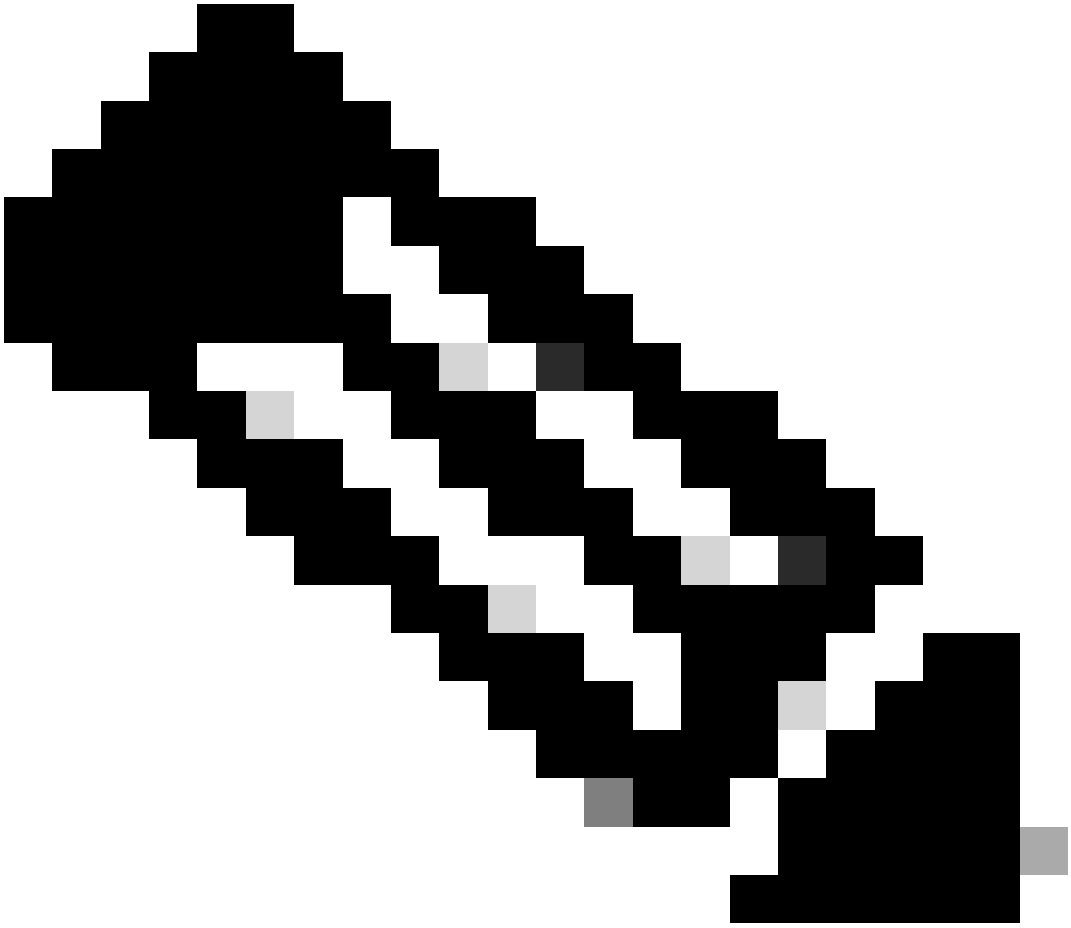
Umgehung von Medien

Der Media Stream Flow-around ist ein Modus, in dem Signalisierungspakete von zwei separaten Signalisierungskomponenten (Geräten oder Servern) verarbeitet werden, während der Media Stream (Sprache oder Video) von einem dritten Gerät, dem so genannten Mediengerät, verwaltet wird.





In diesem Modus werden die Rollen der beteiligten Geräte sowie die Unterscheidung zwischen Signalisierungs- und Medien-Streams bzw. -Geräten erläutert.



Anmerkung: Dies ist besonders wichtig zu erwähnen, wenn die Fehlerbehebung der Zugriffsliste erstellt könnte die Signalisierungskomponenten (Geräte oder Server), aber wenn der Medien-Stream ein anderes Mediengerät verwendet, müssen wir es erlauben, auch auf der Zugriffsliste unserer FW-Gerät.

Session Initiation Protocol (SIP)

SIP ist ein Steuerungsprotokoll auf Anwendungsebene, das von der Internet Engineering Task Force (IETF) in RFC 3261 definiert wurde.

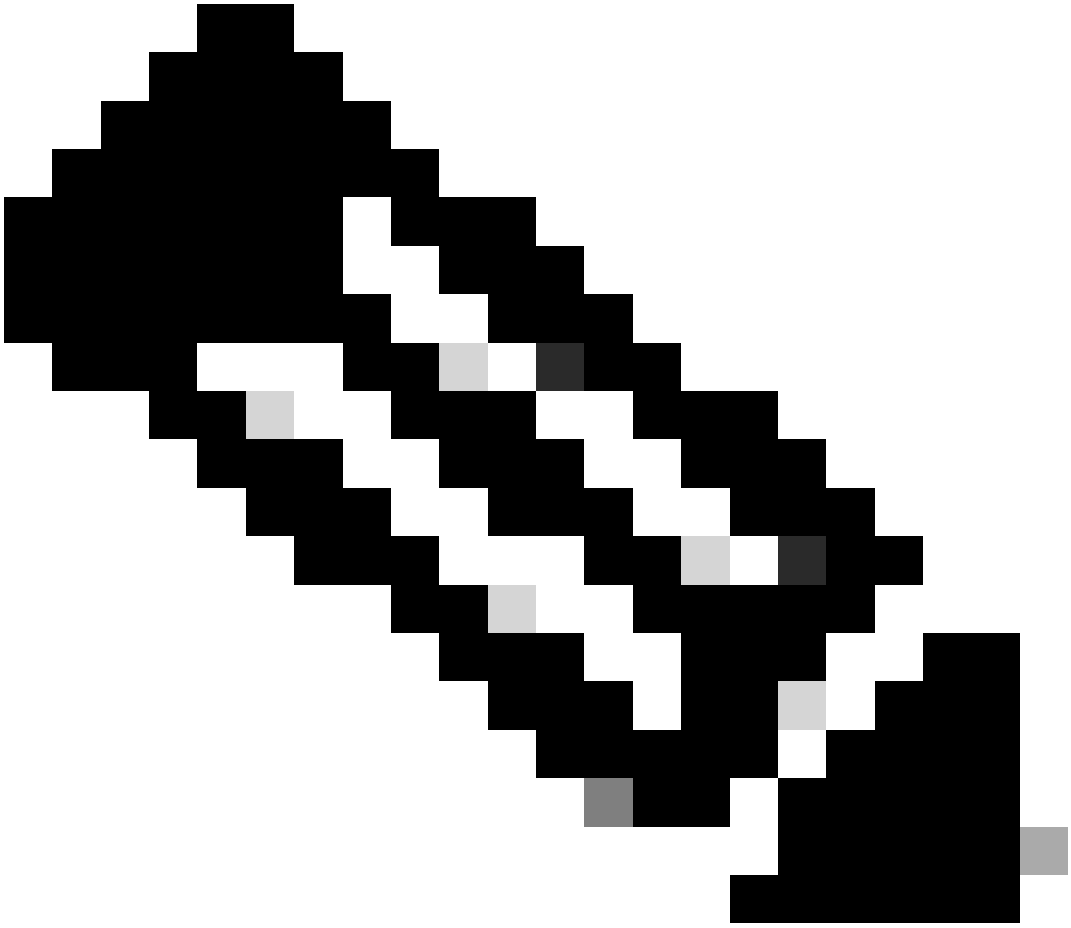
SIP ist ein textbasiertes Protokoll. Das bedeutet, dass SIP-Nachrichten ähnlich wie HTTP aus von Menschen lesbarem Text bestehen.

SIP wurde entwickelt, um die Funktionen der Signalisierung und des Sitzungsmanagements in einem Telefonienetzwerk zu erfüllen.

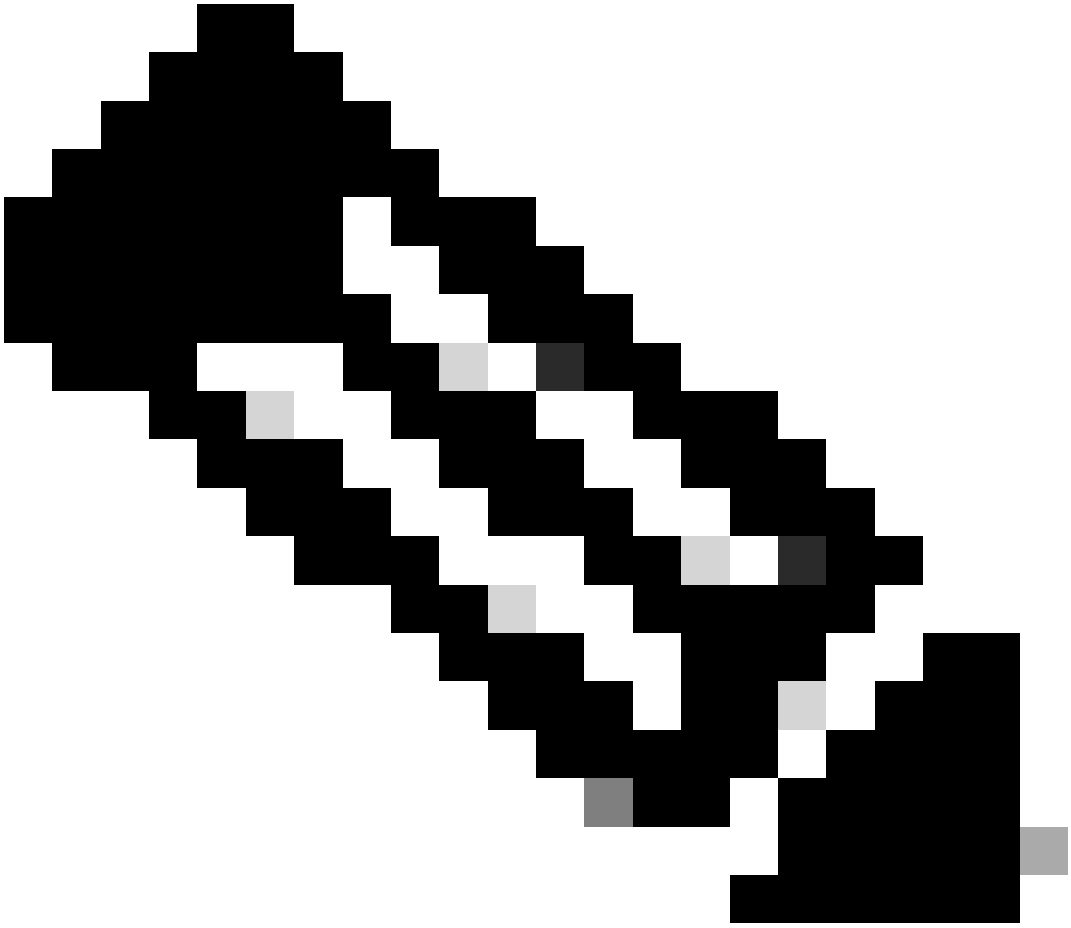
SIP kann:

- Anruf erstellen
- einen Anruf ändern
- Anruf beenden

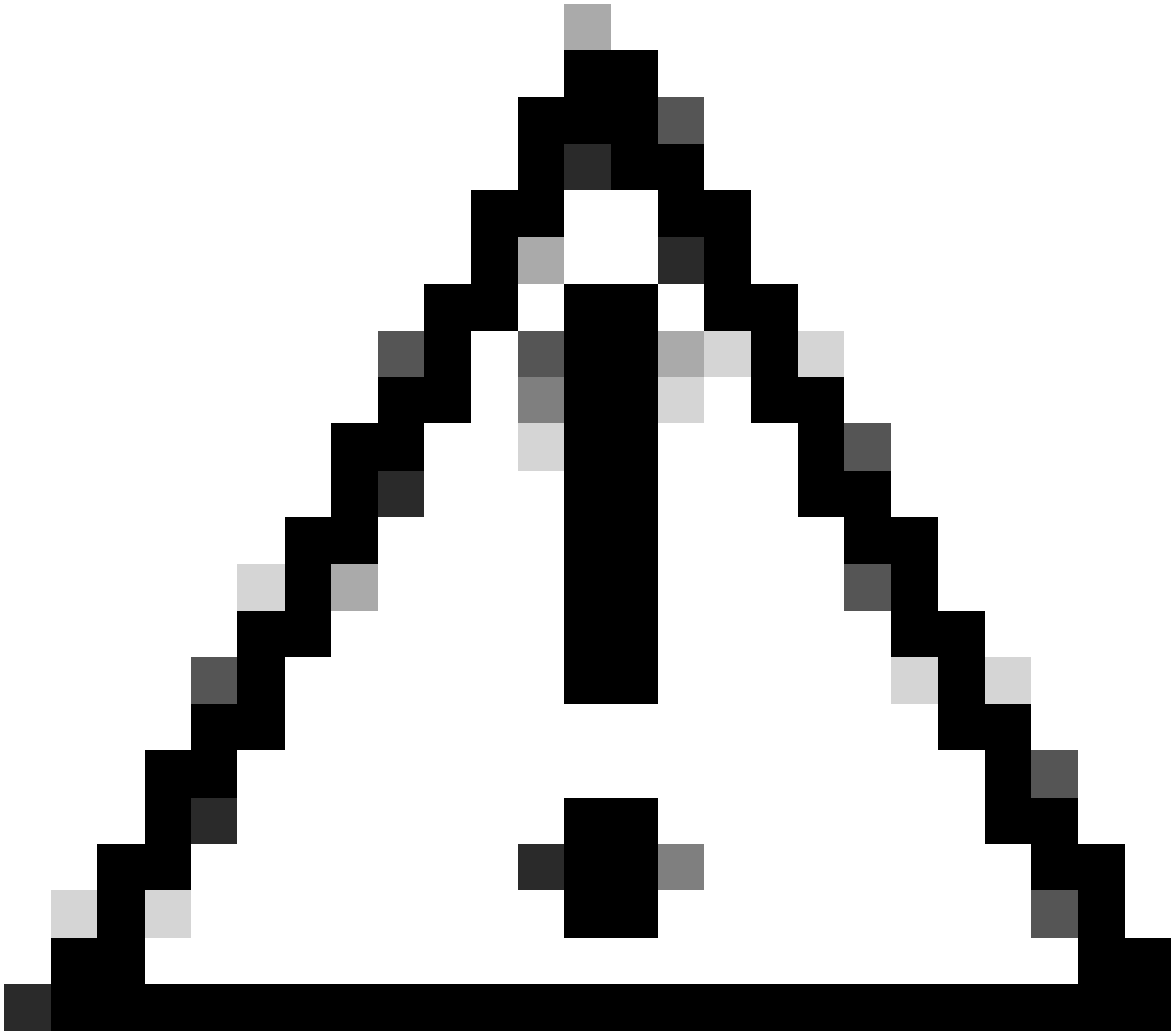
SIP kann entweder mit UDP oder TCP auf dem standardisierten Port 5060 verwendet werden. Wenn das SIP mit Transport Layer Security (TLS) verschlüsselt wird, kann der standardisierte Port 5061 verwendet werden.



Anmerkung: Wenn die SIP-Signalisierung verschlüsselt ist, sind die tatsächlichen SIP-Pakete bei der Paketerfassung auf ASA- oder FTD-Geräten nicht sichtbar. Sie können jedoch weiterhin den TCP-Handshake gefolgt vom TLS-Handshake zwischen den SIP-Clients und SIP-Servergeräten beobachten.



Anmerkung: Die SIP-Inspektion ist auf Cisco Secure Firewall Threat Defense (FTD) und Secure Firewall Adaptive Security Appliance (ASA) standardmäßig aktiviert.



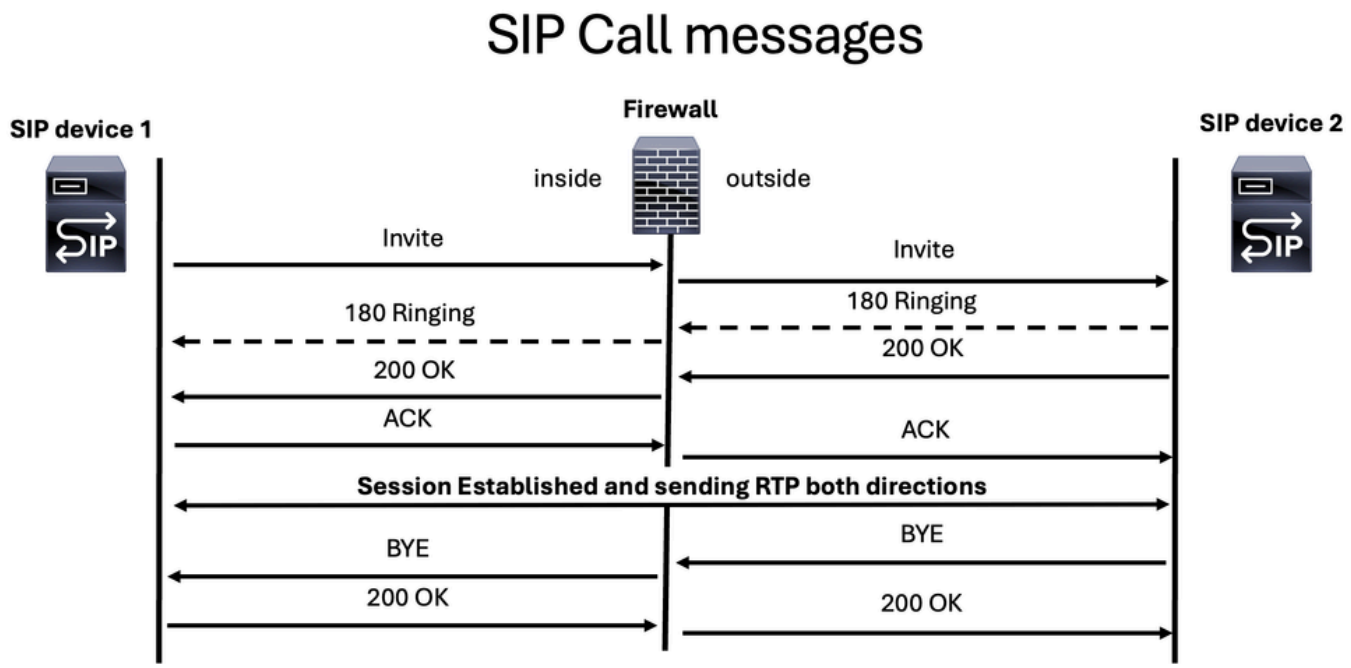
Vorsicht: Bestätigen Sie stets, welche Ports für die Signalisierung verwendet werden. Beachten Sie, dass das SIP-Protokoll in der Regel die Ports 5060 oder 5061 verwendet. In einigen Bereitstellungen können jedoch von diesen Standards abweichen und verschiedene Ports für das SIP-Protokoll verwendet werden.

Bei der Behebung eines SIP-Signalisierungsproblems gibt es drei Szenarien:

- SIP-Signalisierungsnachrichten
- SIP OPTION-Nachrichten
- SIP REGISTER-Nachrichten

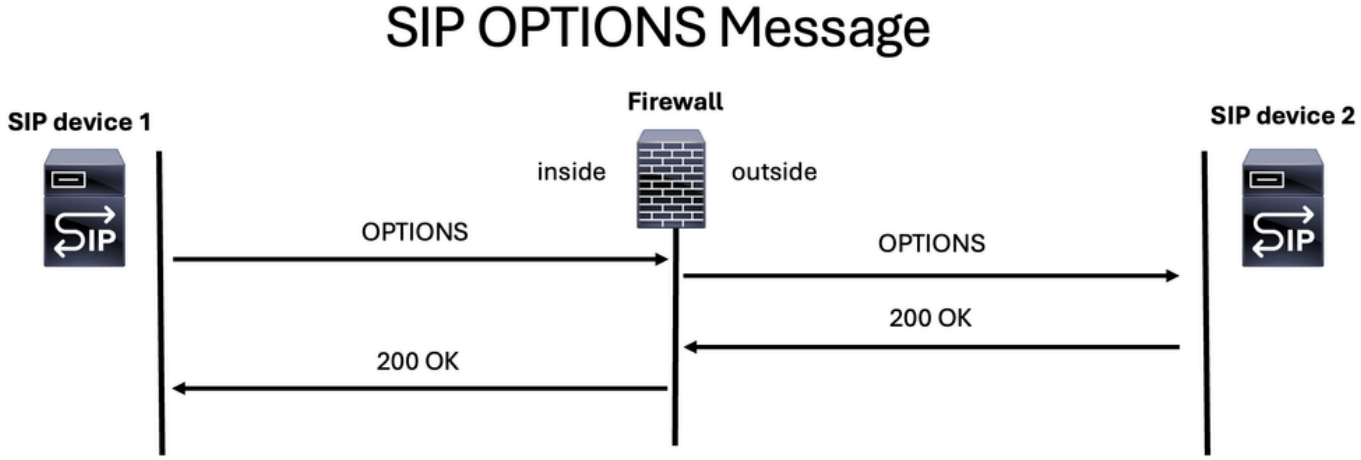
SIP-Anrufnachrichten

Die wichtigsten SIP-Nachrichten zum Einrichten und Beenden eines Sprachanrufs sind:



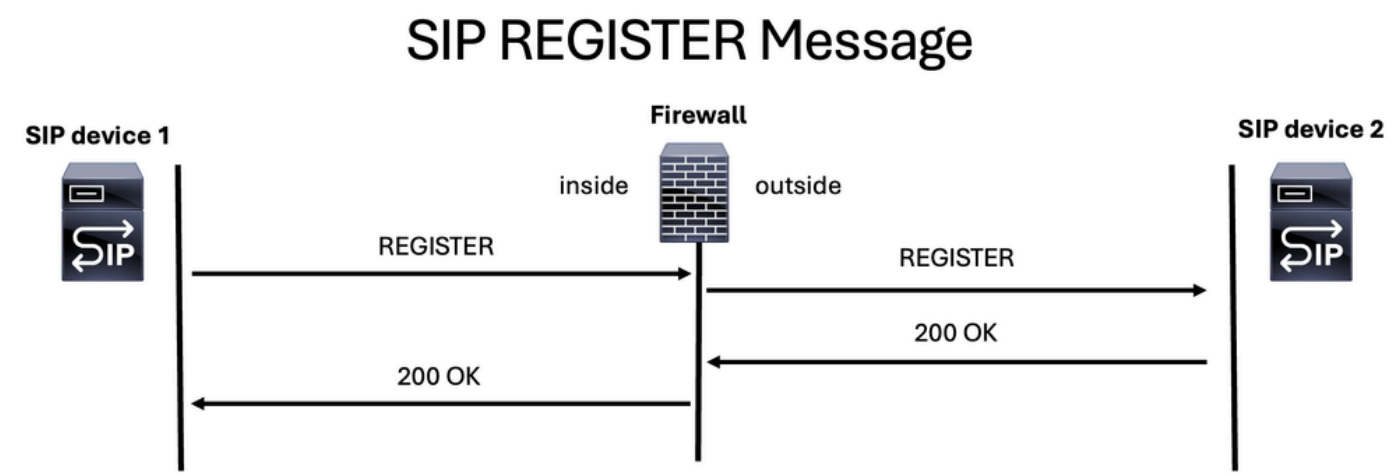
Nachrichten zu SIP-OPTION

SIP OPTIONS-Meldungen sind wichtig, um zu bestimmen, ob ein SIP-Gerät online ist und antworten kann. Es ist wie Ping-ICMP-Nachricht, aber auf SIP Welt.

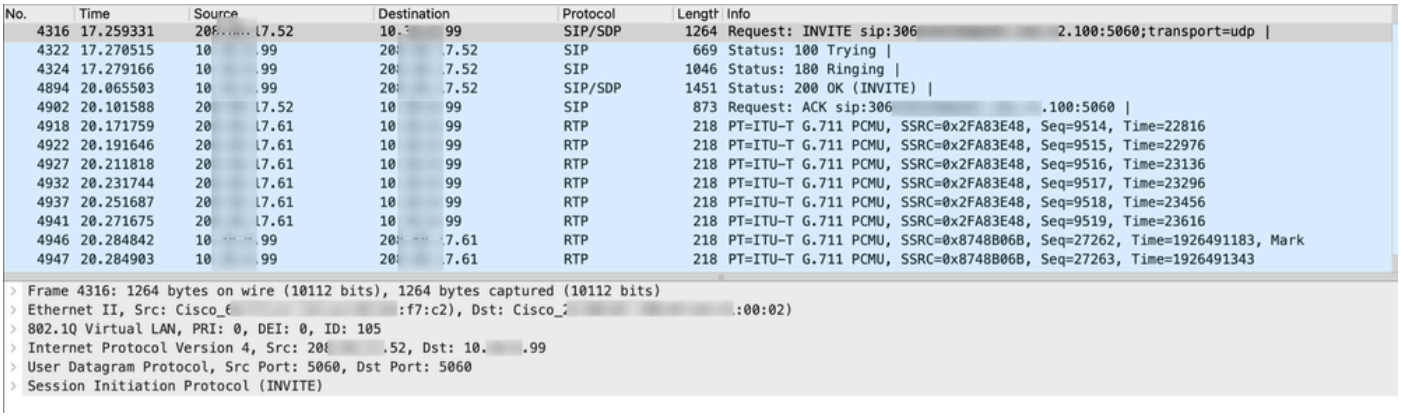


SIP REGISTER-Nachricht

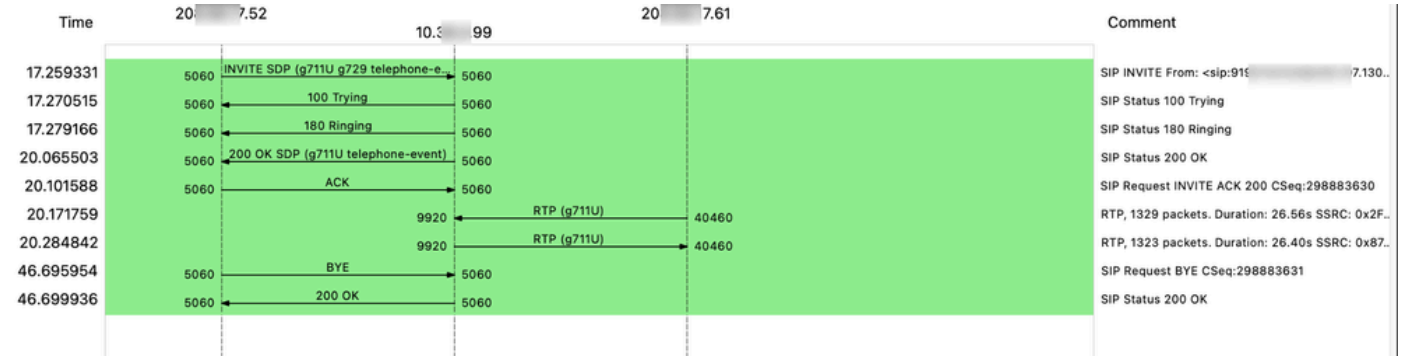
Eine weitere SIP-Nachricht, die Sie während einer Sitzung zur Behebung von Firewall-Problemen finden können, ist die SIP-REGISTER-Nachricht, mit der sich ein Gerät bei einem SIP-Server registrieren kann.



Diese Paketerfassung zeigt Anforderungen und Antworten von zwei SIP-Geräten sowie den Medien- (Sprach-) Datenverkehr:

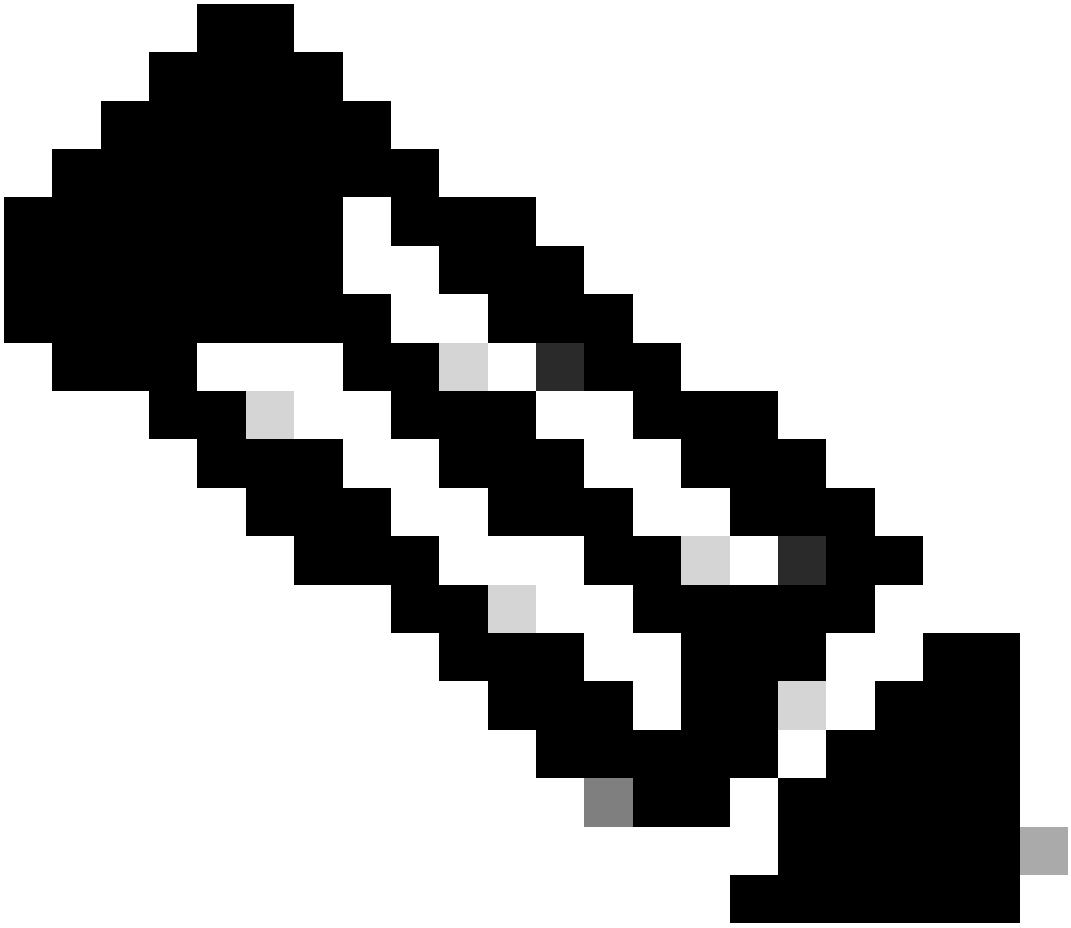


Dies ist ein Beispiel für den Fluss von SIP-Signalisierung und RTP-Medien (Sprache):



Session Description Protocol (SDP)

Session Description Protocol (SDP) ist eine Standarddarstellung zur Beschreibung von Medien-Streams für Multimedia-Sitzungen. Er überträgt keine Medien selbst, sondern wird verwendet, um Medientyp und -format zwischen Endpunkten auszuhandeln. SDP wird in Verbindung mit dem Session Initiation Protocol (SIP) verwendet, um die Medieneigenschaften einer Sitzung zu verwalten und auszuhandeln.

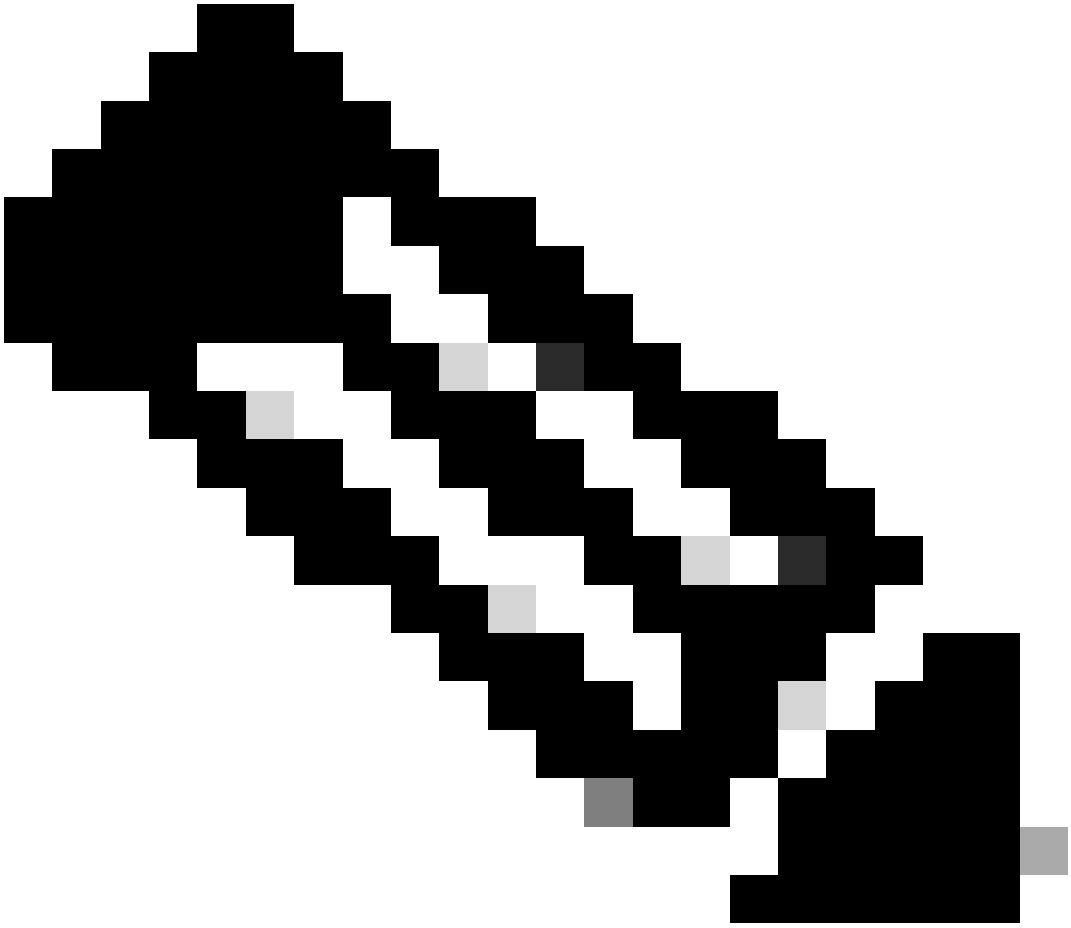


Anmerkung: MGCP beinhaltet das Konzept von SDP, das für denselben Zweck verwendet wird.

Dies ist ein Beispiel für eine SDP-Nachricht in einem SIP-Protokoll:

```
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
```



Anmerkung: Einige der SDP-Nachrichten enthalten die folgenden Parameter im Beispiel:

++c-IN IP4: IP-Adresse des Medienservers

++m=Audio: Dies zeigt an, dass es sich bei dem Medientyp um Audio handelt.

8266 ++: Dies ist die Portnummer, an die der Audio-Stream gesendet wird.

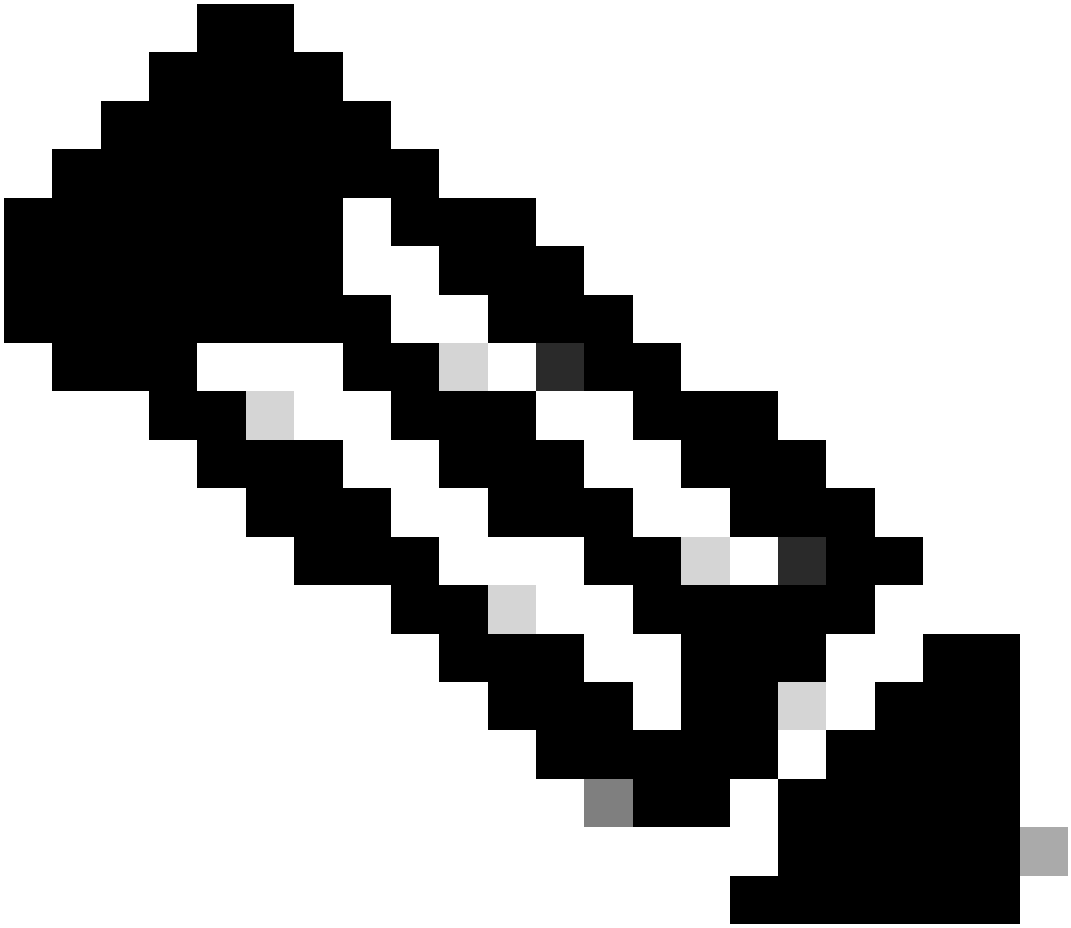
++RTP/AVP: Diese Eigenschaft gibt das Transportprotokoll an, das RTP unter Verwendung des Audio/Video Profile (AVP) ist.

18.127 ++: Dies sind die Payload-Typen für die Audio-Codecs. Der Payload-Typ 18 entspricht normalerweise dem G.729-Codec, und "127" ist ein dynamischer Payload-Typ, der einem Codec gemäß der Aushandlung zwischen den Endpunkten zugewiesen werden kann.

Das Session Description Protocol (SDP) ist in verschiedenen SIP-Nachrichten zu finden, z. B.: INVITE, 183 Session in Progress, 200 OK, ACK usw. SDP dient als Antwortmethode für den

Austausch von Sprach- und/oder Videofunktionen zwischen den Parteien. Bei der Behebung von Anruffehlern ist es wichtig, drei Hauptkonzepte zu verstehen:

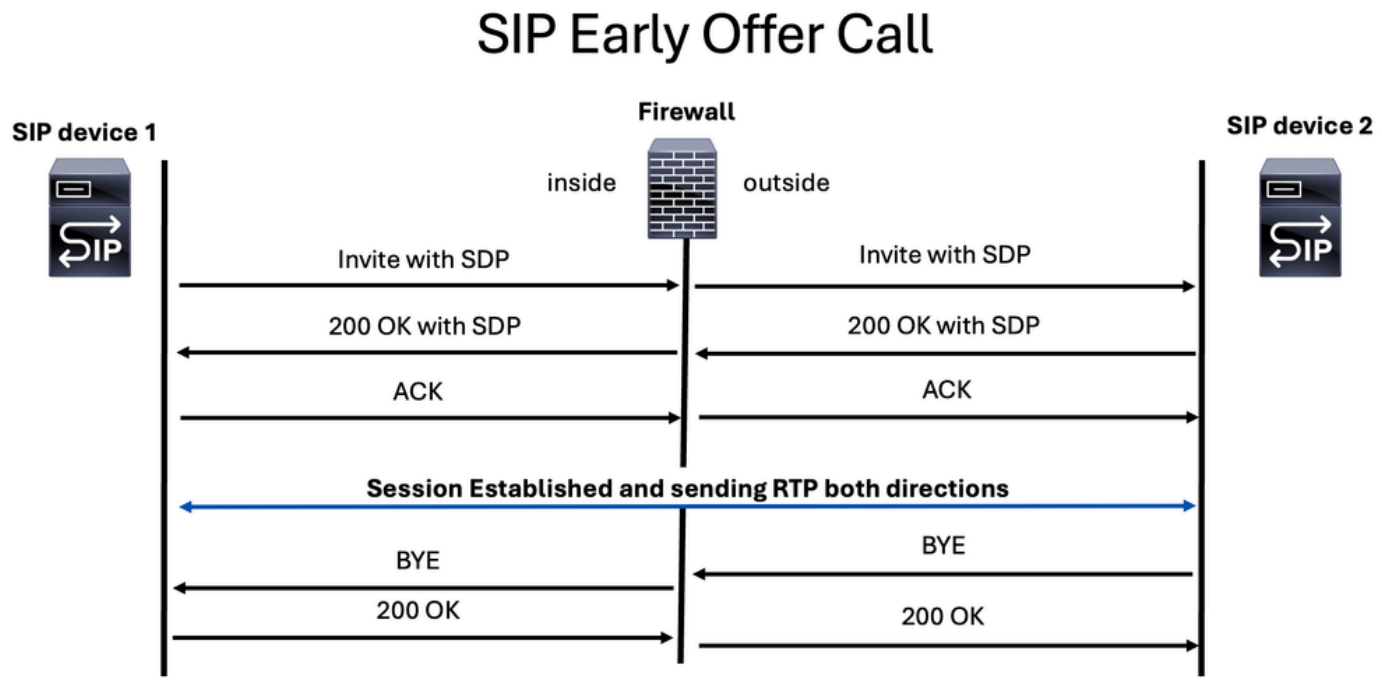
1. Frühzeitige Angebote
2. Angebot verzögern
3. Early Media



> Anmerkung: Es ist wichtig, das Ziel von SDP-Nachrichten zu kennen, da die Überprüfungsfunktion der Firewall IP-Adressen nicht nur innerhalb von SIP-Headern, sondern auch im SDP-Abschnitt ändern kann.

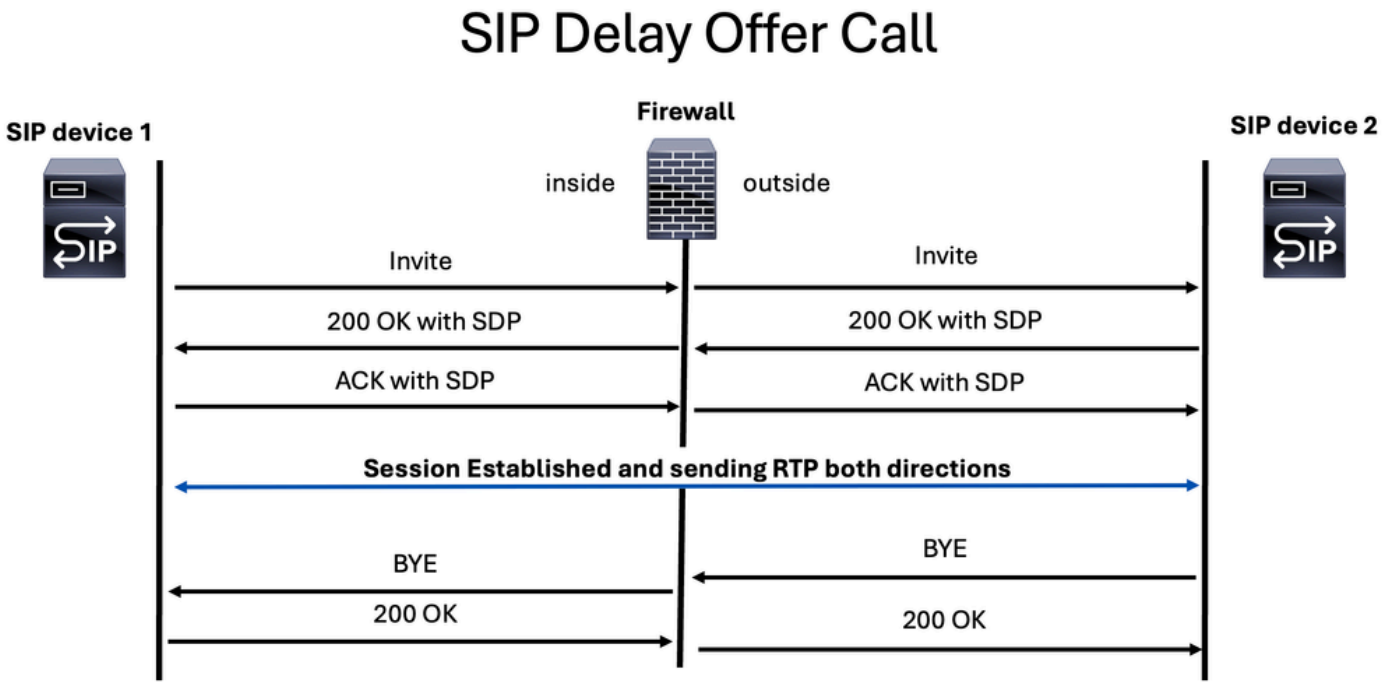
Frühzeitige Angebote

Hier finden Sie Medienparameter zu SDP in den INVITE- und 200 OK SIP-Nachrichten.



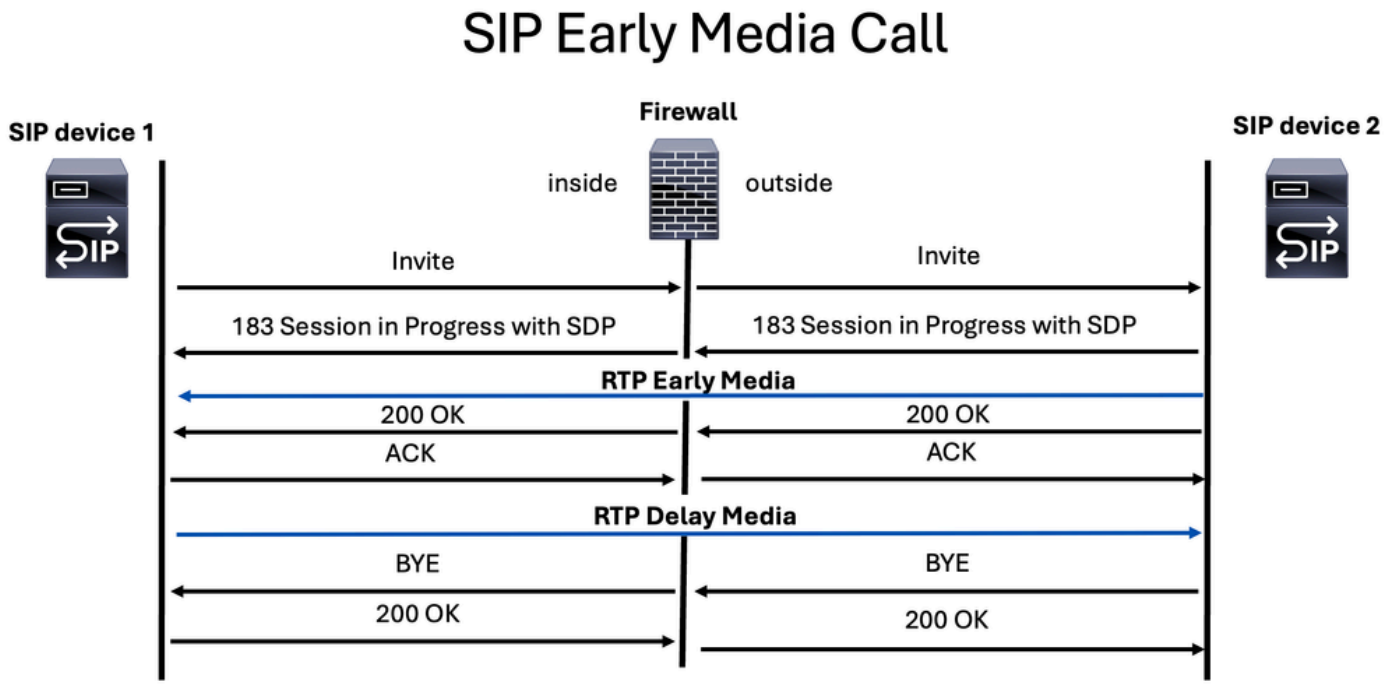
Angebot verzögern

Bei dieser Methode wird das SDP in 200 OK- und ACK SIP-Nachrichten gefunden.



Early Media

Early Media wird über eine spezielle SIP-Nachricht übertragen, die als "183 Session Progress Response" (SIP-Antwort) bezeichnet wird. Diese Nachricht enthält das Session Description Protocol (SDP) mit Medienparametern für den angerufenen Teilnehmer. In der Regel senden Netzbetreiber und SIP-Anbieter dem Anrufer automatisierte Sprachnachrichten oder andere Medien, bevor der Anruf offiziell verbunden wird.

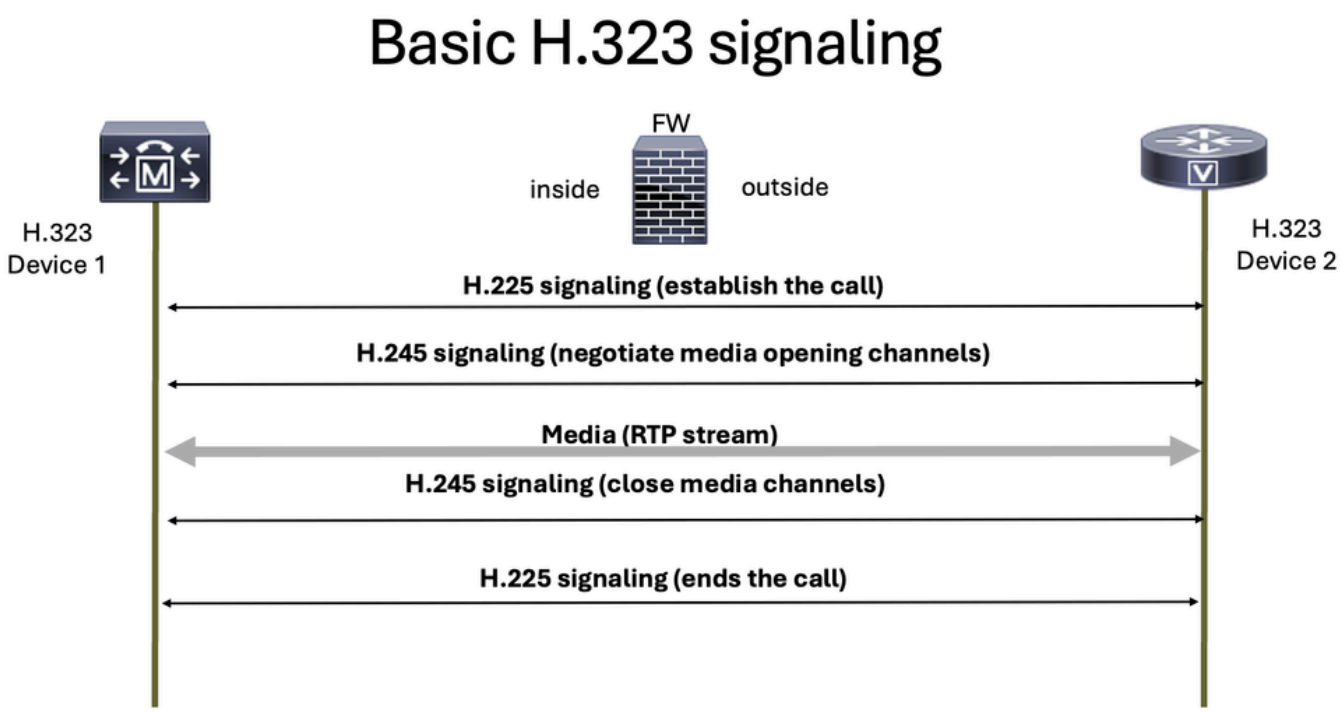


H,323

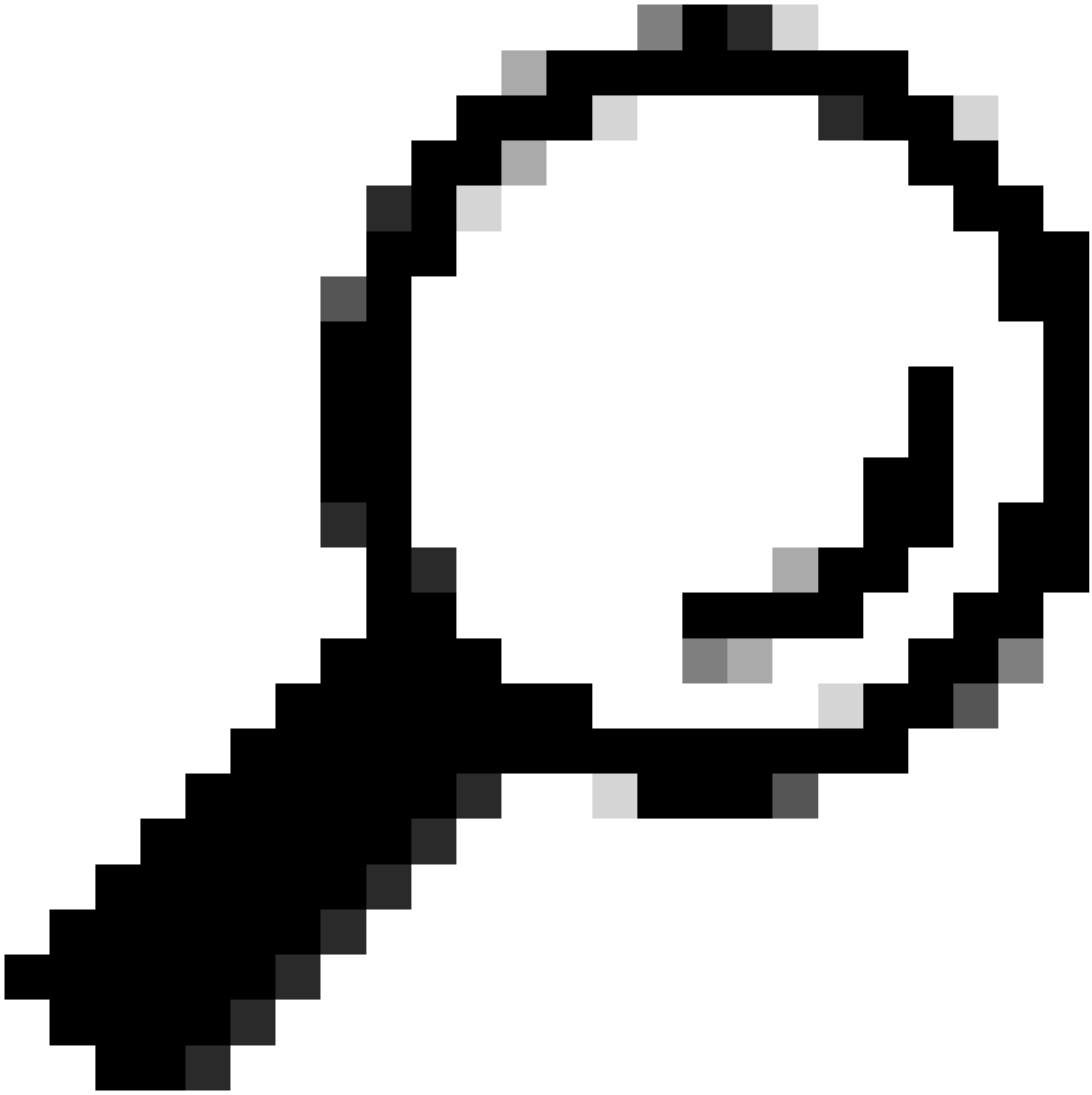
H.323 ist eine Reihe von Protokollen, die von der Internationalen Fernmeldeunion (ITU) für die Sprach-, Video- und Datenkommunikation über paketvermittelte Netzwerke wie das Internet definiert werden.

Das H.323-Protokoll besteht aus zwei Hauptkomponenten:

1. H.225: Diese Funktion verarbeitet die Anrufsignalisierung, einschließlich der Einrichtung und Beendigung von Anrufen.
2. H.245: Diese ist für den Austausch von Funktionen sowie das Öffnen und Schließen von Audio- und Videokanälen zuständig.



Die vom H.323-Signalisierungsprotokoll verwendeten Ports sind 1718, 1719 und 1720.

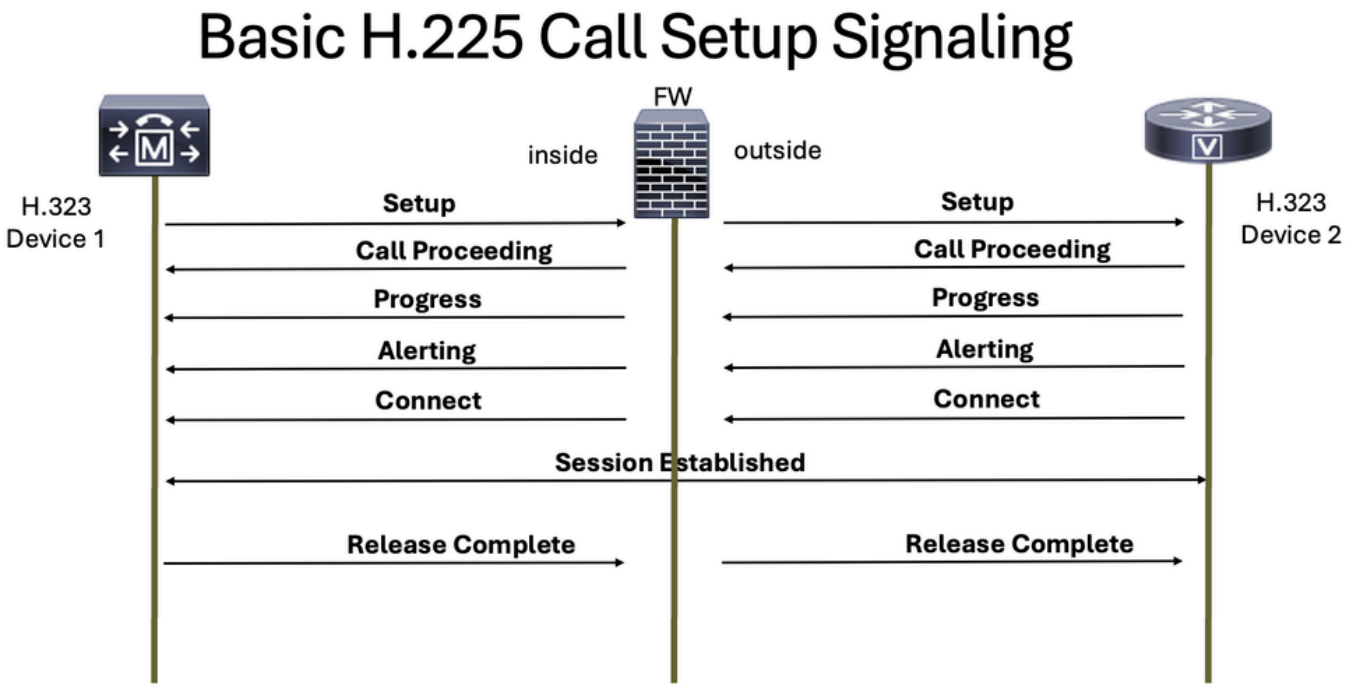


Tipp: Bei der Kommunikation über ein sicheres H.323-Protokoll können beim Wechsel von UDP zu TCP Probleme auftreten, da TLS für die Verschlüsselung verwendet wird. Dies kann dazu führen, dass eine Firewall die Verbindung fälschlicherweise als verdächtige Aktivität blockiert. Daher ist es wichtig, die Firewall so zu konfigurieren, dass sowohl UDP- als auch TCP-Datenverkehr für H.323-Endpunkte oder -Server zugelassen wird.

H.323 ist ein Protokoll mit zwei Betriebsmodi: Langsamer Start und schneller Start.

H,225

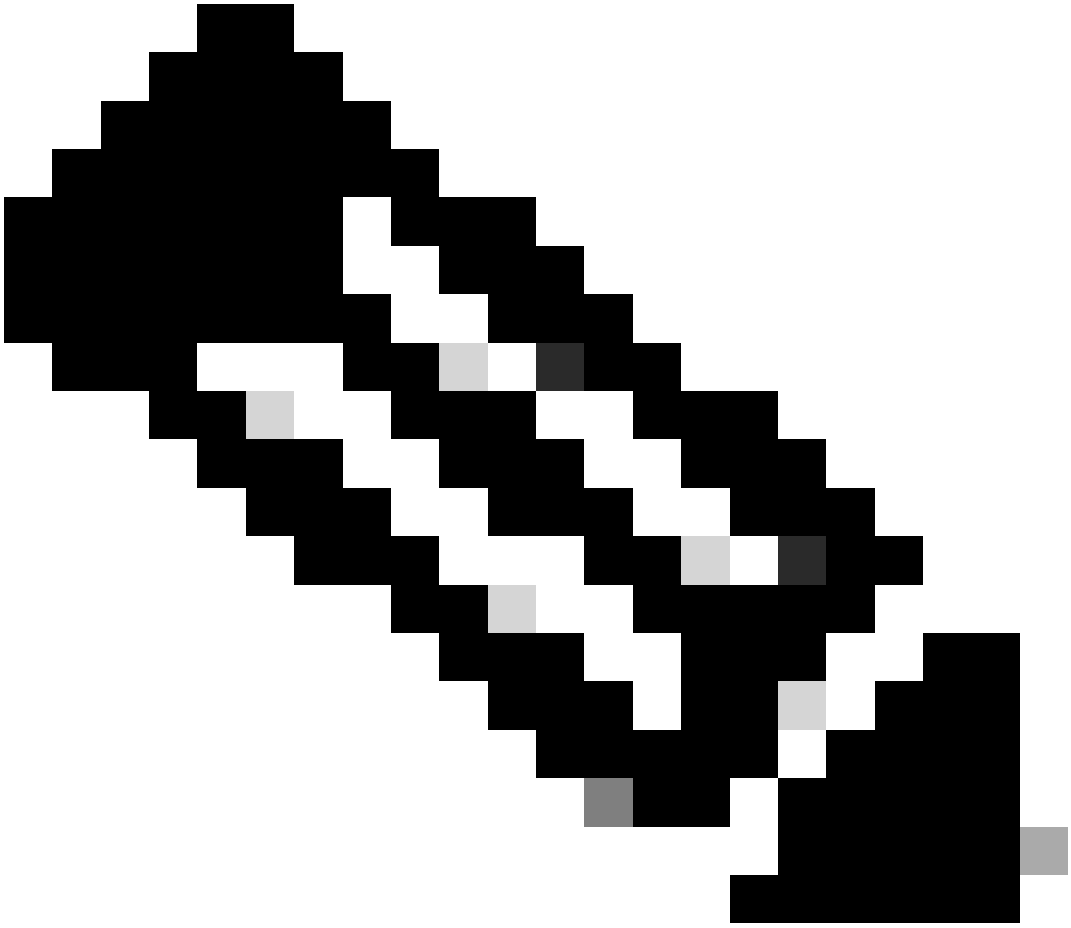
Dieses Protokoll ist für die Einrichtung des Anrufs und das Beenden eines Sprachanrufs zuständig, wenn einer der Teilnehmer auflegt.



H,245

H.245 bietet folgende Funktionen:

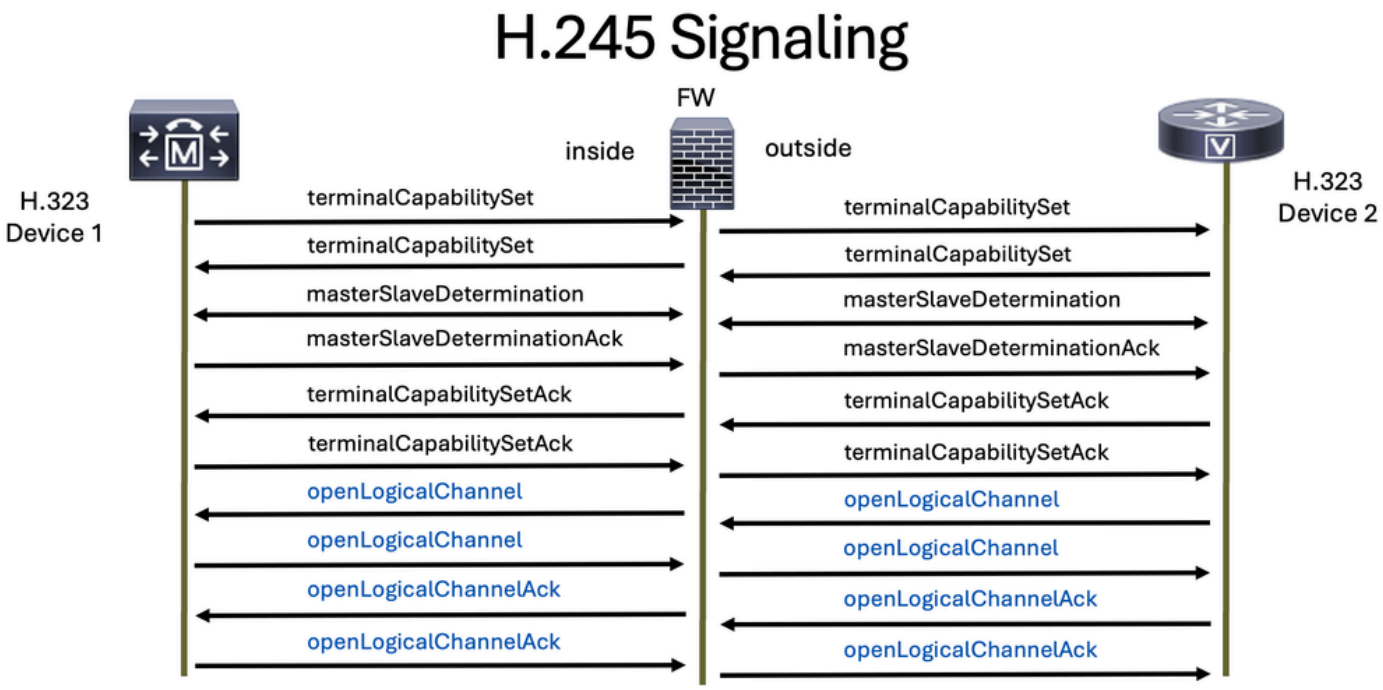
- Austausch von Terminalfunktionen
- Master-/Slave-Festlegungen
- Signalisierung logischer Kanäle



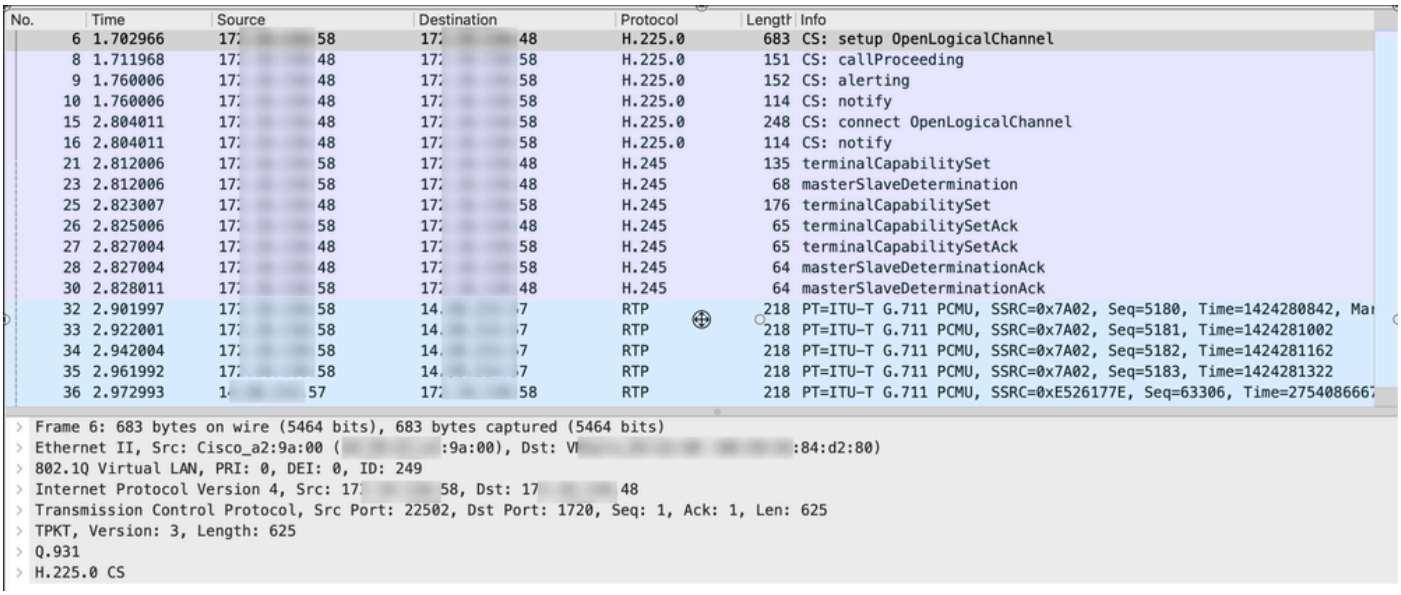
> Anmerkung: Die in diesem Dokument verwendeten Begriffe "Master" und "Slave" sind im ursprünglichen H.323-Protokoll fest codiert und spiegeln nicht die Richtlinien oder Werte unseres Unternehmens wider. Wir engagieren uns für die Förderung einer inklusiven und respektvollen Sprache.

Das H.245-Protokoll wird nach dem Empfang der H.225-Connect-Nachricht gesendet.

Dieses Protokoll hilft bei der Bestimmung, welches Sprachprotokoll für RTP verwendet wird, und wird auf dem öffnenden logischen Kanal und schließenden logischen Kanalnachrichten für diesen angegeben.



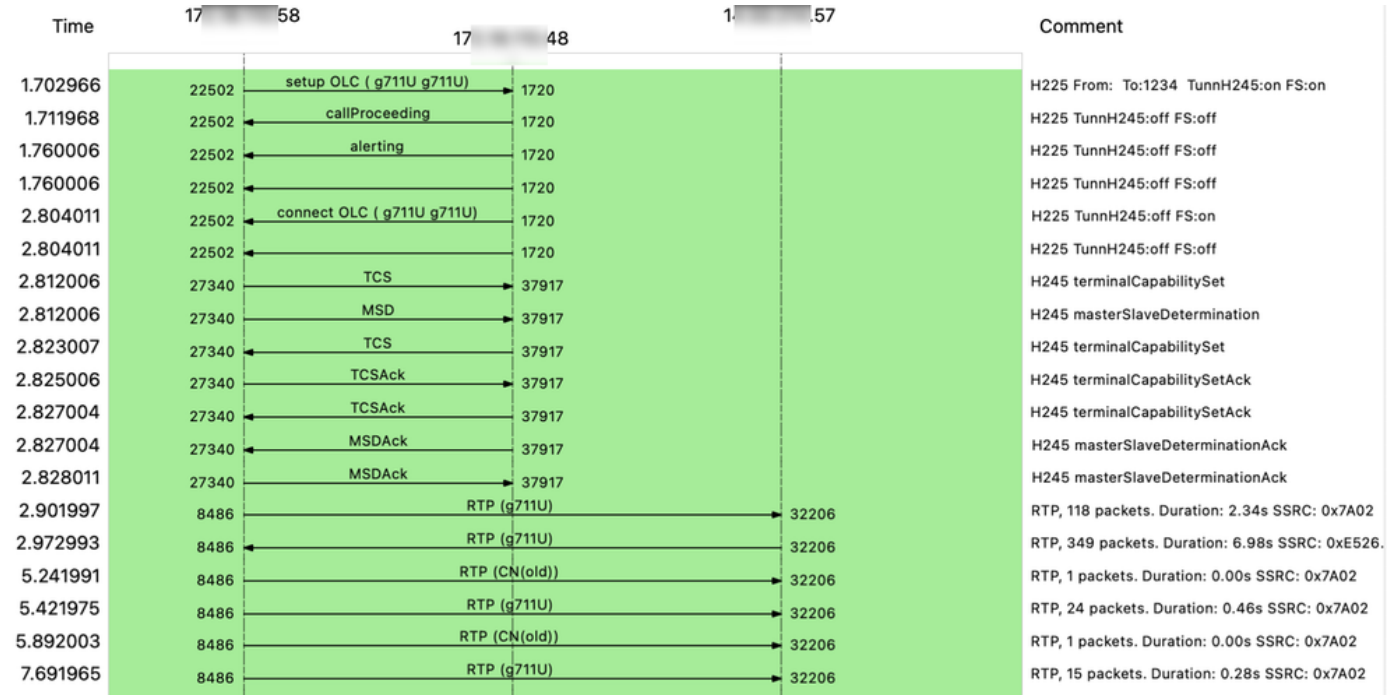
Diese Paketerfassung zeigt Anforderungen und Antworten von zwei H.323-Geräten mit H.225 und H.245 sowie den Medien-(Sprach-)Datenverkehr:

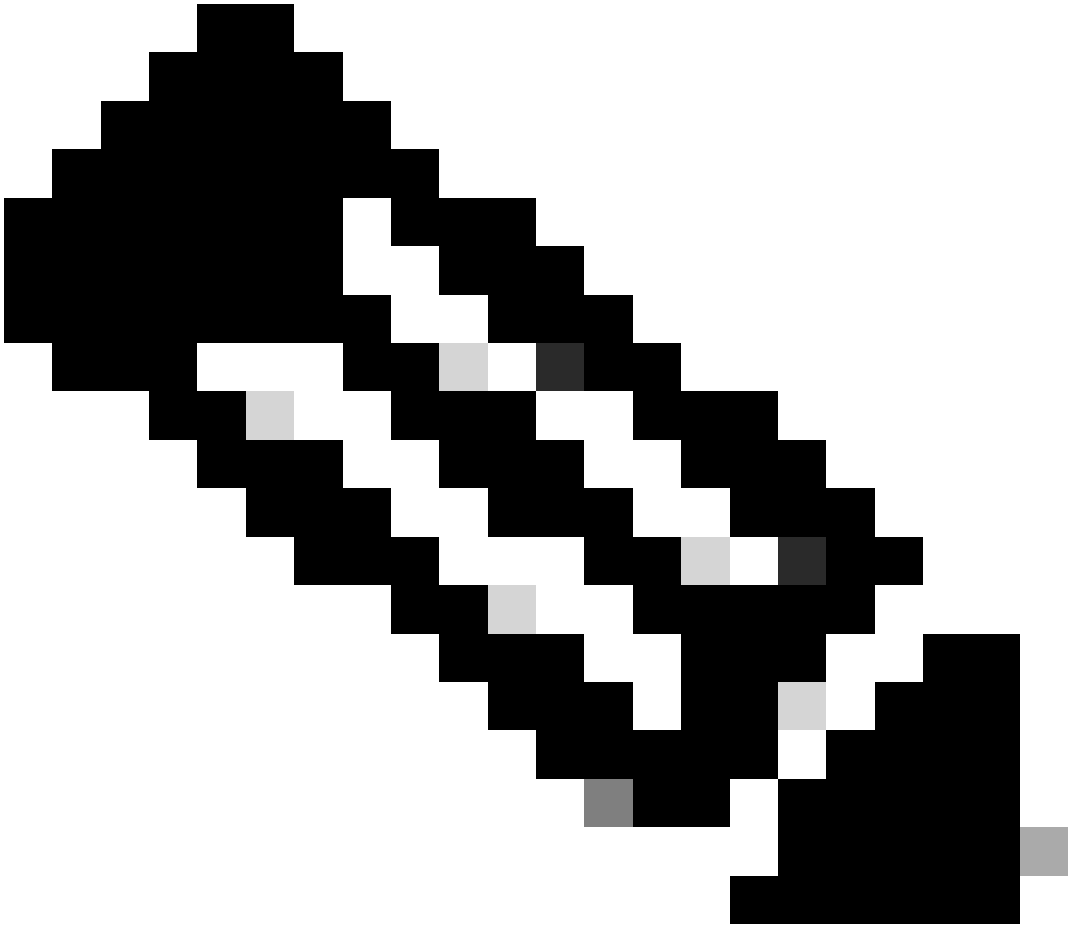


No.	Time	Source	Destination	Protocol	Length	Info
6	1.702966	17 58	17 48	H.225.0	683	CS: setup OpenLogicalChannel
8	1.711968	17 48	17 58	H.225.0	151	CS: callProceeding
9	1.760006	17 48	17 58	H.225.0	152	CS: alerting
10	1.760006	17 48	17 58	H.225.0	114	CS: notify
15	2.804011	17 48	17 58	H.225.0	248	CS: 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
```

Dies ist ein Beispiel für einen Fluss der H.323-Signalisierung mit H.225- und H.245- sowie RTP-Medien (Sprache):

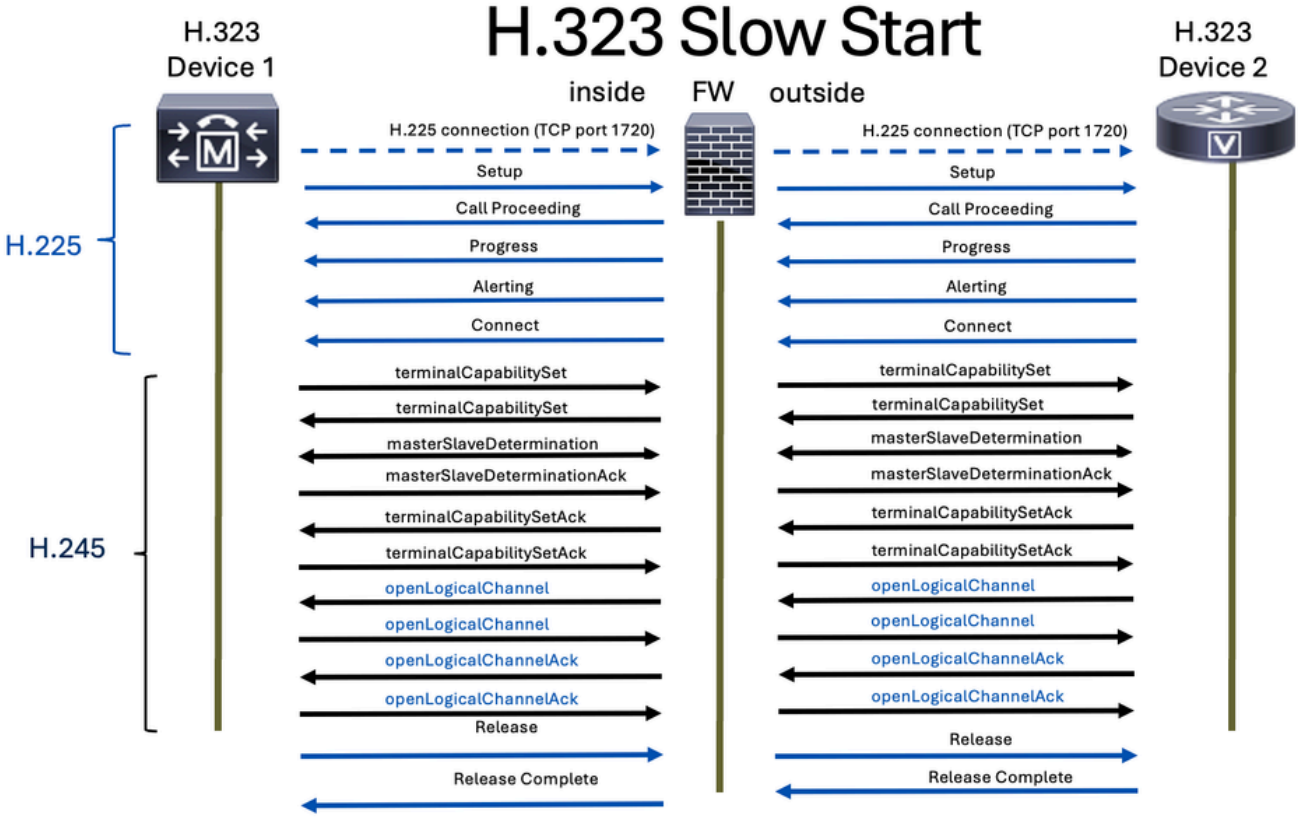

Time
Comment
1.702966 22502 setup OLC (g711U g711U) 1720 H225 From: To:1234 TunnH245:on FS:on
1.711968 22502 callProceeding 1720 H225 TunnH245:off FS:off
1.760006 22502 alerting 1720 H225 TunnH245:off FS:off
1.760006 22502 1720 H225 TunnH245:off FS:off
2.804011 22502 connect OLC (g711U g711U) 1720 H225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



Anmerkung: Die H.323-Inspektion ist auf Cisco Secure Firewall Threat Defense (FTD) und Secure Firewall Adaptive Security Appliance (ASA) standardmäßig aktiviert.

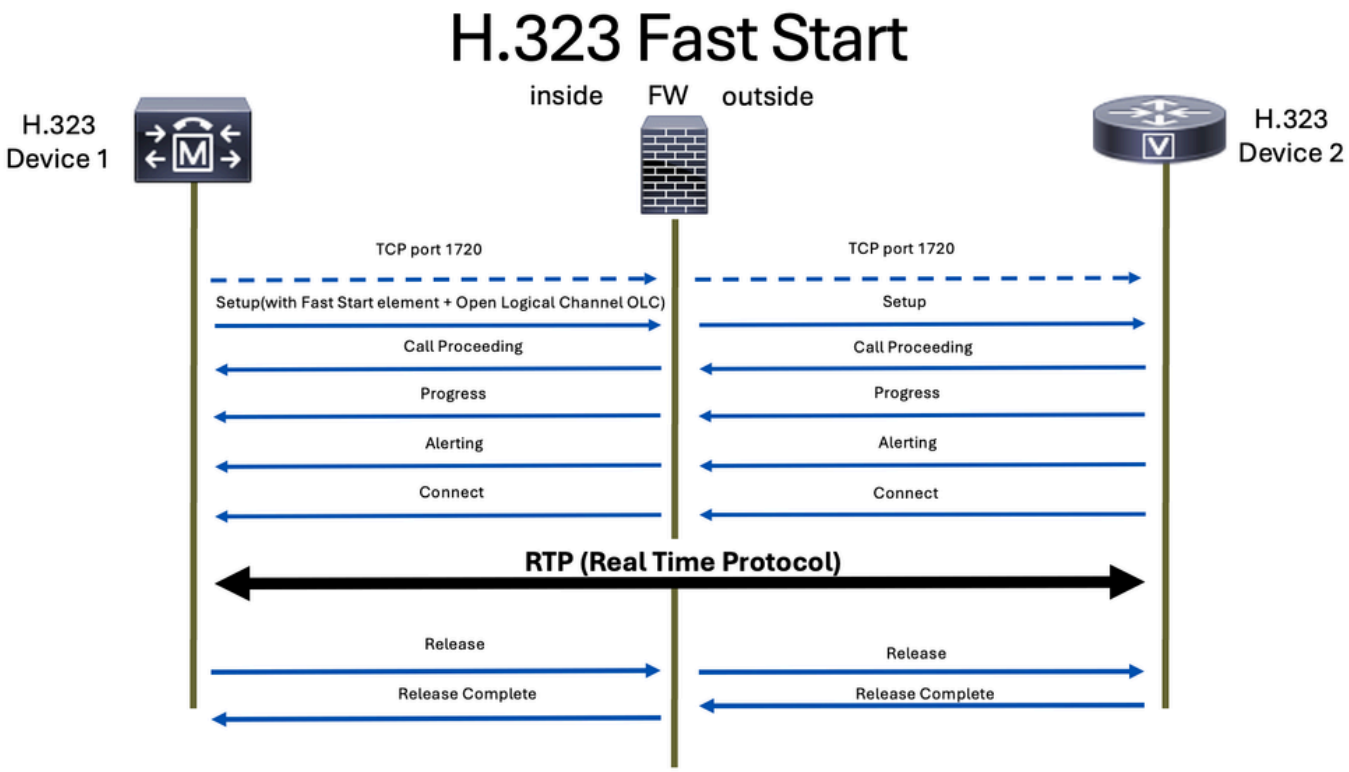
Langsamer Start

Im Slow-Start-Modus umfasst der Verbindungsaufbau mehrere Signalisierungsschritte, bevor Medienkanäle aufgebaut werden. Die Schritte umfassen Einrichtung, Anrufweiterleitung, Warnmeldungen und Verbinden. Nach diesen Schritten wird die H.245-Medienaushandlung separat durchgeführt. Dies bedeutet, dass die Medienkanäle erst nach Abschluss der Anrufsignalisierung aufgebaut werden, was zu einer längeren Einrichtzeit führen kann.



Schnellstart

Im Gegensatz dazu ermöglicht der Schnellstartmodus die Medienaushandlung innerhalb der anfänglichen Setup-Meldung. Dadurch können die Medienkanäle schneller eingerichtet werden, da die Verhandlung im Rahmen der Ersteinrichtung des Anrufs stattfindet. Fast Start rationalisiert den Prozess, indem die Anzahl der ausgetauschten Nachrichten und der Verarbeitungsaufwand reduziert werden, bevor die Medienkanäle eingerichtet werden.

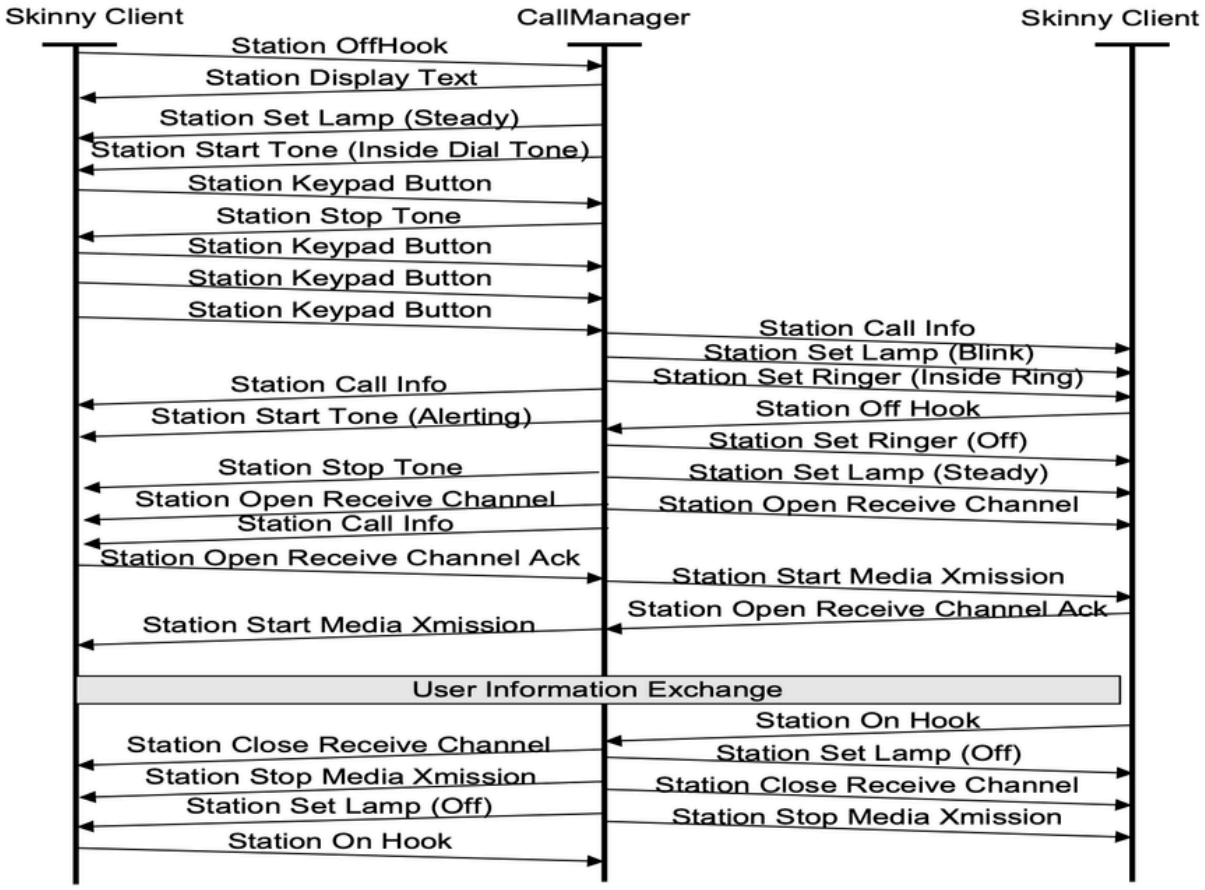


SCCP

Das Skinny Client Control Protocol (SCCP), das häufig einfach als Skinny bezeichnet wird, ist ein proprietäres Signalisierungsprotokoll von Cisco. Es wird hauptsächlich von Cisco Unified Communications Manager (CUCM)-, Cisco Unified Communications Manager Express (CME)-Routern und Cisco IP-Telefonen verwendet, um die Einrichtung und Steuerung von Anrufen zu vereinfachen.

Das SCCP-Protokoll verwendet TCP auf Port 2000 für nicht sicheres SCCP und Port 2443 für sicheres SCCP.

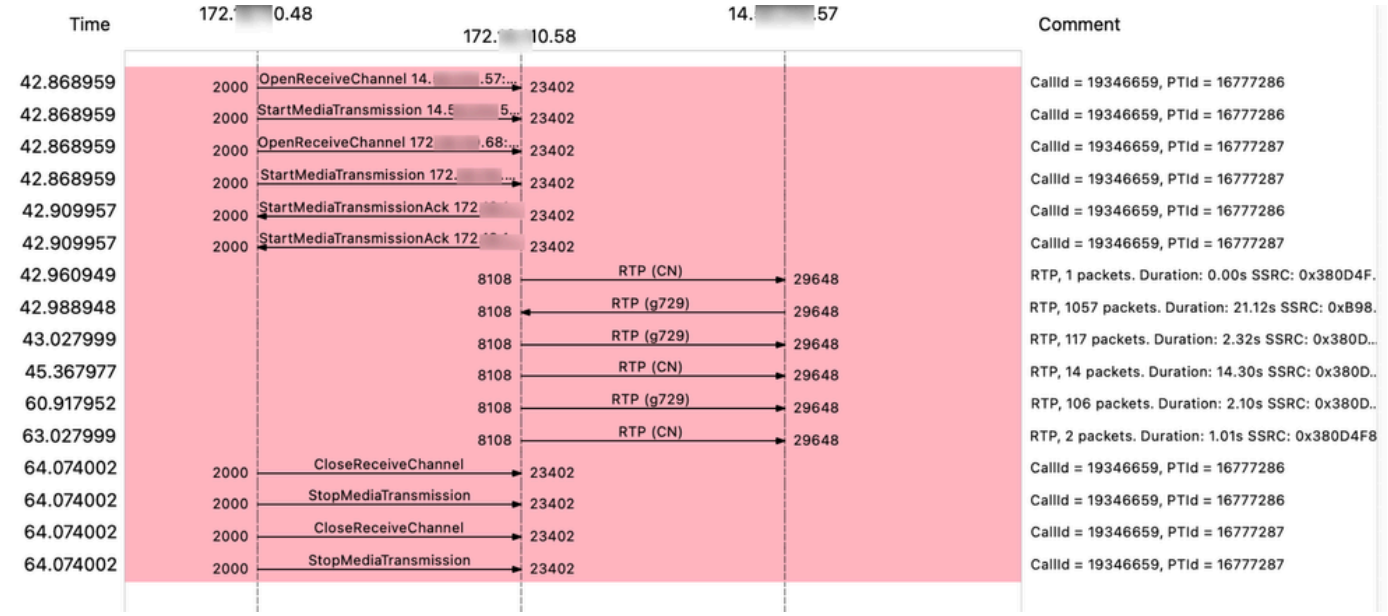
Folgende SCCP-Nachrichten sind bei SCCP-Anrufen häufig zu finden:

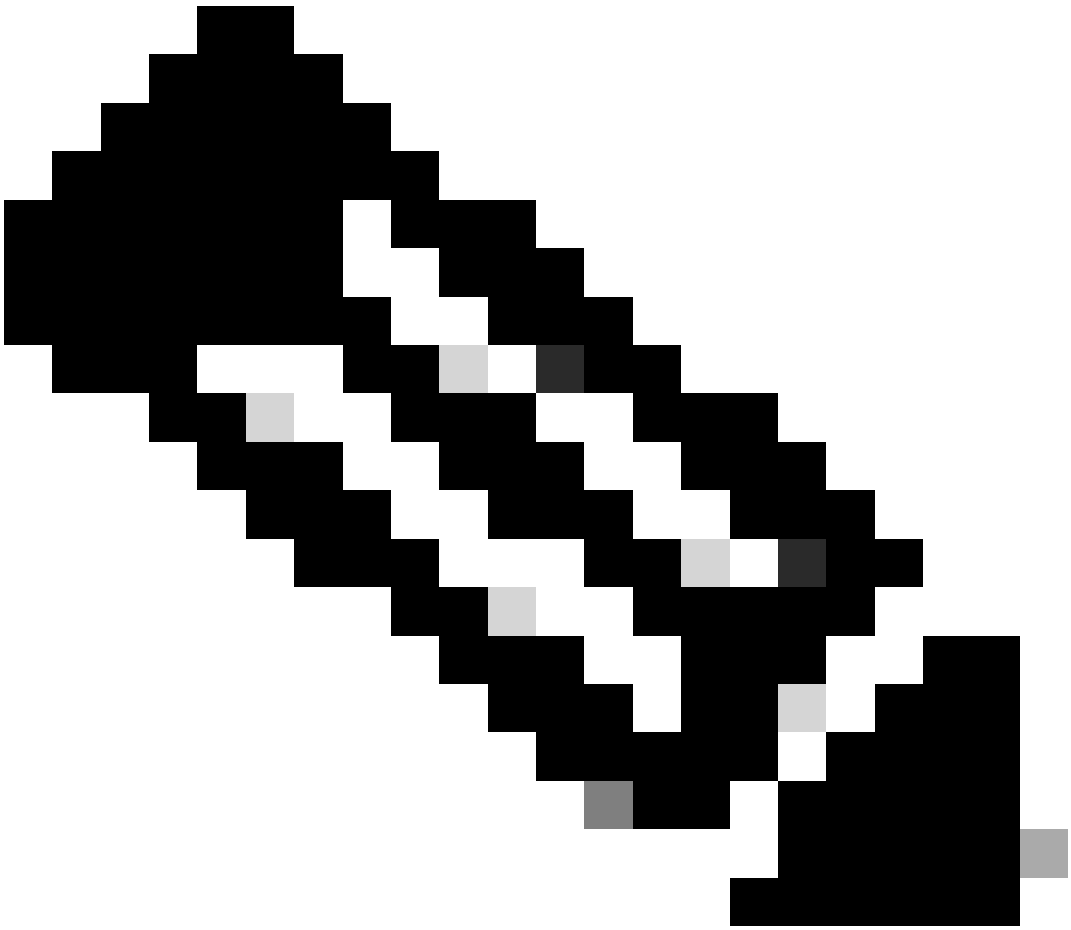


Diese Paketerfassung zeigt Anforderungen und Antworten von zwei SCCP-Geräten sowie den Medien- (Sprach-) Datenverkehr:

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

Dies ist ein Beispiel für einen Fluss der SCCP-Signalisierung und der RTP-Medien (Sprache):





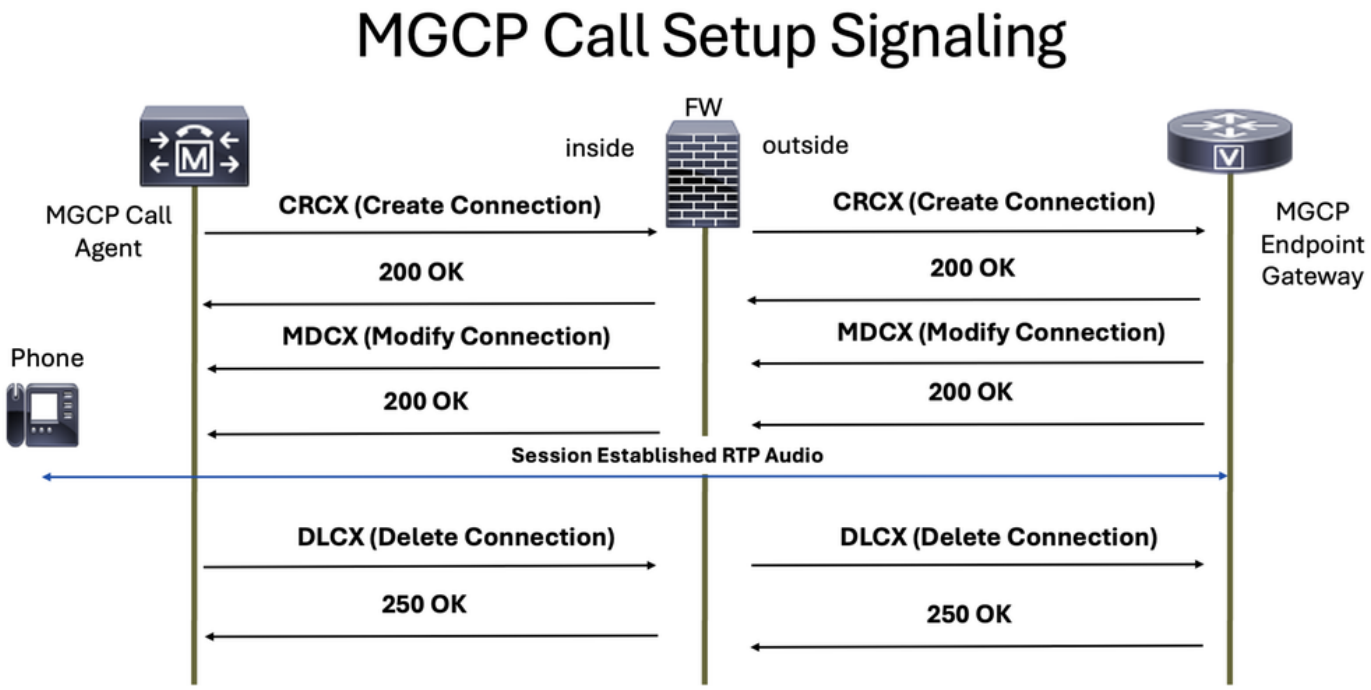
Anmerkung: Die SCCP-Inspektion ist standardmäßig auf Cisco Secure Firewall Threat Defense (FTD) und Secure Firewall Adaptive Security Appliance (ASA) aktiviert.

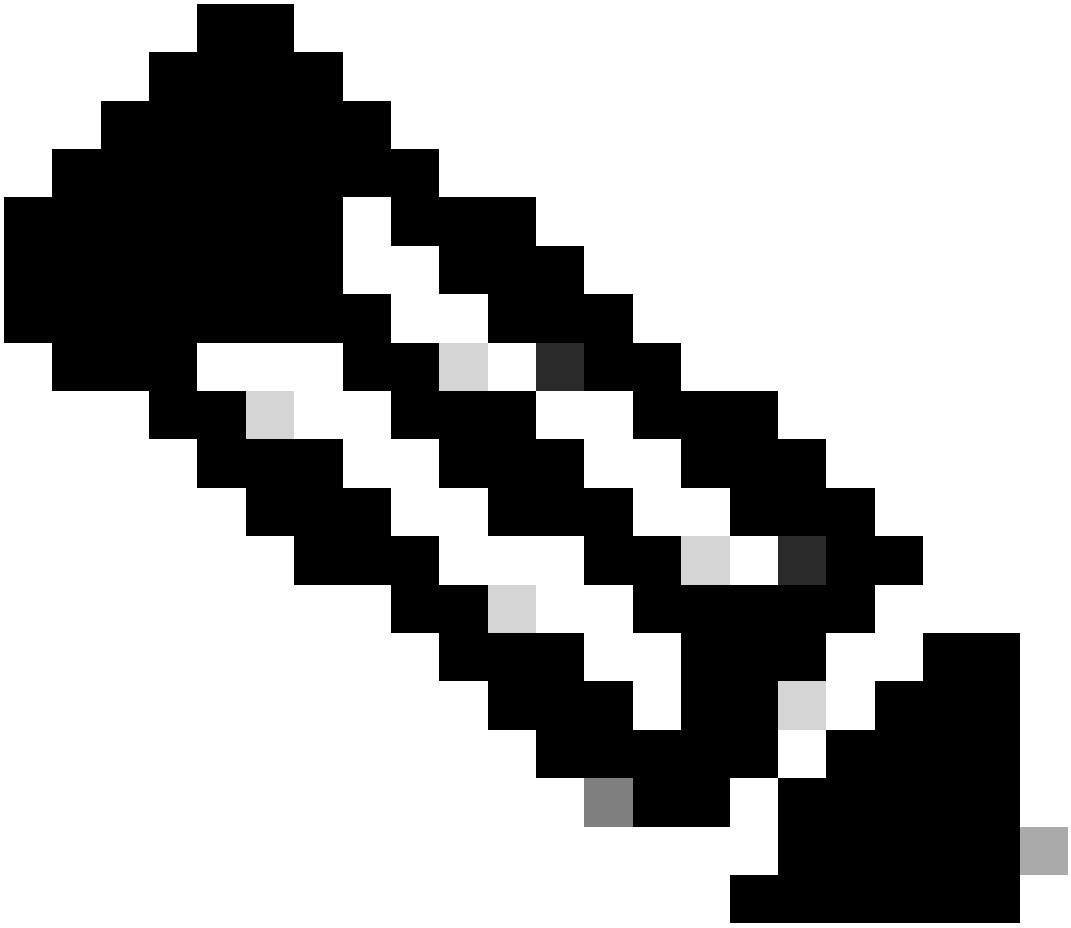
MGCP

Media Gateway Control Protocol (MGCP) ist ein Protokoll, das zur Steuerung von VoIP-Anrufen durch ein Anrufsteuergerät, z. B. CUCM, verwendet wird.

Das MGCP-Signalisierungsprotokoll ist in RFC 2705 definiert und verwendet den TCP-Port 2428 und den UDP-Port 2427 für die Kommunikation.

Die für eine Anrufkommunikation erwarteten normalen MGCP-Pakete sind:



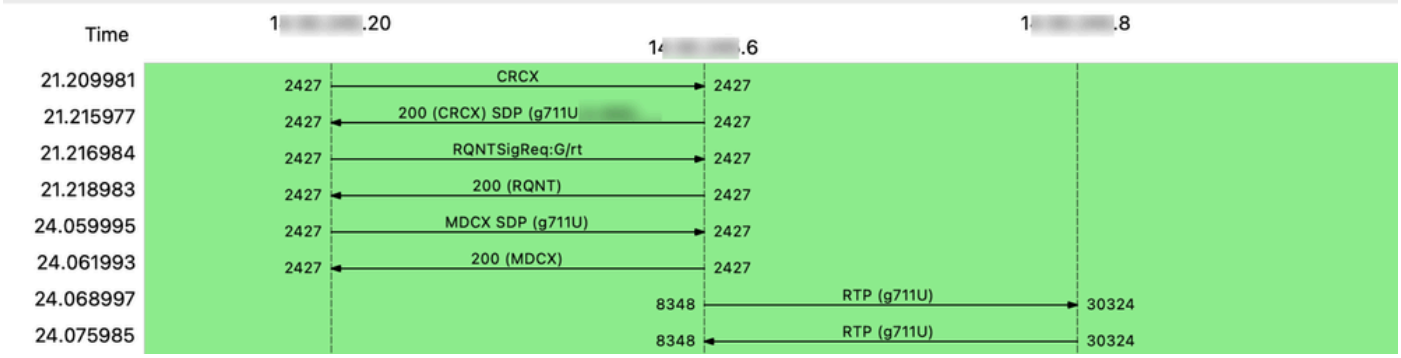


Anmerkung: Die MGCP-Inspektion ist in der Standardinspektionsrichtlinie für Cisco Secure Firewall Threat Defense (FTD) und Secure Firewall Adaptive Security Appliance (ASA) nicht aktiviert. Sie müssen sie daher aktivieren, wenn Sie diese Inspektion benötigen.

Diese Paketerfassung zeigt Anforderungen und Antworten von zwei MGCP-Geräten sowie den Medien- (Sprach-) Datenverkehr:

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

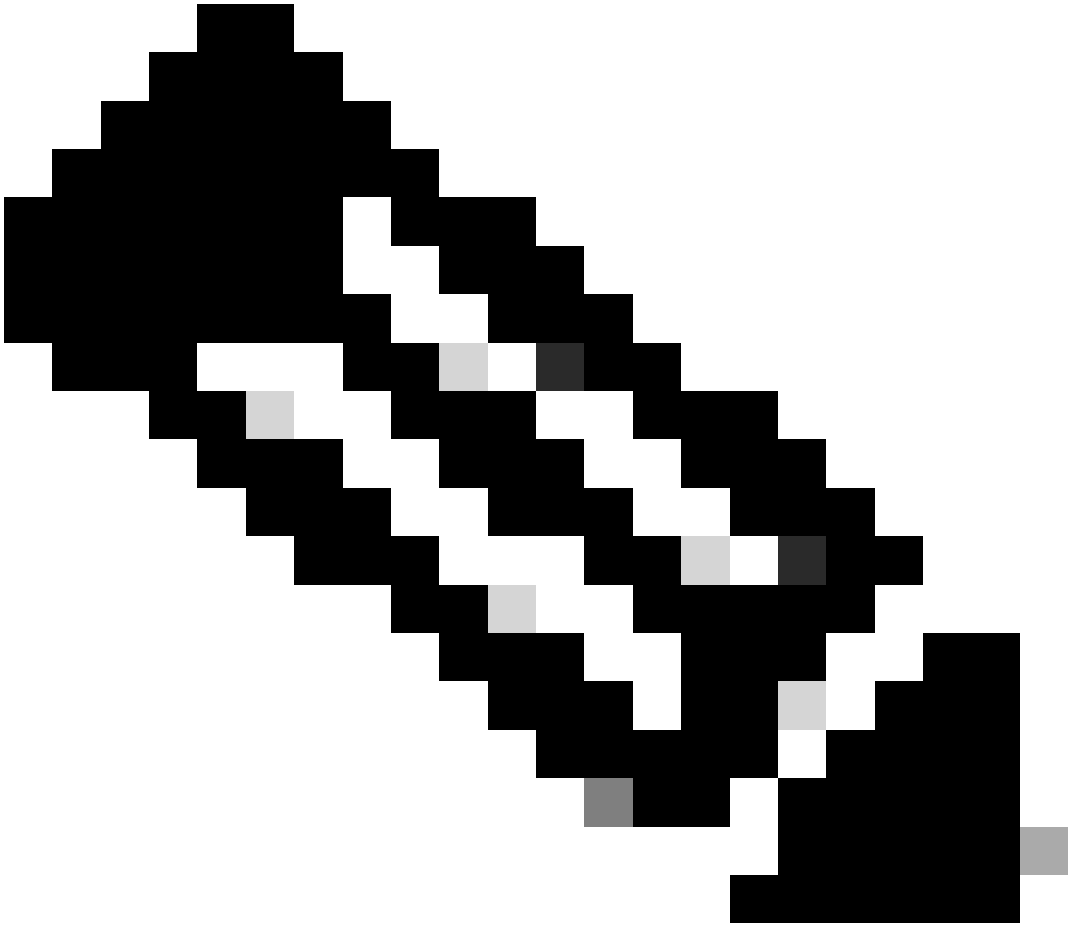
Dies ist ein Beispiel für den Fluss von MGCP-Signalisierung und RTP-Medien (Sprache):



Best Practices

Für ASA:

- Verwenden Sie eine Zulässigkeitsregel, die den Datenverkehr zu und von den beiden Signalkomponenten (Geräten oder Servern) zulässt. Dies kann durch die Ports beschränkt werden, die für das angegebene VoIP-Signalisierungsprotokoll verwendet werden.
- Lassen Sie den RTP-Port-Bereich zwischen den Mediengeräten zu, die Audio- und/oder Video-Streams senden und/oder empfangen können.



Anmerkung: Denken Sie daran, dass sich diese Audio- oder Mediengeräte von den Signalisierungskomponenten (Geräten oder Servern) unterscheiden können.

Für FTD:

- Definieren Sie Vorfilterregeln für Signalisierungskomponenten (Geräte oder Server) und definieren Sie den spezifischen Port, um nur den Datenverkehr für das angegebene Signalisierungsprotokoll zu begrenzen.
- Vorfilter für das Audio- und/oder Video-RTP-Protokoll konfigurieren

Fehlerbehebung

Bei der Behebung von Sprachproblemen müssen Sie wissen, ob es sich um ein Signalisierungs- oder ein Medienproblem (Sprache oder Video) oder um beides handelt. Hier einige Beispiele, die Ihnen helfen können, dies zu differenzieren:

Beispiel für Signalprobleme:

++ Der Benutzer meldet, dass der Anruf nicht getätigt wurde.

++ Der Benutzer kann keine anderen Benutzer oder Nummern anrufen.

++ Der SIP-Trunk wird nicht angezeigt, da die SIP-Nachricht "OPTIONS" keine Antwort erhält.

++Mein Gerät kann sich nicht registrieren.

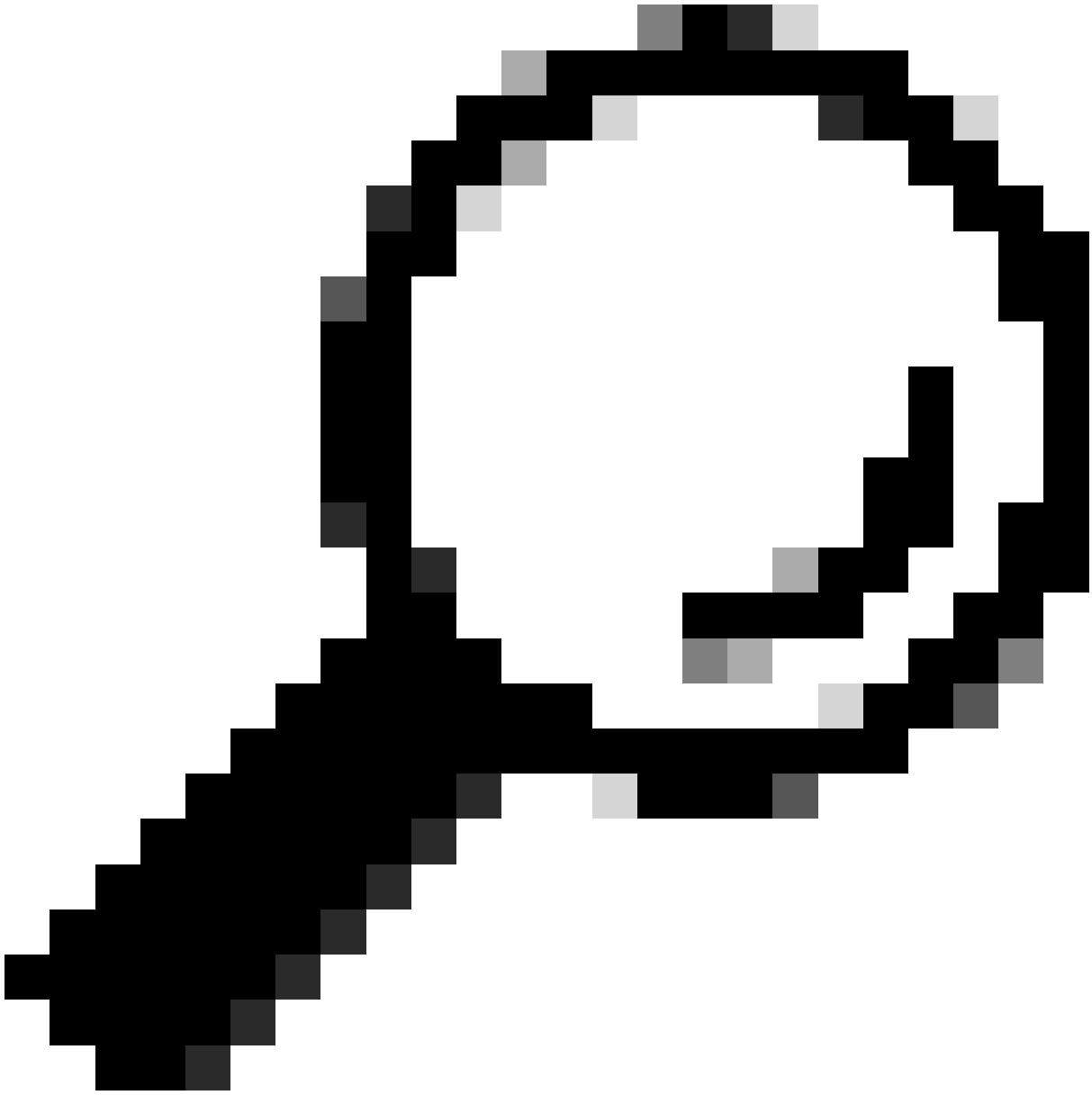
Beispiel für Probleme mit Medien (Sprache oder Video):

++Es liegt ein unidirektionales Audioproblem vor.

++Es ist kein Audio verfügbar.

++Es ist überhaupt kein Video vorhanden.

++ Der Anruf wird stumm.



Tipp: Während eines Videoanrufs kann das SDP bis zu drei Medienleitungen aushandeln: Audio, Video und Bild. Jede m-Leitung entspricht einem separaten RTP-Stream (Real-Time Transport Protocol) pro Anrufstrecke, d. h. es können bis zu drei verschiedene RTP-Streams - einer für jeden Medientyp - auf jeder Strecke des Anrufs vorhanden sein.

Fehlerbehebung bei Signalisierungsproblemen der Firewall

Zur Fehlerbehebung des Signalisierungsteils müssen Sie Folgendes sicherstellen:

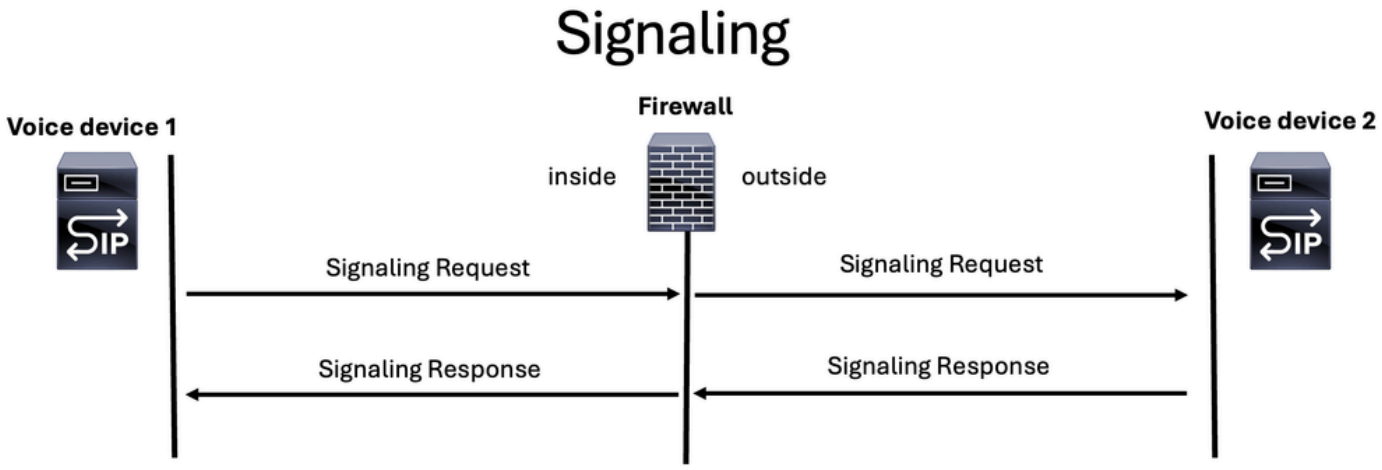
++Ermitteln Sie alle Signalisierungskomponenten (Geräte oder Server), die an dem Anruf von der Eingangs- und Ausgangsschnittstelle beteiligt sind, und konfigurieren Sie in den Paketerfassungen auf CLI von Secure FW die entsprechenden Abgleichkriterien.

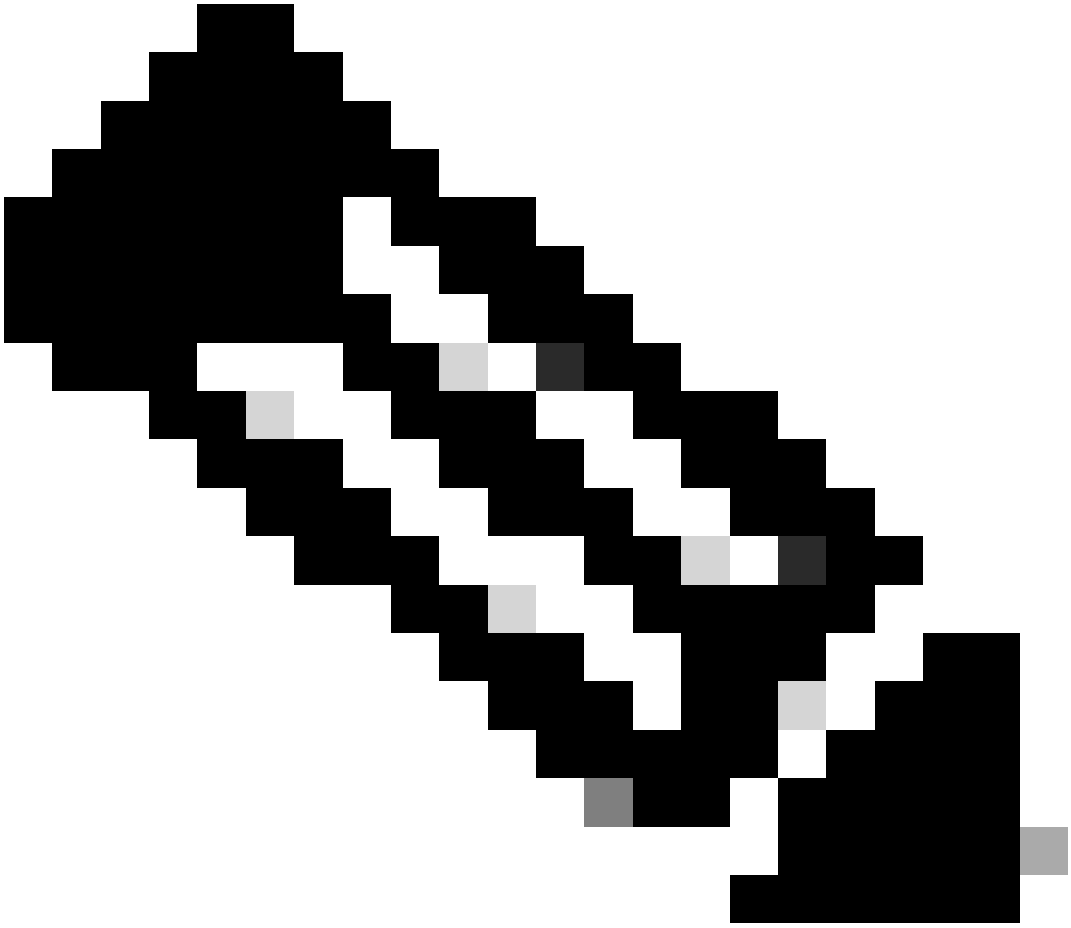
++Denken Sie daran, dass die Anzahl der Signalisierungsnachrichten an der Eingangsschnittstelle

mit der Ausgangsschnittstelle übereinstimmen muss.

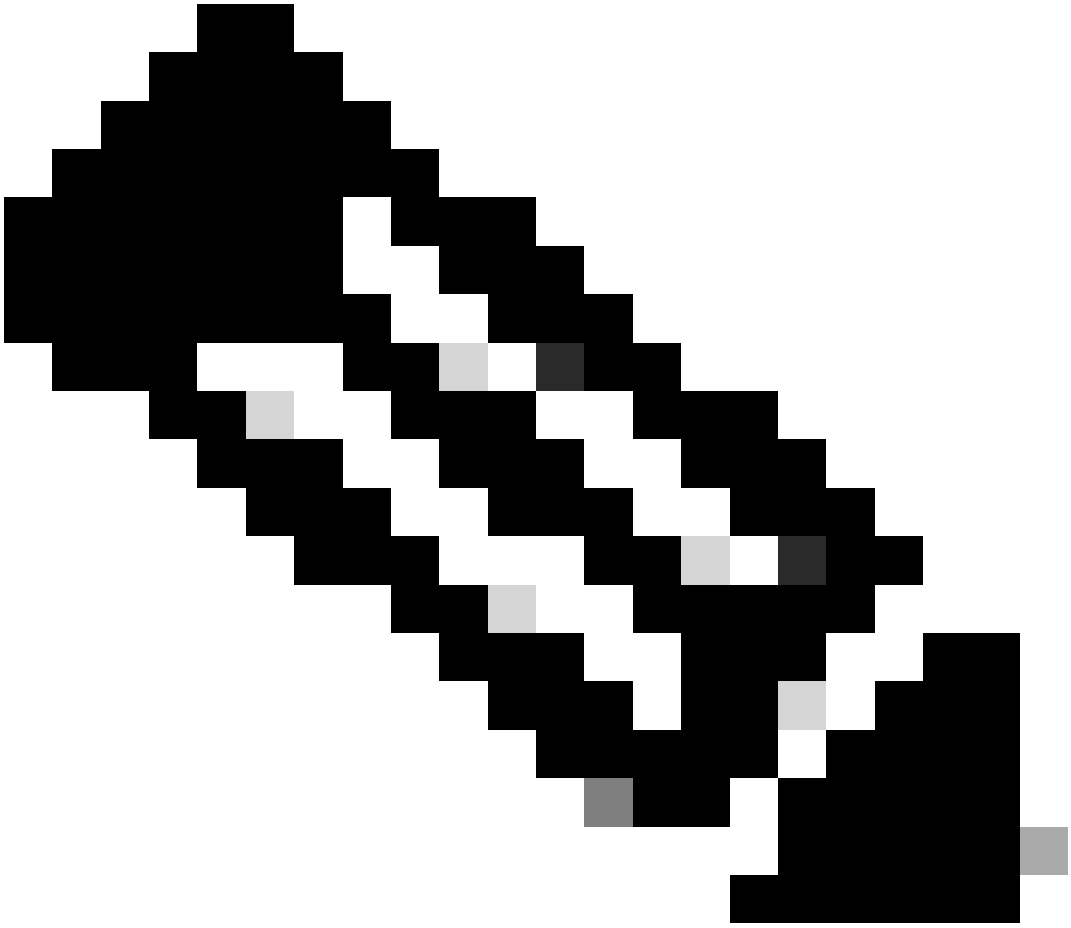
++ Die Paketerfassung kann effizienter gestaltet werden, indem angegeben wird, ob das Signalisierungsprotokoll TCP oder UDP verwendet, und indem die erwartete Portnummer gefiltert wird. Da alle Signalisierungsprotokolle über IP ausgeführt werden, hilft die Anwendung dieser Filter in der CLI, die Menge an Datenverkehr einzuschränken, die Sie in Ihren Erfassungen sehen.

++Stellen Sie nur für Ausgangsschnittstellen sicher, dass die dem ausgehenden Datenverkehr zugewiesene NAT-IP-Adresse im Paketerfassungsfilter angegeben ist. Dadurch wird sichergestellt, dass Sie den richtigen Datenverkehr erfassen, der auf der Ausgangsschnittstelle angezeigt wird.





Hinweis: Beachten Sie, dass unabhängig vom Signalisierungsprotokoll für Sprache stets eine Anforderung und eine Antwort vorhanden sein und sowohl die Eingangs- als auch die Ausgangsschnittstelle einheitlich sein müssen.

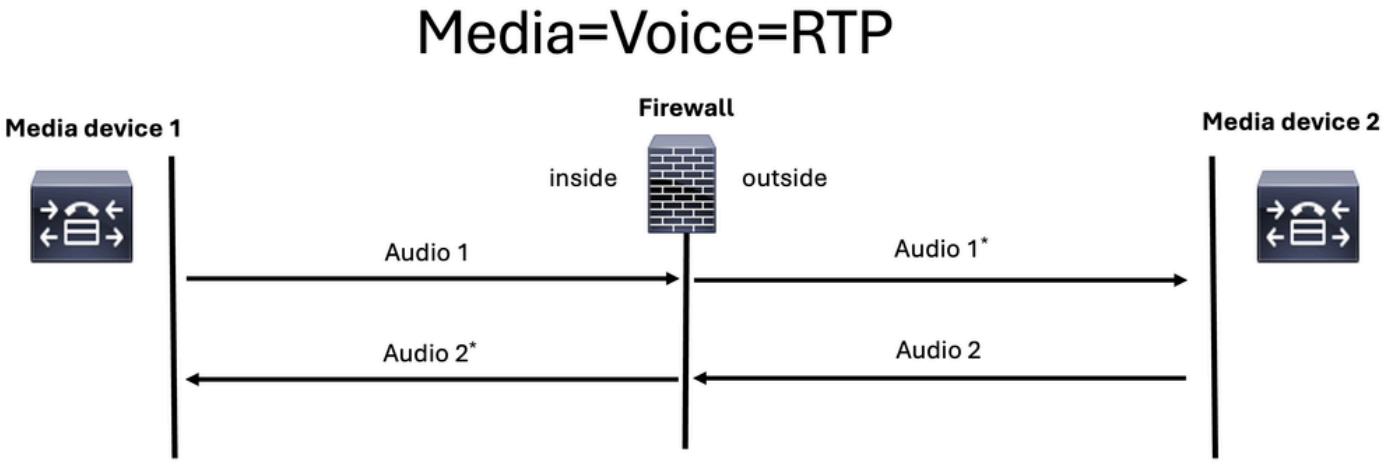


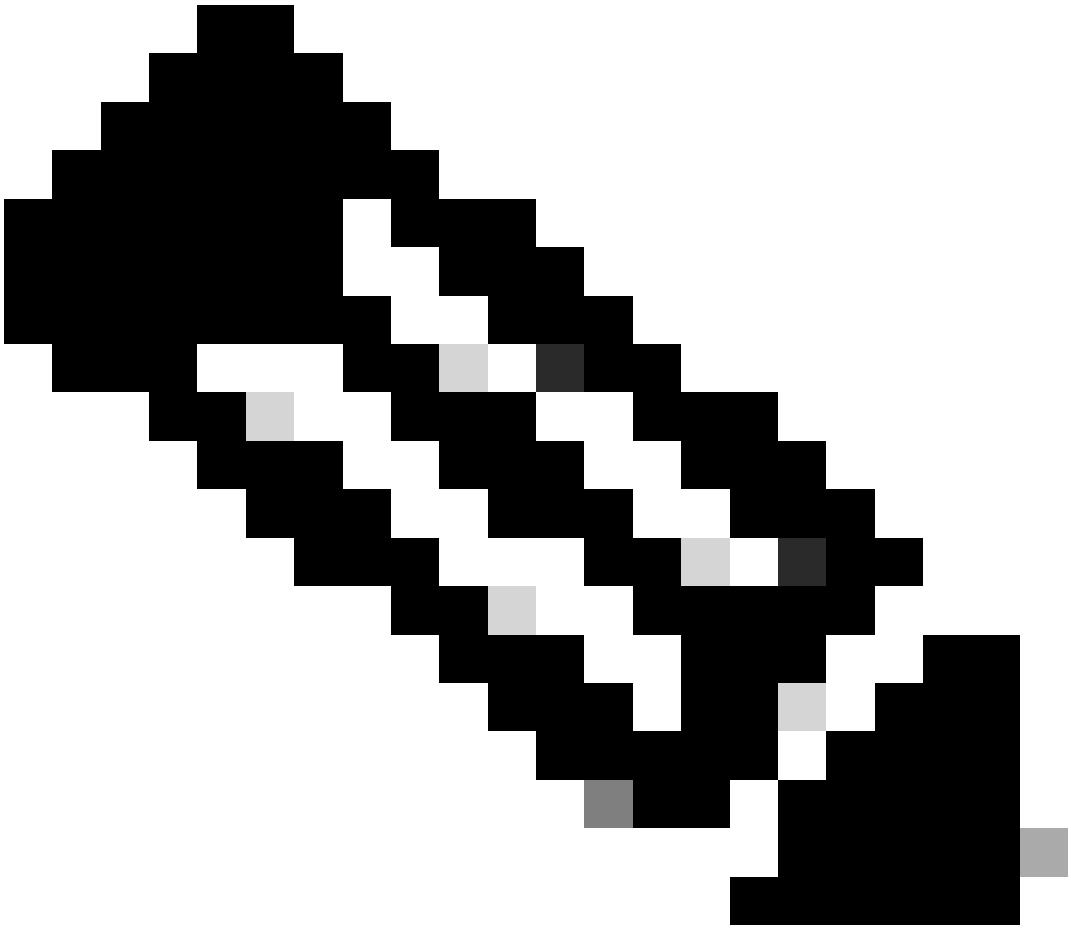
Hinweis: Stellen Sie nach Möglichkeit sicher, dass nur eine Firewall am Kommunikationspfad beteiligt ist. In einigen Bereitstellungen können Sprachsignalisierungs- und Medien-Streams separate Firewalls durchlaufen. In diesen Fällen sollten Sie alle relevanten Firewalls in den Fehlerbehebungsprozess einbeziehen.

Fehlerbehebung bei Medienproblemen in der Firewall

Aus FW-Sicht müssen bei der Fehlerbehebung von Einweg-Audio vier Streams analysiert werden. Dies gilt für Zweiwege-Audio-Probleme oder für Audio-Probleme.

1. RTP-Stream vom Anrufer zum Angerufenen (Eingangsschnittstelle).
2. RTP-Stream vom Anrufer zum Angerufenen (Ausgangsschnittstelle).
3. RTP-Stream vom Angerufenen zum Anrufer (Ausgangsschnittstelle).
4. RTP-Stream vom Angerufenen zum Anrufer (Eingangsschnittstelle).



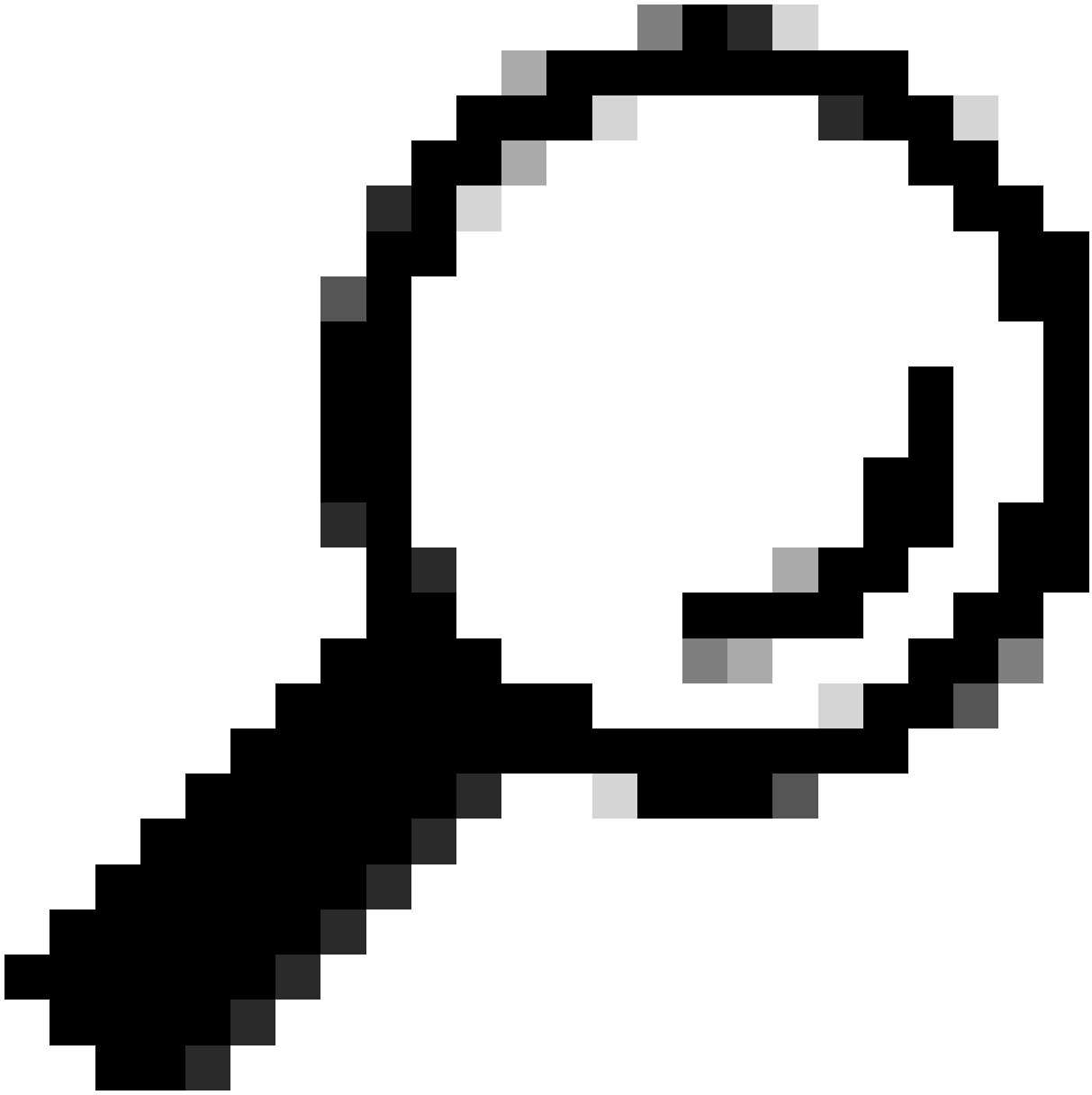


Anmerkung: Stellen Sie sicher, dass Sie die Fehlerbehebung mithilfe von CLI-Paketerfassungen entweder im ASA- oder im LINA-Modus des FTD durchführen, da dies mehr Flexibilität beim Anwenden mehrerer Übereinstimmungen innerhalb einer einzelnen Paketerfassung bietet.

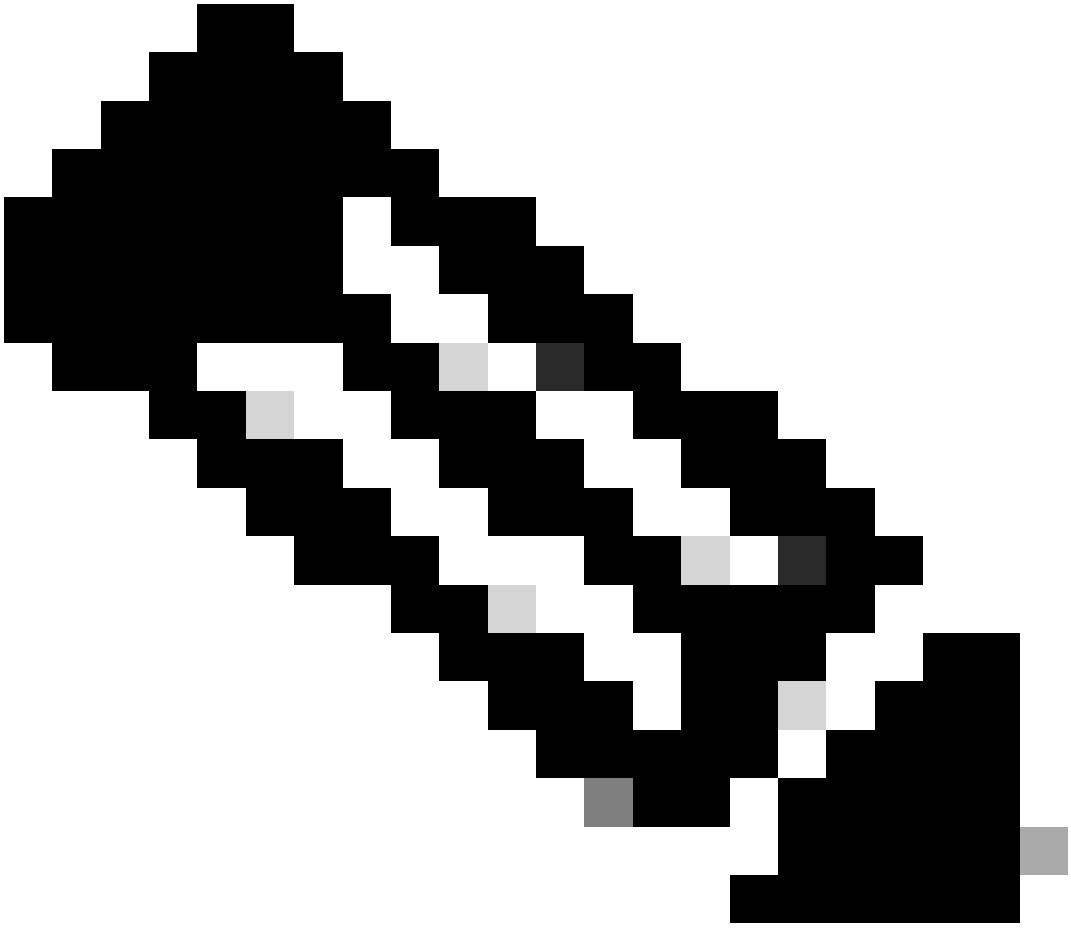
Fehlerbehebung bei SIP-Anrufen

Bei der Behebung von Sprachproblemen mit Secure FW (ASA oder FTD) müssen Sie folgende Schritte durchführen:

1. Stellen Sie sicher, dass der Anruffluss und das Topologiediagramm vorhanden sind.
2. Stellen Sie sicher, dass Sie das Problem aus der Perspektive des Benutzers verstehen.
3. Verstehen des Pfads für das Signalisierungsprotokoll
4. Informieren Sie sich über den Pfad des RTP-Protokolls für Medien.
5. Nehmen Sie Paketerfassungen sowohl an der Eingangs- als auch an der Ausgangsschnittstelle.
6. Überprüfen der ACL-Konfigurationsregeln und NAT-Regeln
7. Vergewissern Sie sich, dass der SIP-Signalisierungsverkehr nicht von der Firewall blockiert wird. Vergleichen Sie außerdem die Eingangs- und Ausgangsschnittstellen, um den Sprachdatenfluss zu analysieren.
8. Überprüfen Sie, ob der RTP-Medienverkehr von der Firewall blockiert wird, indem Sie den Datenverkehrsfluss an den Eingangs- und Ausgangsschnittstellen vergleichen.
9. Stellen Sie sicher, dass die Signalisierungsgeräte eine Überprüfung unterstützen, und deaktivieren Sie diese, wenn dies nicht der Fall ist.



Tipp: Die SIP-Signalisierungsnachrichten, die in die FW eingehen, müssen mit denen der FW-Austritt übereinstimmen.



Anmerkung: Die Tipps zur Fehlerbehebung für SIP können auch auf H.323-, MGCP- und SCCP-Protokolle angewendet werden.

Zugehörige Informationen

- Konfigurieren von ASA-Paketerfassungen mit CLI
- Nutzung von FirePOWER Threat Defense-Aufzeichnungen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.