Conoscere le basi dei protocolli Voice over IP per un firewall sicuro

Sommario

Introduzione

Questo documento descrive i principi di base dei vari protocolli VoIP per assistere i tecnici nella risoluzione efficace dei problemi su firewall sicuri.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Questo documento è stato redatto per essere utilizzato nella risoluzione dei problemi relativi a questi dispositivi:

- Secure Firewall Threat Defense (FTD)
- Appliance ASA (Secure Firewall Adaptive Security Appliance)

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

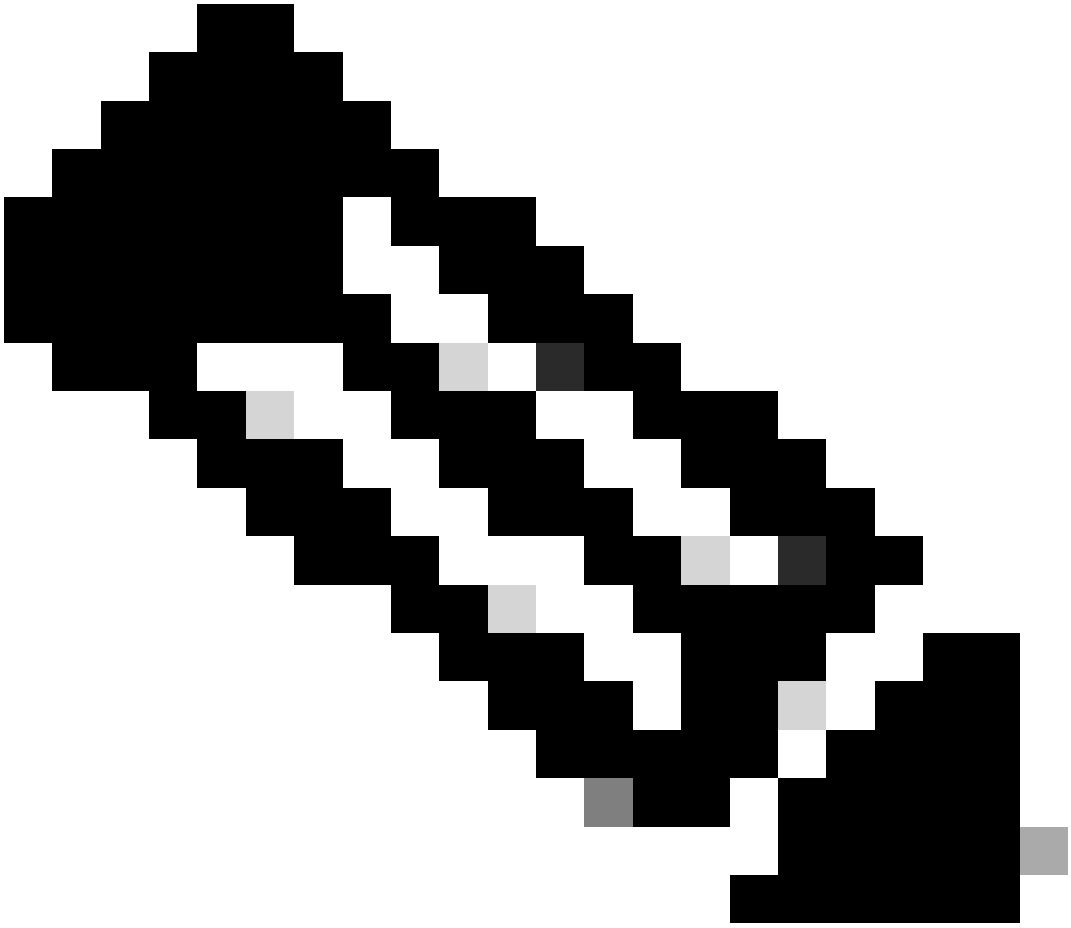
Nozioni di base sul VoIP

La comunicazione è fondamentale per le interazioni umane, i protocolli VoIP (Voice over IP) sono diventati indispensabili per la comunicazione umana. Ecco perché è importante conoscere le parti che le compongono quando si risolve un problema relativo a uno scenario che include un firewall (FW).

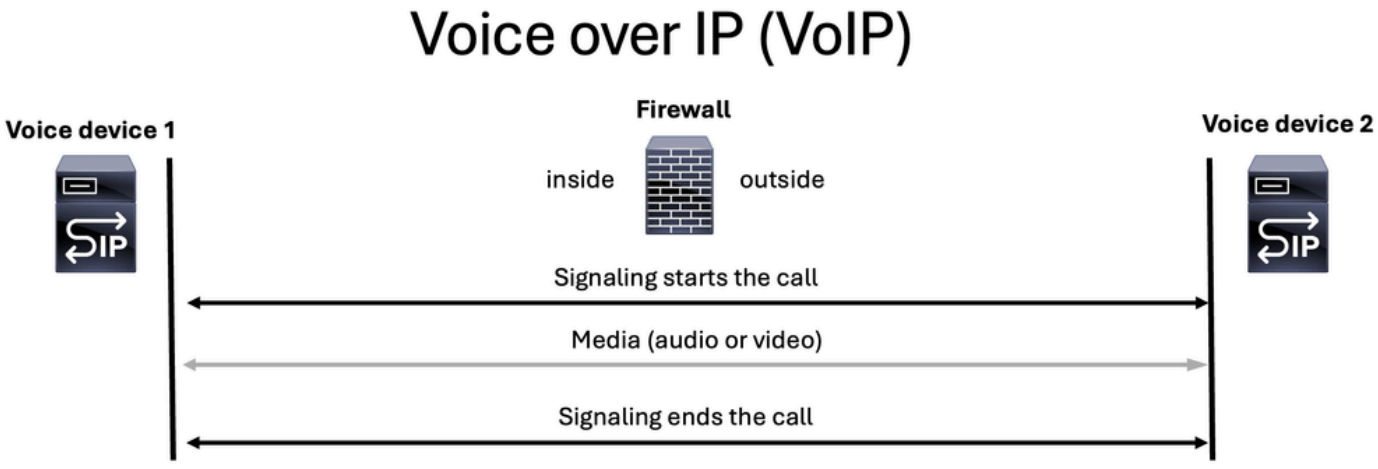
Il VoIP è composto da due parti:

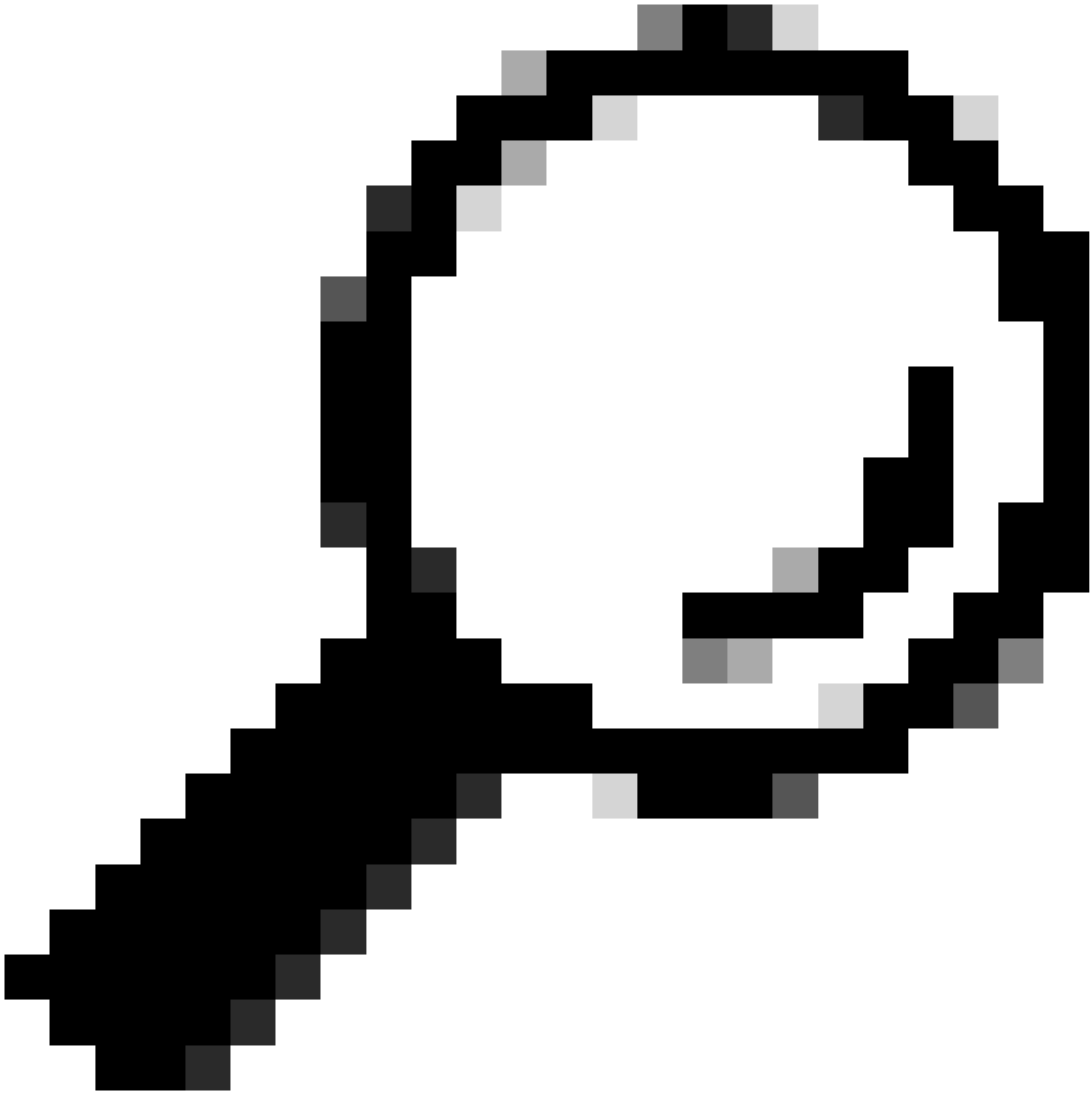
- Trasmissione dei segnali
- Supporti (voce o video)

Le comunicazioni VoIP iniziano sempre con una porzione di segnalazione per iniziare una chiamata, quindi il supporto (voce o video) viene trasmesso in streaming e la segnalazione termina la chiamata.

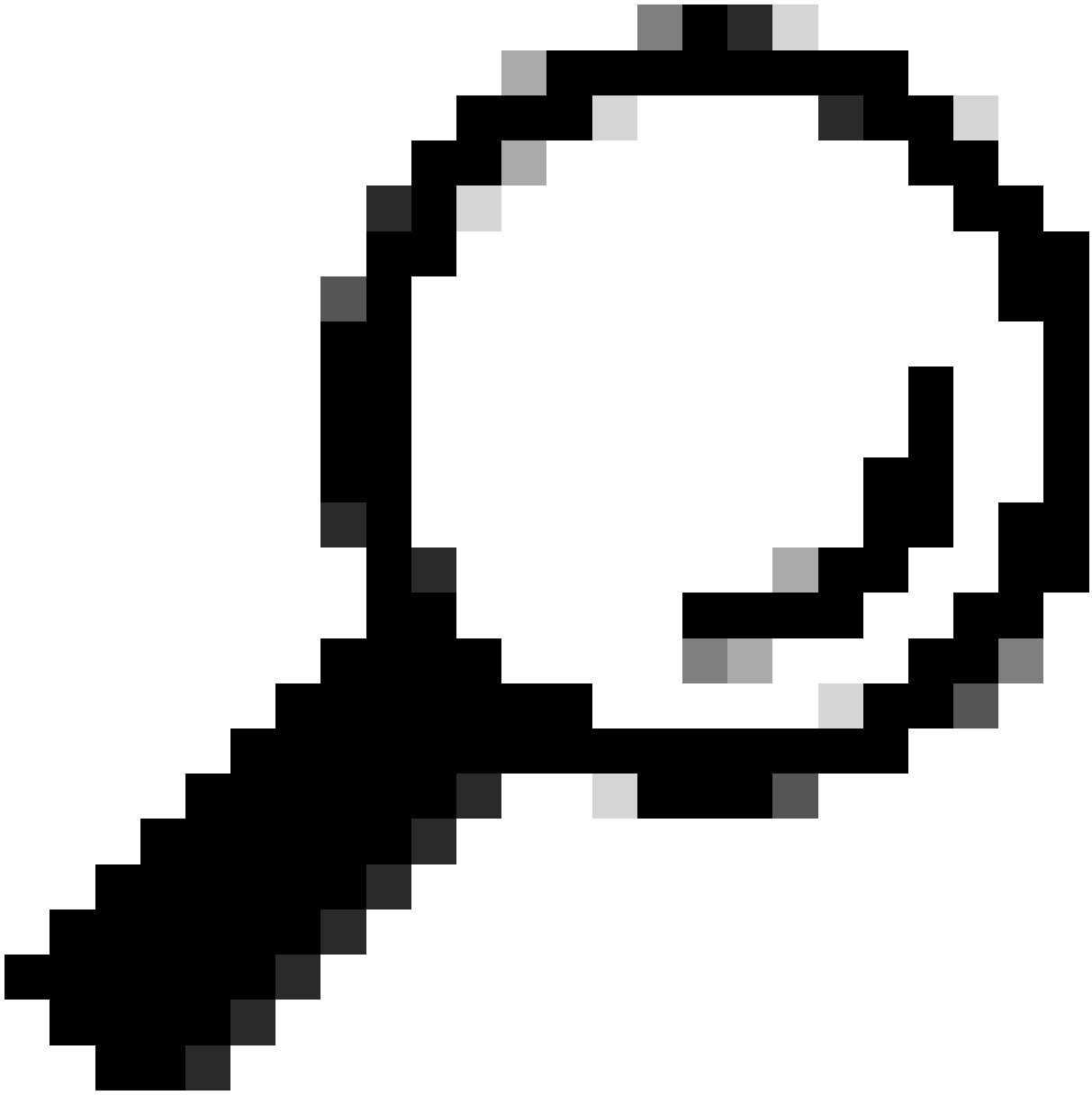


Nota: Il protocollo SIP è il più utilizzato, quindi è rappresentato in modo coerente come icona del server vocale SIP in molti diagrammi.





Suggerimento: Quando si risolve un problema vocale per ASA o FTD, è fondamentale considerare lo scenario dal punto di vista dell'utente. È necessario determinare se la chiamata è stabilita o se non è presente audio o audio unidirezionale. Queste informazioni forniscono utili indizi sulla causa del problema, ossia se si tratta di un problema relativo al protocollo di segnalazione o al protocollo multimediale (voce o video).



Suggerimento: Un dispositivo voce può gestire il traffico RTP (Voice Real-time Transport Protocol), il traffico di segnalazione o entrambi contemporaneamente. Quando si risolvono i problemi relativi alla voce, è essenziale ricordare i seguenti concetti principali:

++Server di segnalazione: Questi server sono responsabili solo della gestione del traffico di segnalazione.

++Server multimediali: Questi server gestiscono esclusivamente il traffico RTP vocale.

++Alcuni dispositivi possono gestire entrambe le attività.

Trasmissione dei segnali

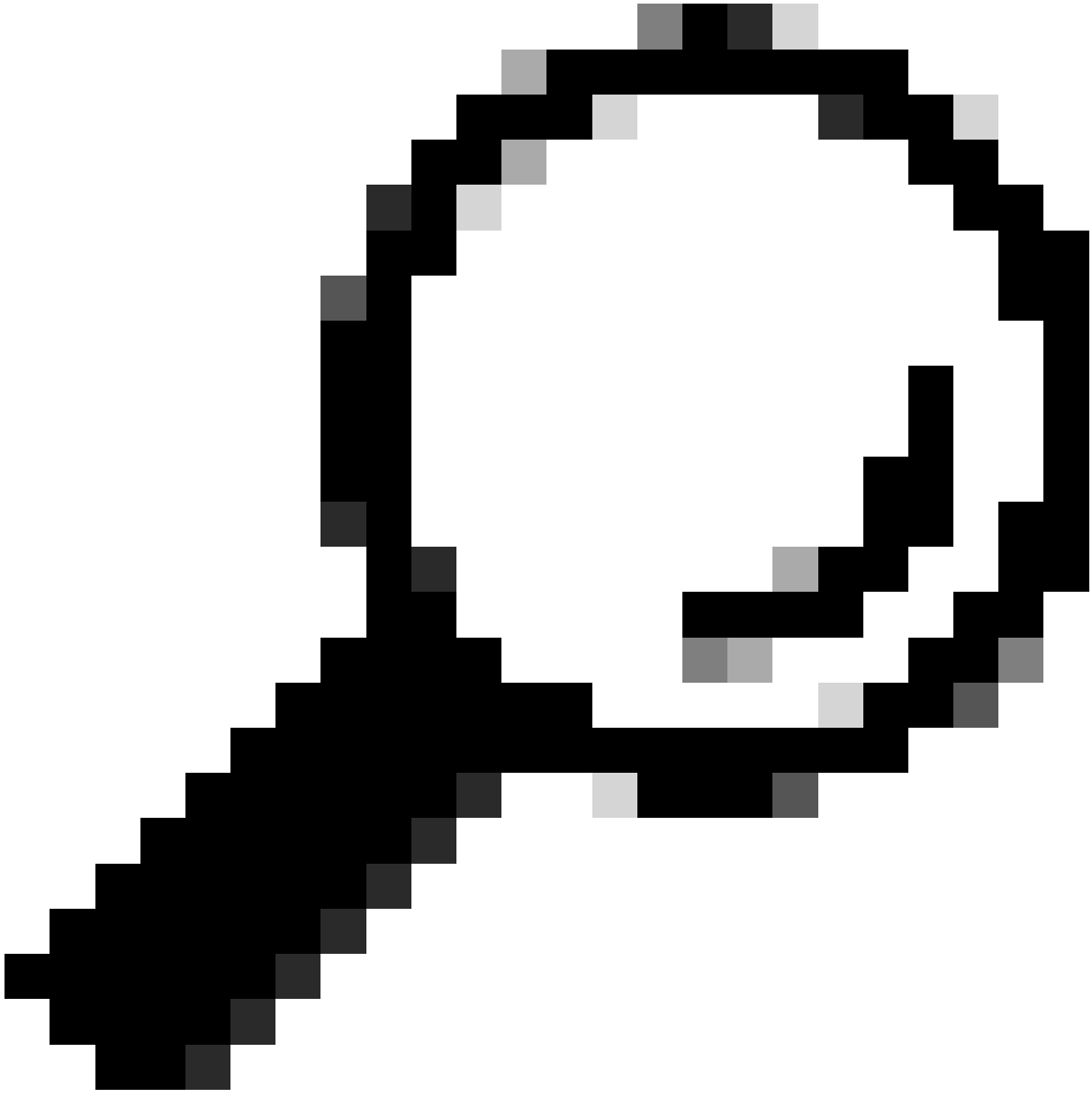
Il protocollo di segnalazione è la parte di una chiamata che avvia la comunicazione vocale, ma

non solo, esegue anche queste funzioni:

- Continua a comunicare.
- Modifica la comunicazione.
- Termina la comunicazione.

I diversi tipi di protocolli di segnalazione consentono di stabilire una chiamata e i più comuni includono:

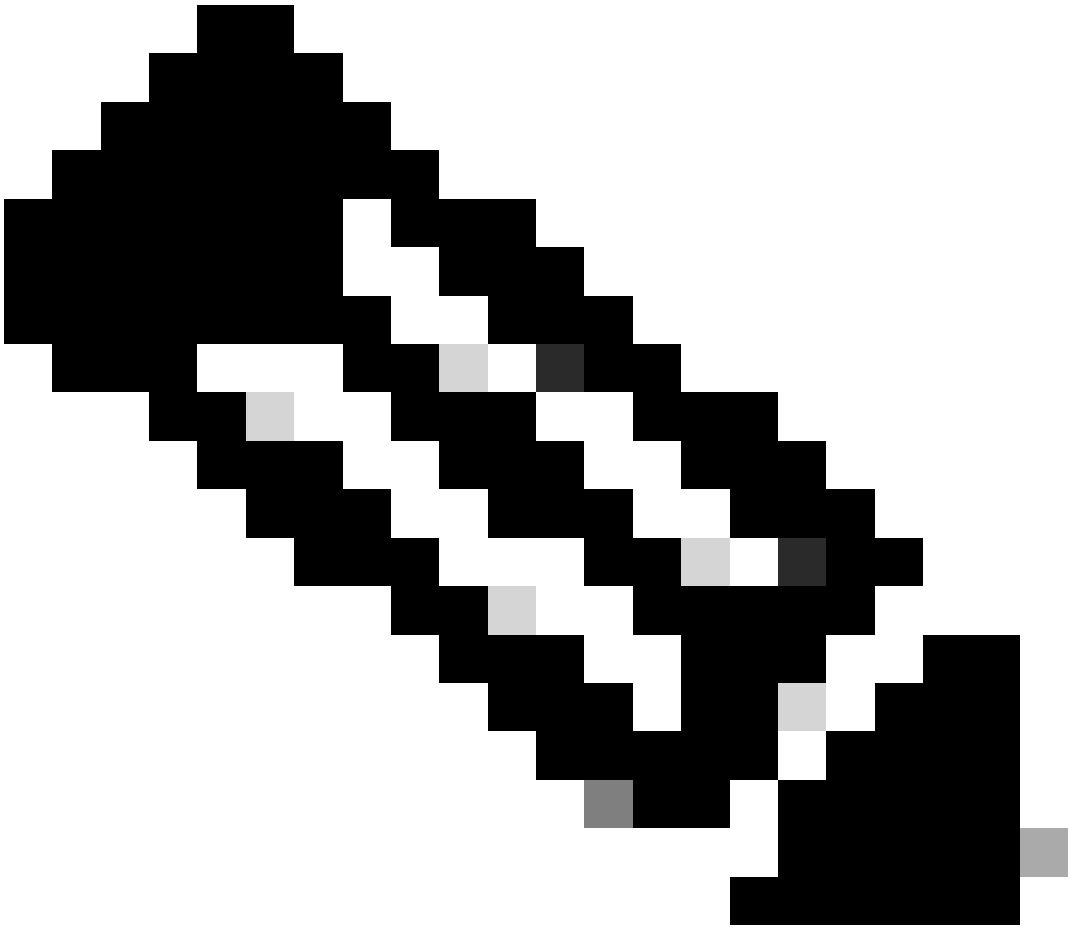
- SIP (Session Initiation Protocol)
- H.323
- Protocollo MGCP (Media Gateway Control Protocol)
- Protocollo SCCP (Skinny Call Control Protocol)



Suggerimento: È essenziale identificare il protocollo di segnalazione in uso per

---

determinare le porte appropriate per l'acquisizione dei pacchetti sull'ASA o sull'FTD. Inoltre, disporre di un flusso di chiamate e di una topologia di rete è utile per comprendere il percorso di segnalazione.

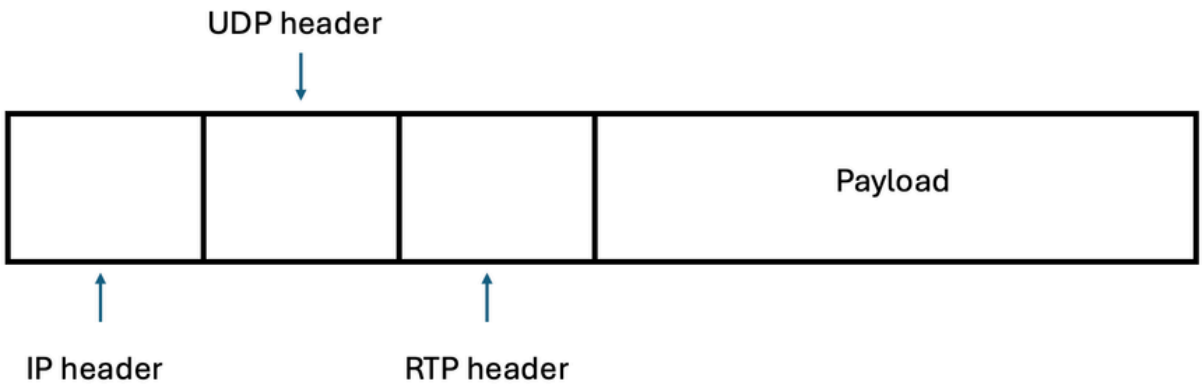


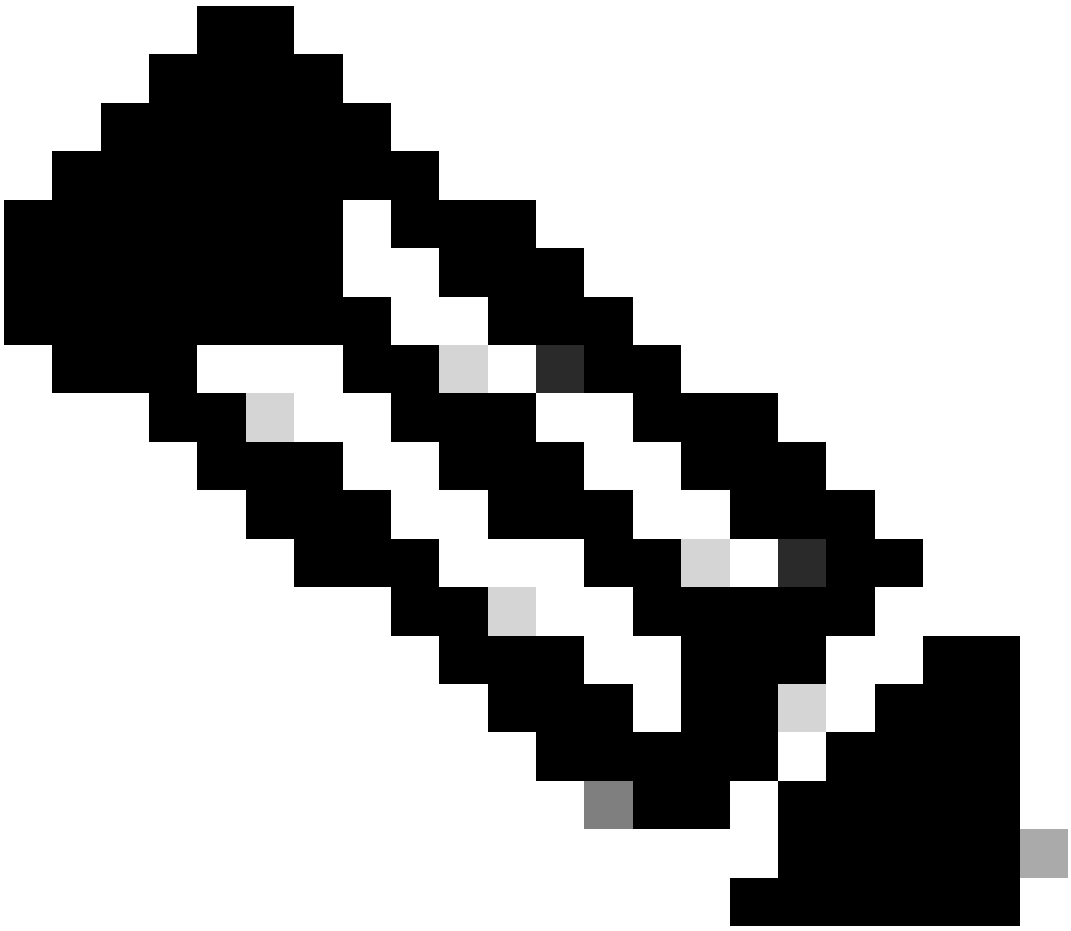
Nota: I pacchetti di segnalazione includono indirizzi IP di origine e di destinazione, che aiutano a identificare le parti coinvolte nell'invio e nella ricezione del flusso multimediale RTP.

Supporti

Al termine della segnalazione e dopo che i componenti di segnalazione (dispositivi o server) concordano sul tipo di supporto, entra in gioco il Real Time Protocol (RTP) per iniziare l'invio di contenuti multimediali (audio e/o video) a tutte le parti coinvolte.

RTP è un protocollo Internet utilizzato per lo streaming multimediale che viene inviato solo dopo che la chiamata è stata stabilita e viene eseguito su UDP (User Datagram Protocol).

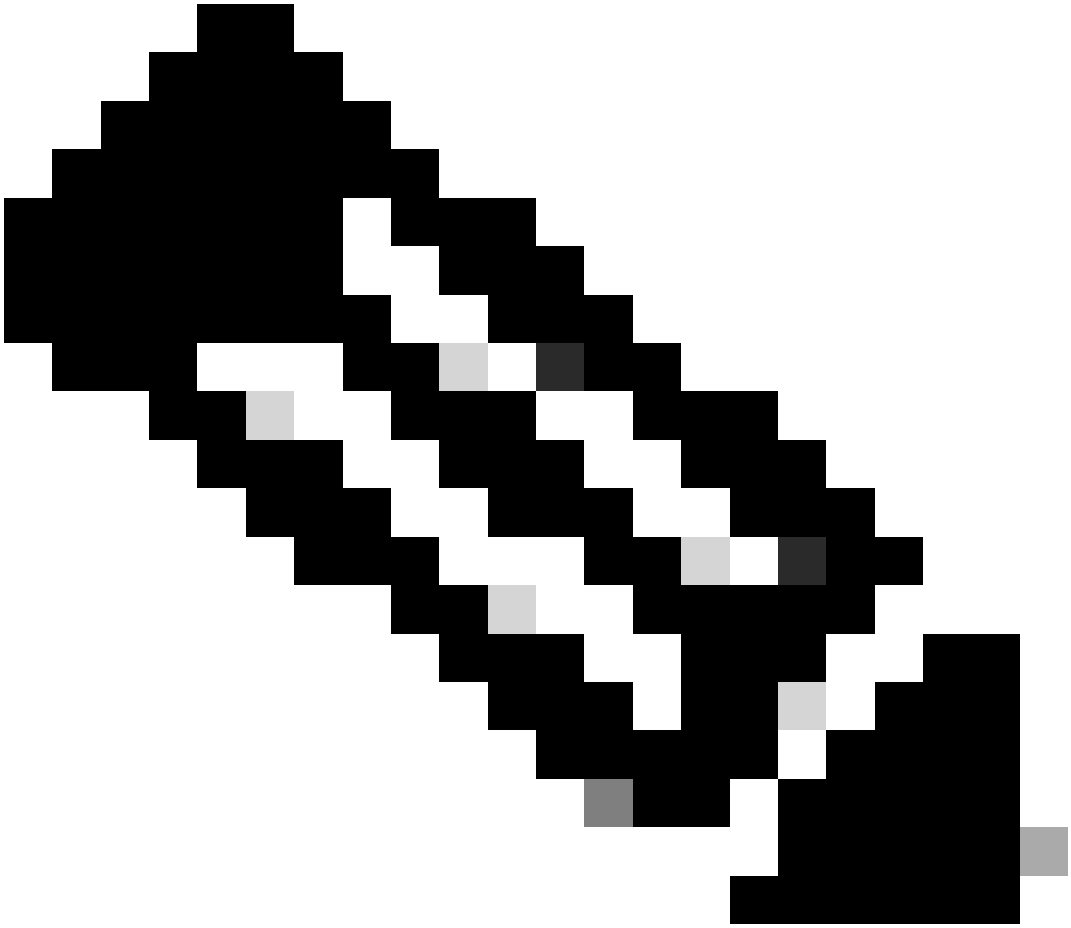




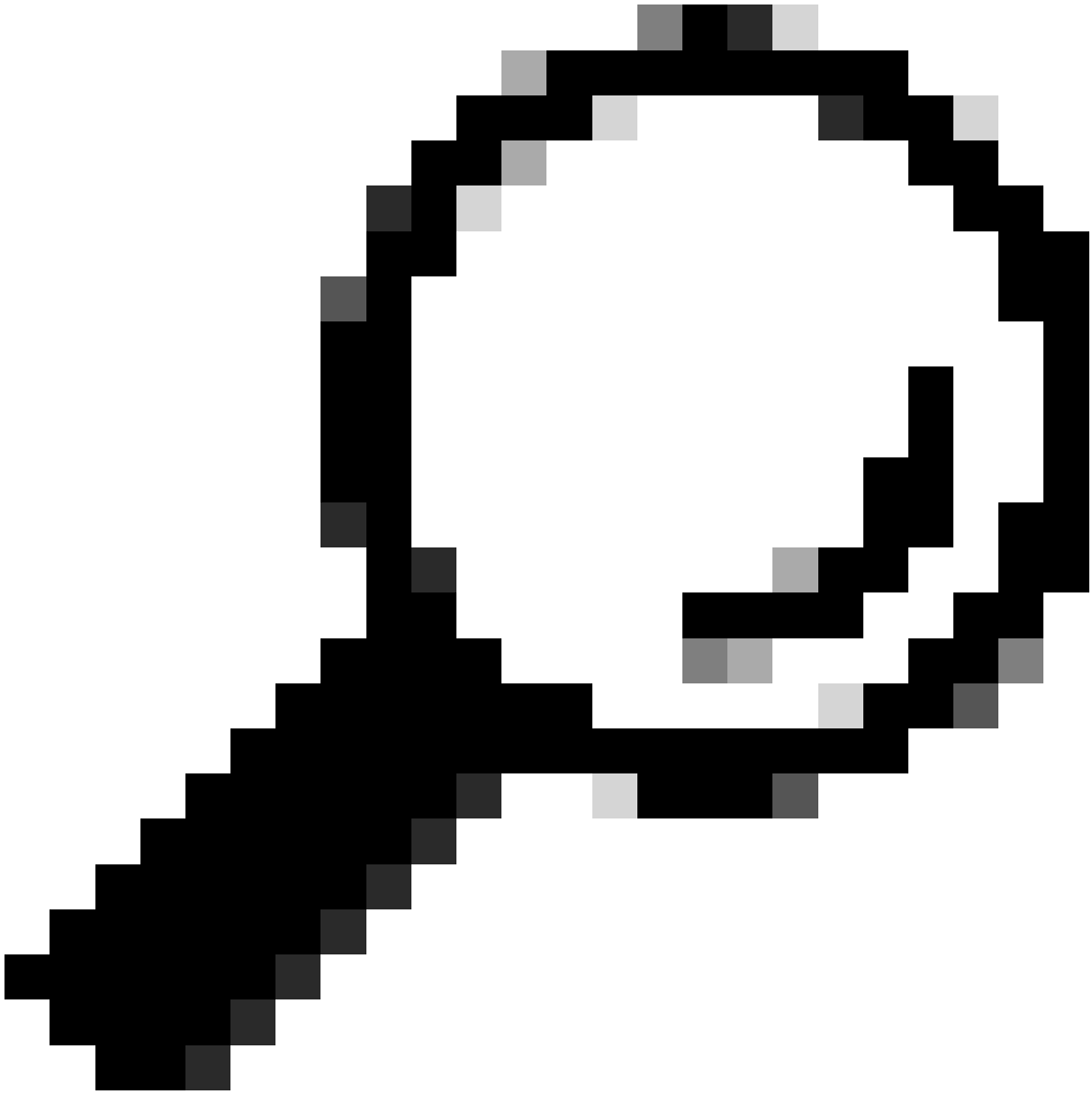
Nota: I supporti possono essere voce e/o video e possono essere trasportati su pacchetti RTP.

I componenti di segnalazione (dispositivi o server) determinano le porte utilizzate per l'invio o la ricezione di supporti (audio e/o video). L'intervallo di porte più comune per il protocollo RTP è in

genere compreso tra 16384 e 32767 per la maggior parte dei dispositivi.



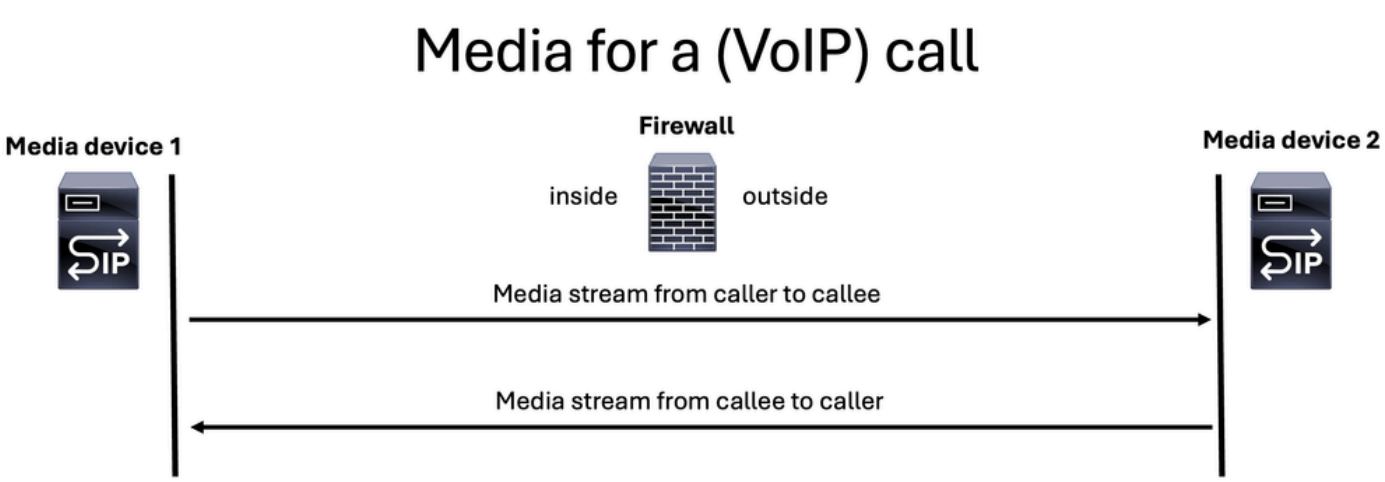
Nota: Alcuni dispositivi Cisco, ad esempio le piattaforme ASR e ISR G3 come la piattaforma ISR4K, utilizzano un intervallo di porte RTP standardizzato compreso tra 8000 e 48200. È fondamentale verificare l'intervallo di porte RTP specifico configurato sui dispositivi, in quanto può differire da questi valori standardizzati e può variare tra dispositivi di terze parti.

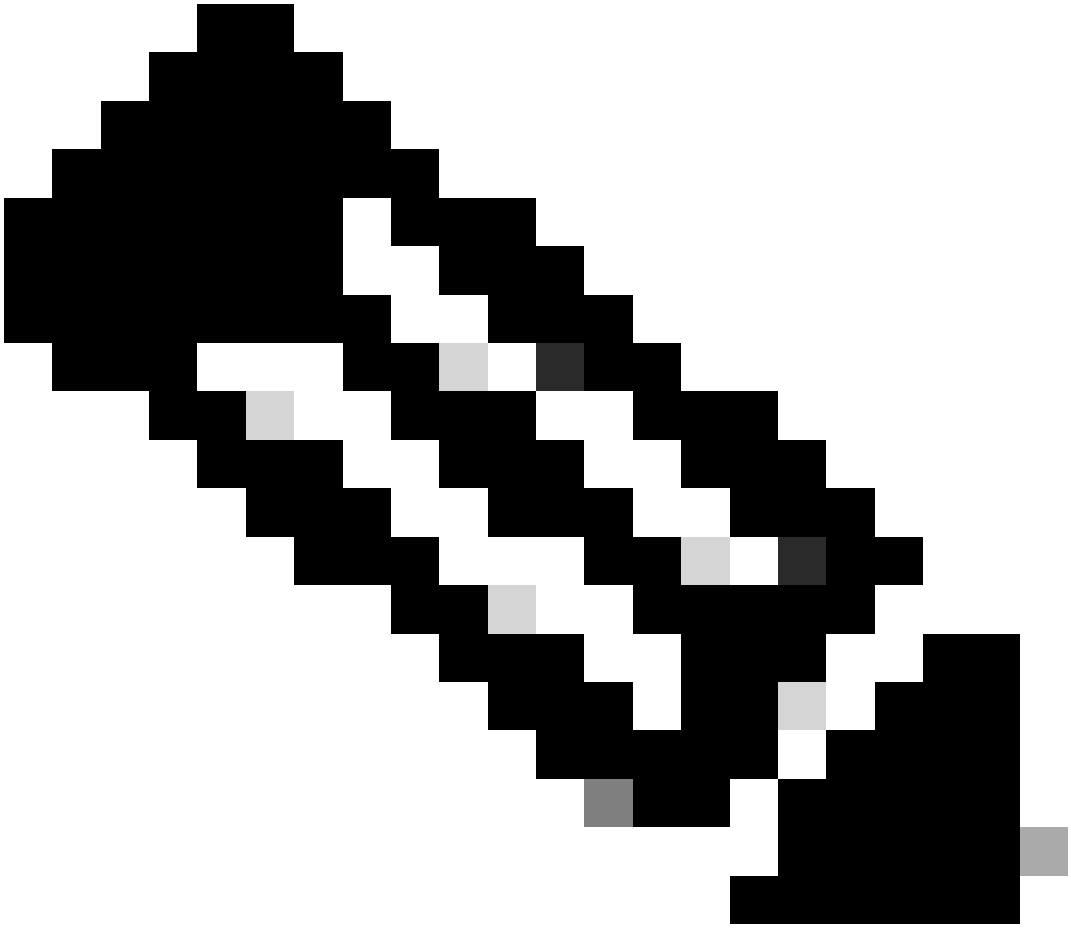


Suggerimento: A volte il percorso RTP differisce dal percorso di segnalazione, rendendo cruciale l'identificazione dei dispositivi responsabili dell'invio e della ricezione dei pacchetti RTP voce. in modo da acquisire il traffico UDP tra i dispositivi che attraversano l'ASA o l'FTD.

In una normale chiamata vocale vengono generati due flussi multimediali o flussi RTP:

1. un flusso multimediale dal chiamante al chiamante
2. un flusso multimediale dal chiamante al chiamante





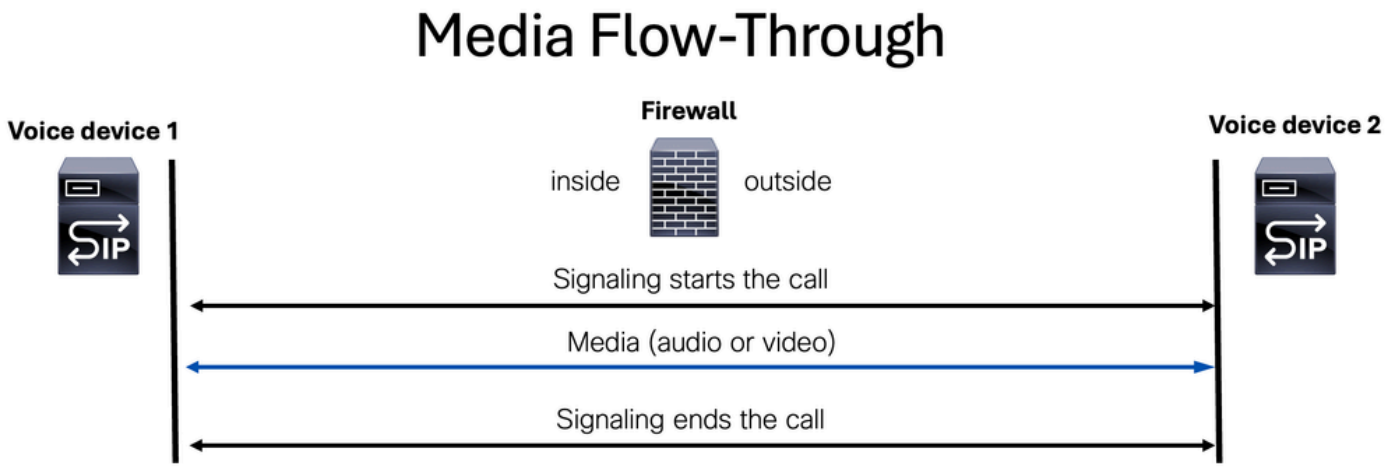
Nota: A scopo illustrativo, l'icona del server SIP viene utilizzata per rappresentare un server di segnalazione o un server multimediale in tutte le immagini.

Quando si parla di streaming multimediale in una chiamata vocale, è importante evidenziare due scenari chiave:

1. Flow-through multimediale
2. Flusso dei supporti

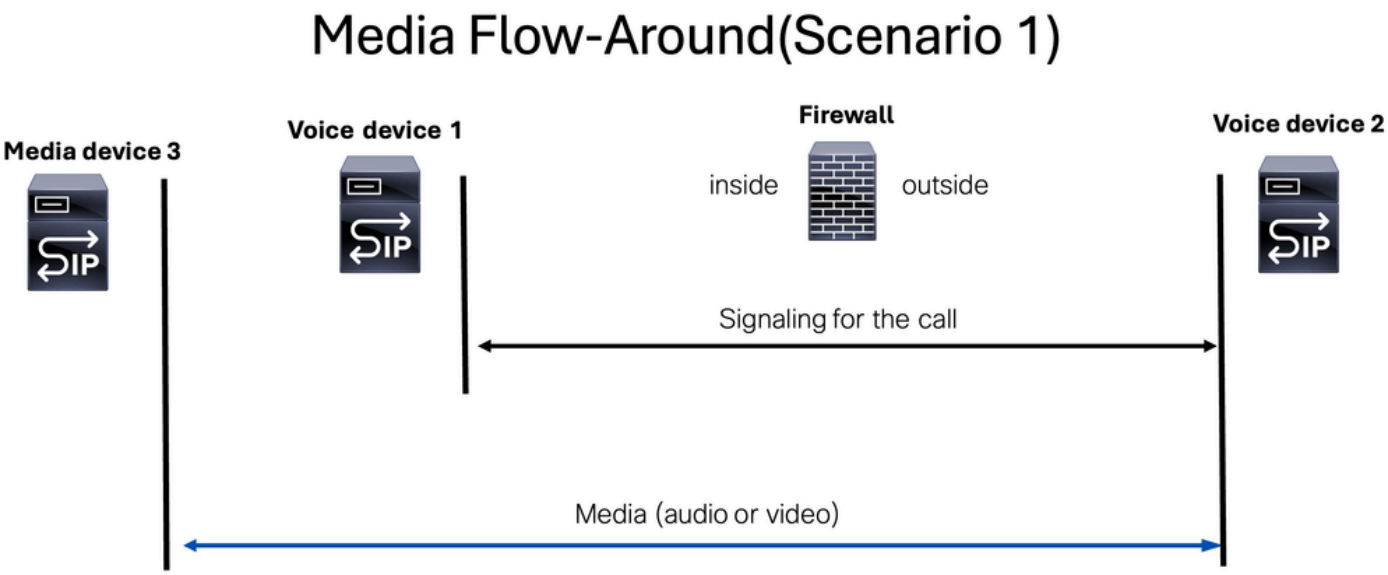
Flow-through multimediale

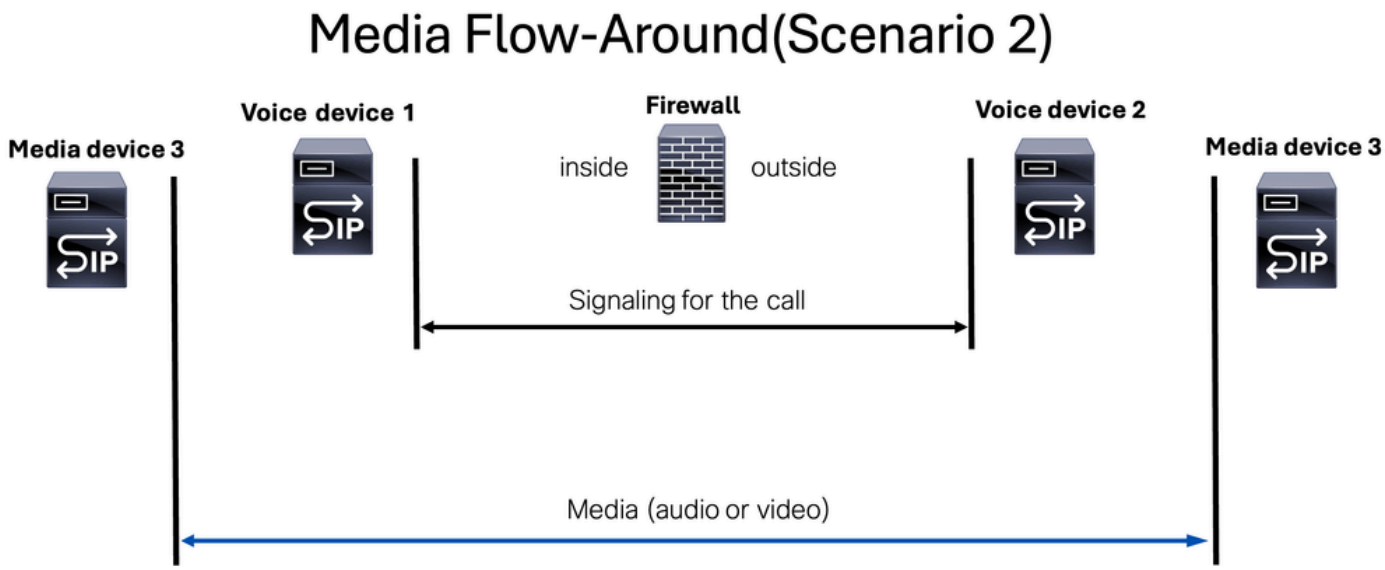
Il flusso attraverso i supporti è una modalità in cui i pacchetti multimediali (voce e/o video) e di segnalazione vengono elaborati dallo stesso dispositivo.



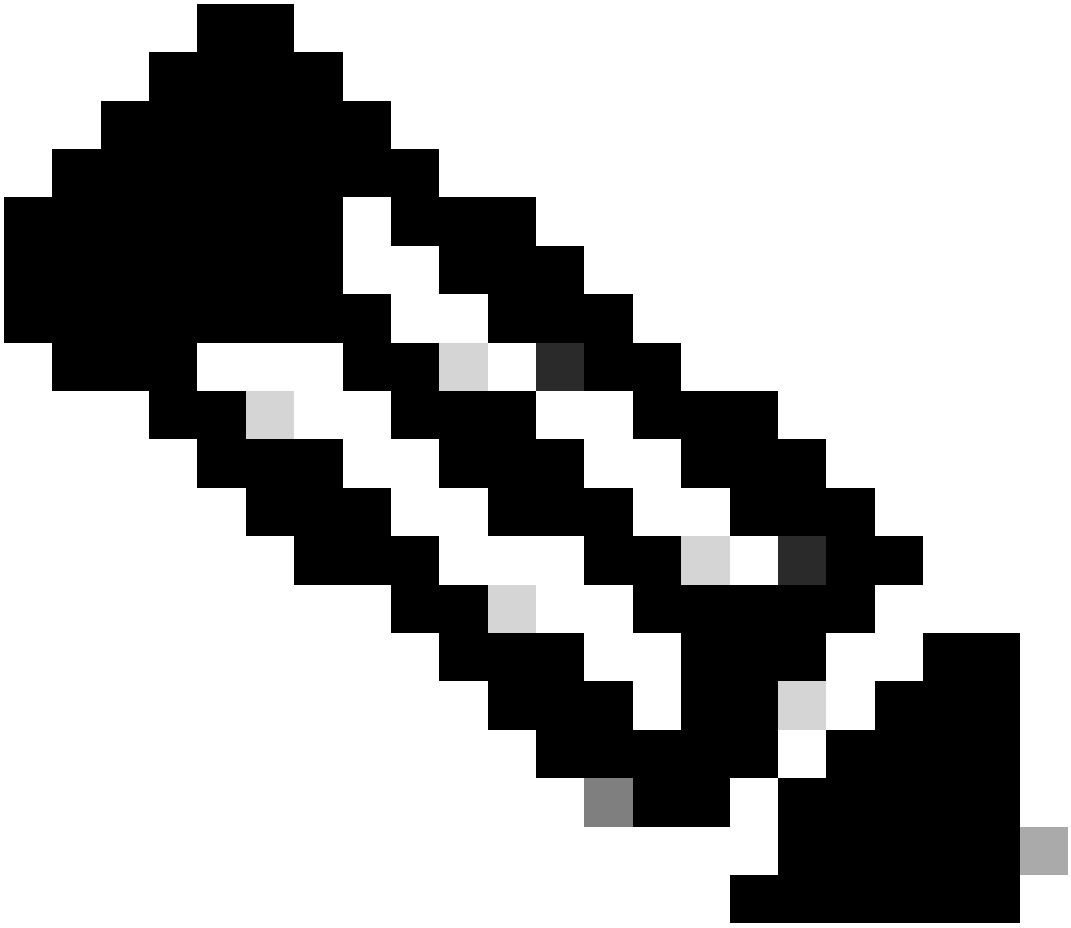
Flusso dei supporti

Il flusso continuo di flussi multimediali è una modalità in cui i pacchetti di segnalazione vengono gestiti da due componenti di segnalazione separati (dispositivi o server), mentre il flusso multimediale (voce o video) viene gestito da un terzo dispositivo noto come dispositivo multimediale.





Questa modalità chiarisce i ruoli dei dispositivi interessati e la distinzione tra segnali e flussi o dispositivi multimediali.



Nota: Questo è particolarmente importante da menzionare quando la risoluzione dei problemi dell'elenco degli accessi creato potrebbe consentire i componenti di segnalazione (dispositivi o server), ma se il flusso multimediale sta utilizzando un altro dispositivo multimediale, dobbiamo consentirlo anche nell'elenco degli accessi del nostro dispositivo FW.

SIP (Session Initiation Protocol)

Il SIP è un protocollo di controllo a livello di applicazione definito dall'Internet Engineering Task Force (IETF) nella RFC 3261.

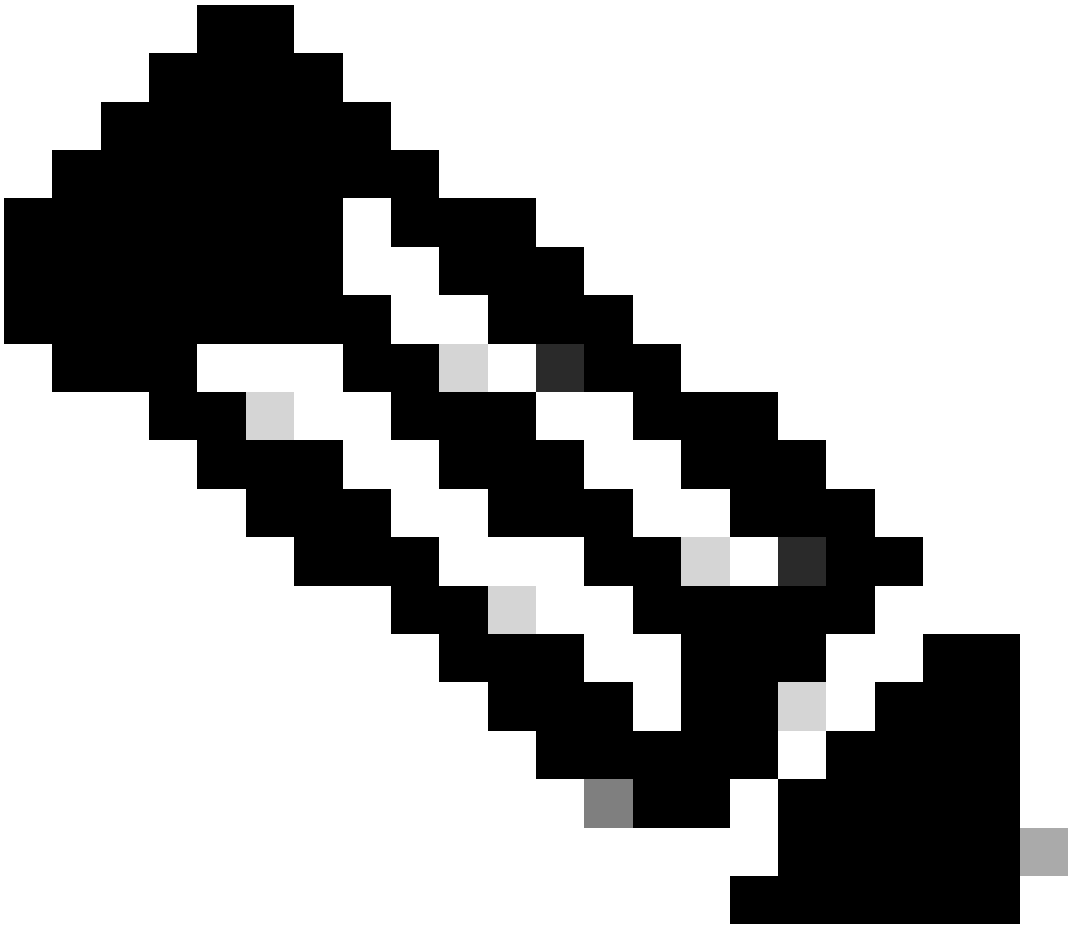
Il SIP è un protocollo basato su testo. Ciò significa che i messaggi SIP sono composti da testo leggibile, in modo simile al funzionamento di HTTP.

Il SIP è progettato per affrontare le funzioni di segnalazione e gestione delle sessioni all'interno di una rete di telefonia a pacchetti.

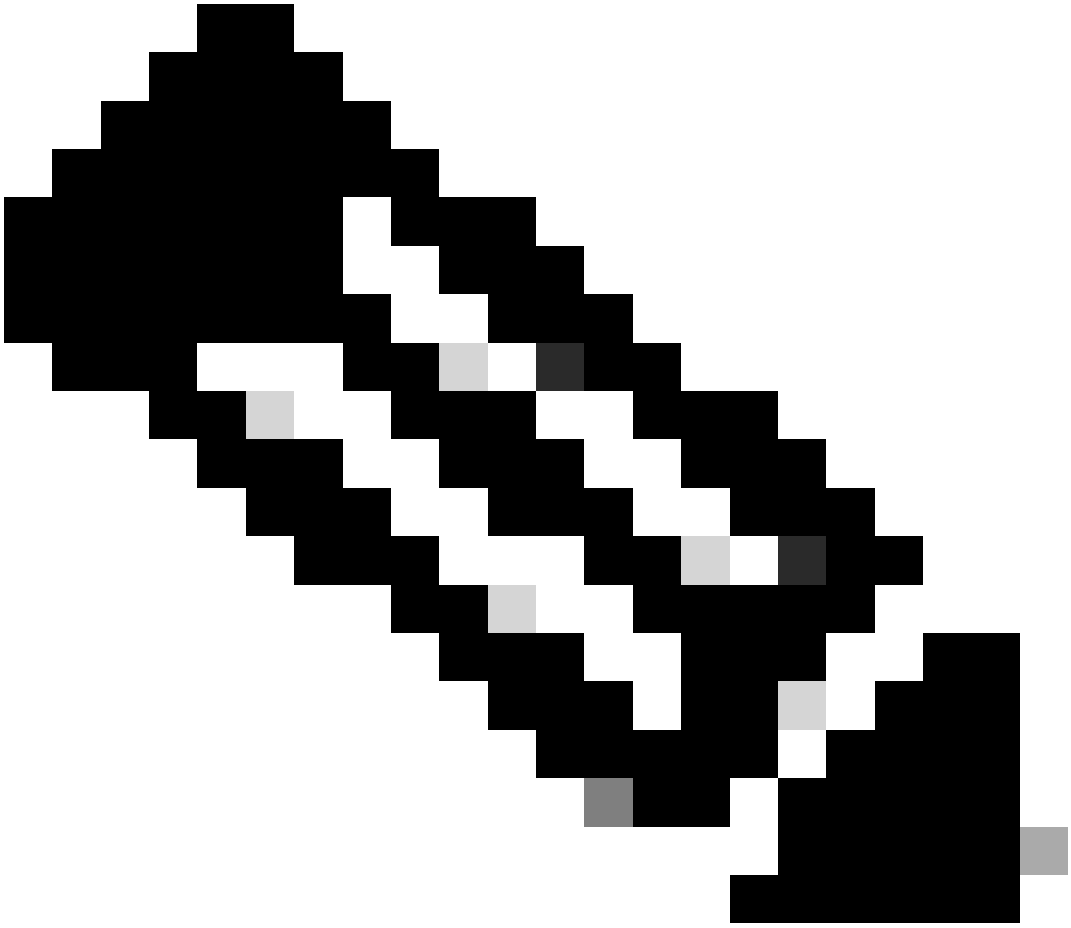
Il SIP può:

- crea una chiamata
- modificare una chiamata
- terminare una chiamata

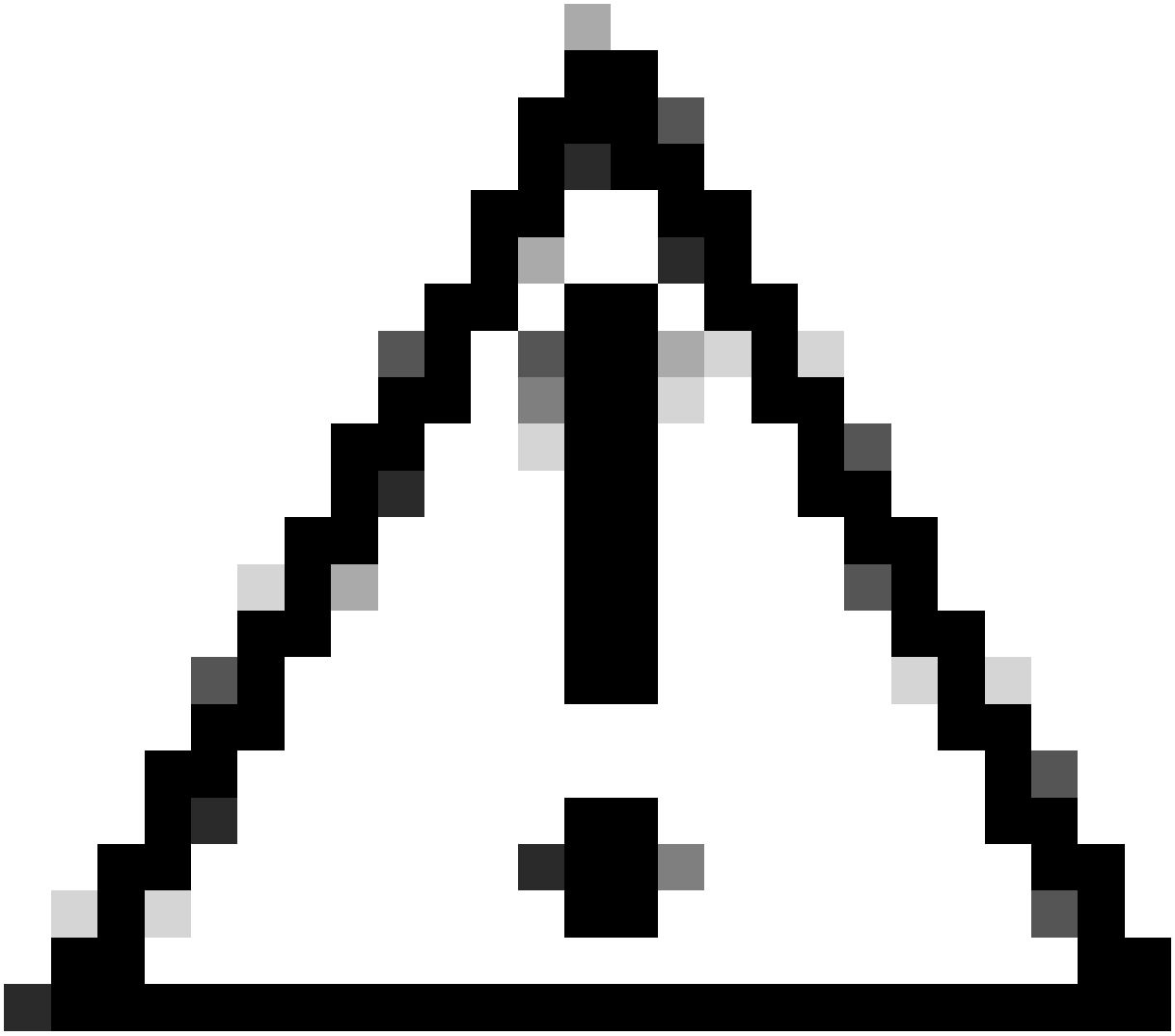
Il SIP può essere utilizzato sia UDP che TCP sulla porta 5060 standardizzata. E se il SIP è crittografato con Transport Layer Security (TLS), può utilizzare la porta standardizzata 5061.



> Nota: Quando la segnalazione SIP è crittografata, i pacchetti SIP effettivi non sono visibili nelle acquisizioni dei pacchetti sui dispositivi ASA o FTD. Tuttavia, è ancora possibile osservare l'handshake TCP seguito dall'handshake TLS tra i client SIP e i dispositivi server SIP.



Nota: L'ispezione SIP è abilitata per impostazione predefinita su Cisco Secure Firewall Threat Defense (FTD) e Secure Firewall Adaptive Security Appliance (ASA).



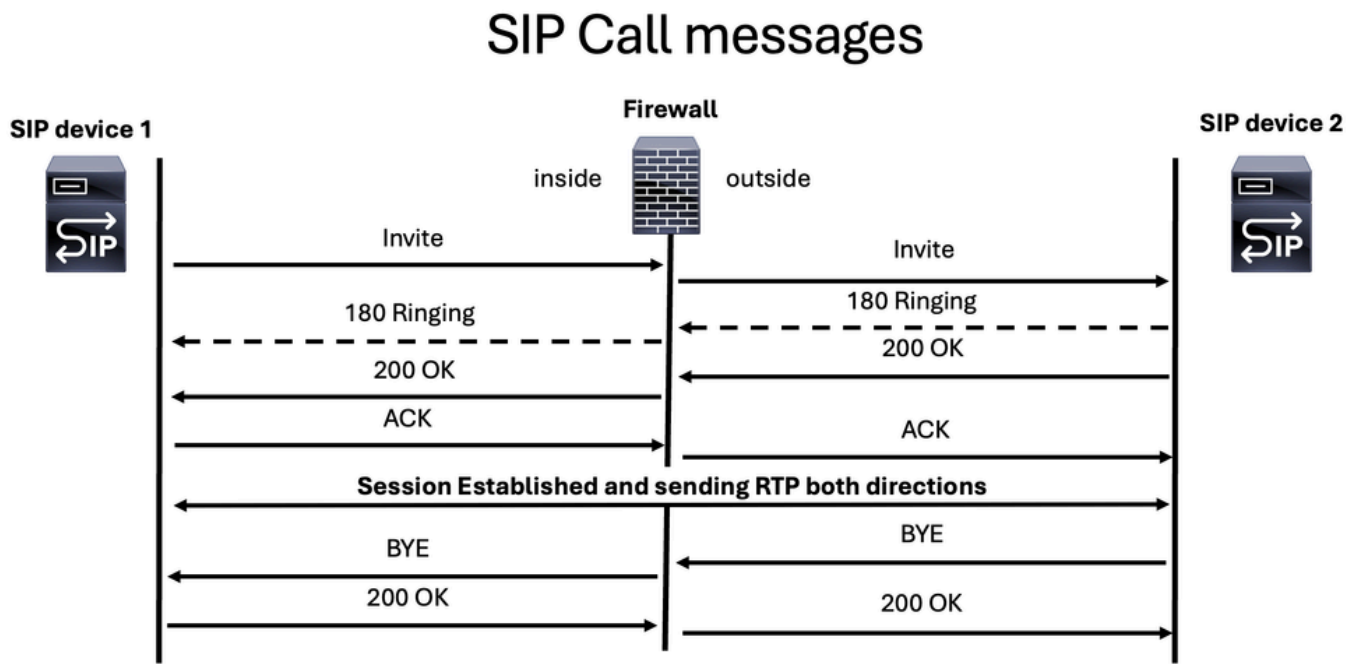
Attenzione: Verificare sempre quali porte vengono utilizzate per la segnalazione. Tenere presente che il protocollo SIP in genere utilizza le porte 5060 o 5061, ma alcune implementazioni possono discostarsi da questi standard e utilizzare porte diverse per il protocollo SIP.

Quando si risolve un problema di segnalazione SIP, è possibile individuare tre scenari:

- Messaggi di segnalazione di chiamata SIP
- messaggi SIP OPTION
- SIP REGISTER, messaggi

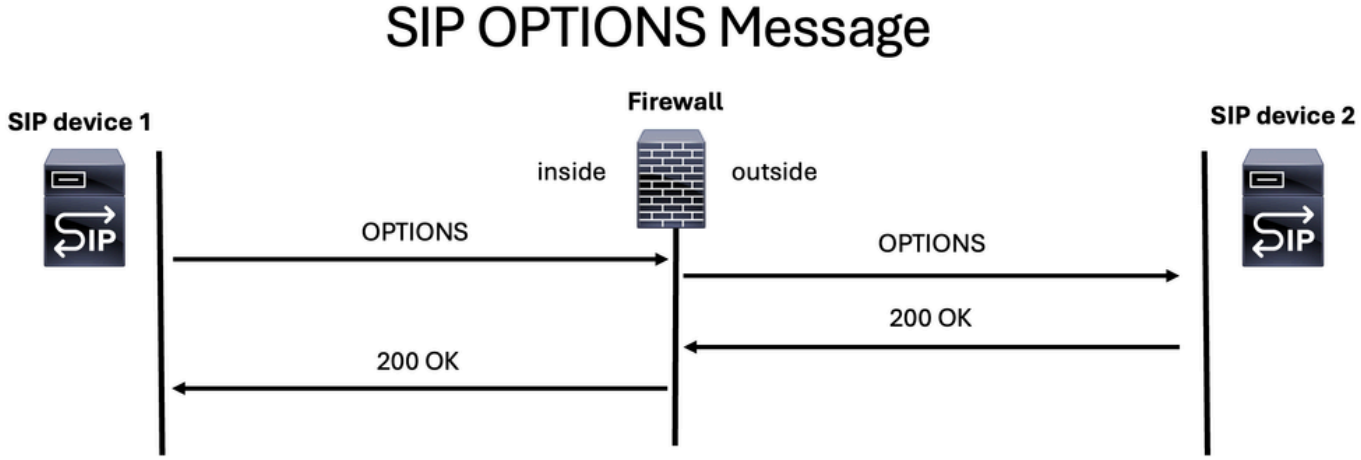
Messaggi di chiamata SIP

I messaggi SIP principali per stabilire e terminare una chiamata vocale sono i seguenti:



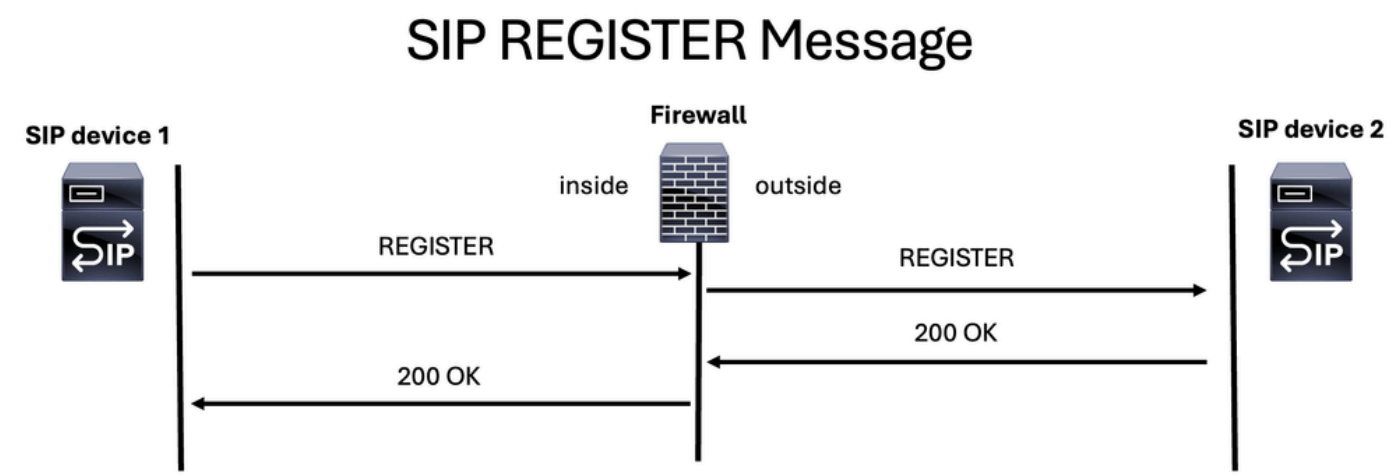
Messaggi SIP OPTION

I messaggi SIP OPTIONS (OPZIONI SIP) sono importanti per determinare se un dispositivo SIP è online e in grado di rispondere. È come eseguire il ping del messaggio ICMP ma sul mondo SIP.

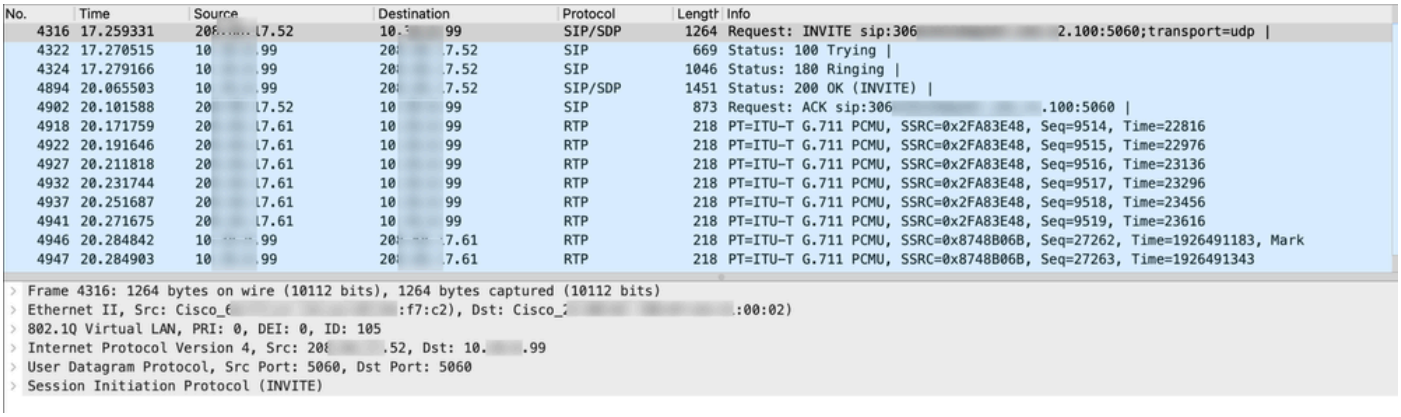


Messaggio REGISTER SIP

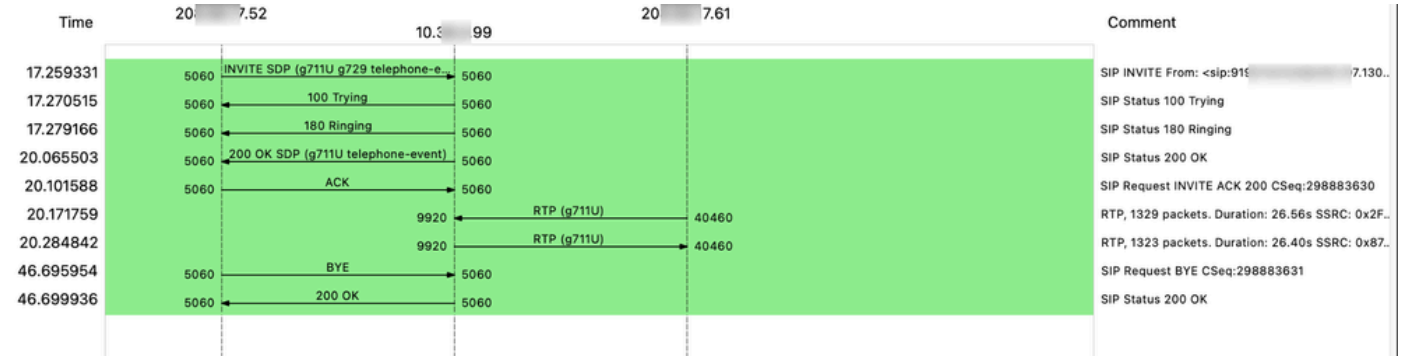
Un altro messaggio SIP che è possibile trovare durante una sessione di risoluzione dei problemi del firewall è il messaggio SIP REGISTER, che consente a un dispositivo di eseguire la registrazione a un server SIP.



Questa acquisizione pacchetto mostra le richieste e le risposte da due dispositivi SIP e anche il traffico (voce) multimediale:

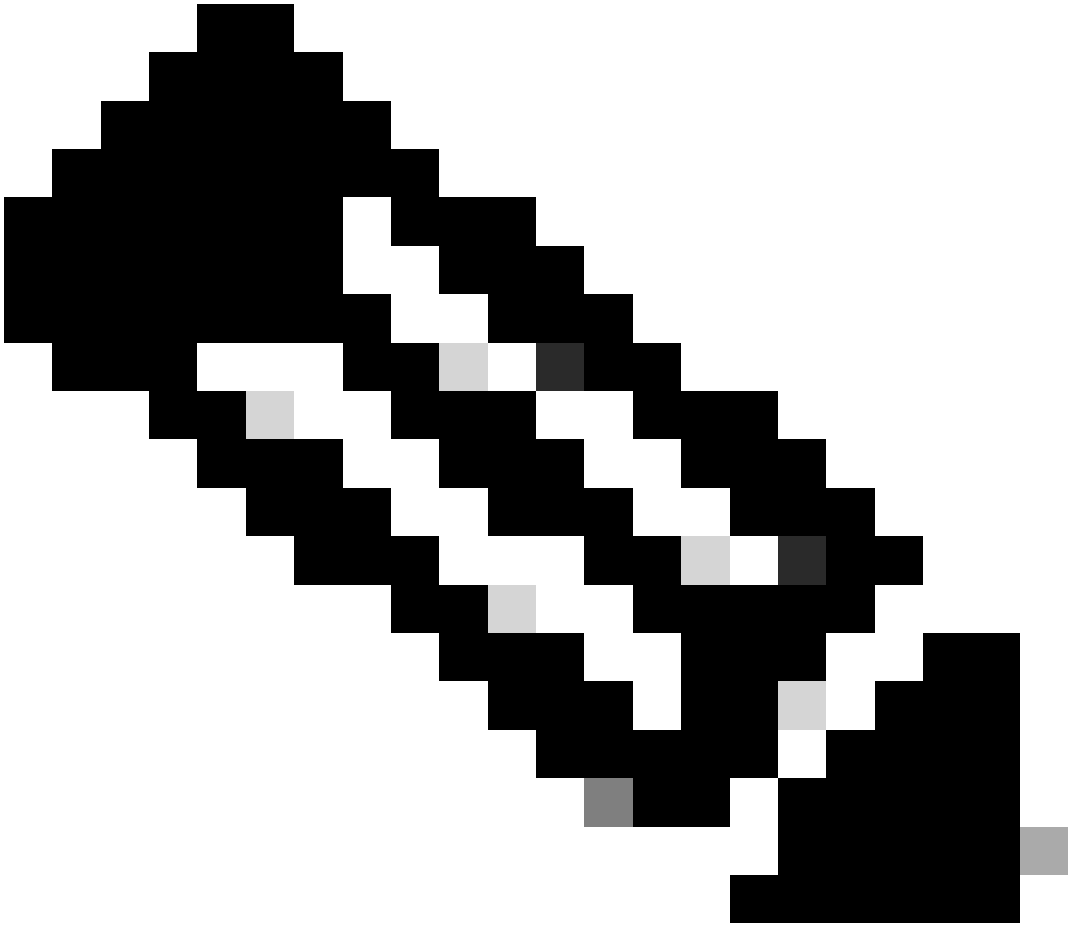


Questo è un esempio di flusso di segnali SIP e supporti RTP (voce):



Protocollo SDP (Session Description Protocol)

Session Description Protocol (SDP) è una rappresentazione standard utilizzata per descrivere i flussi multimediali per le sessioni multimediali. Non è dotato di supporto ma viene utilizzato per negoziare il tipo di supporto e il formato tra gli endpoint. Il protocollo SDP viene utilizzato in combinazione con il protocollo SIP (Session Initiation Protocol) per gestire e negoziare le caratteristiche dei supporti di una sessione.

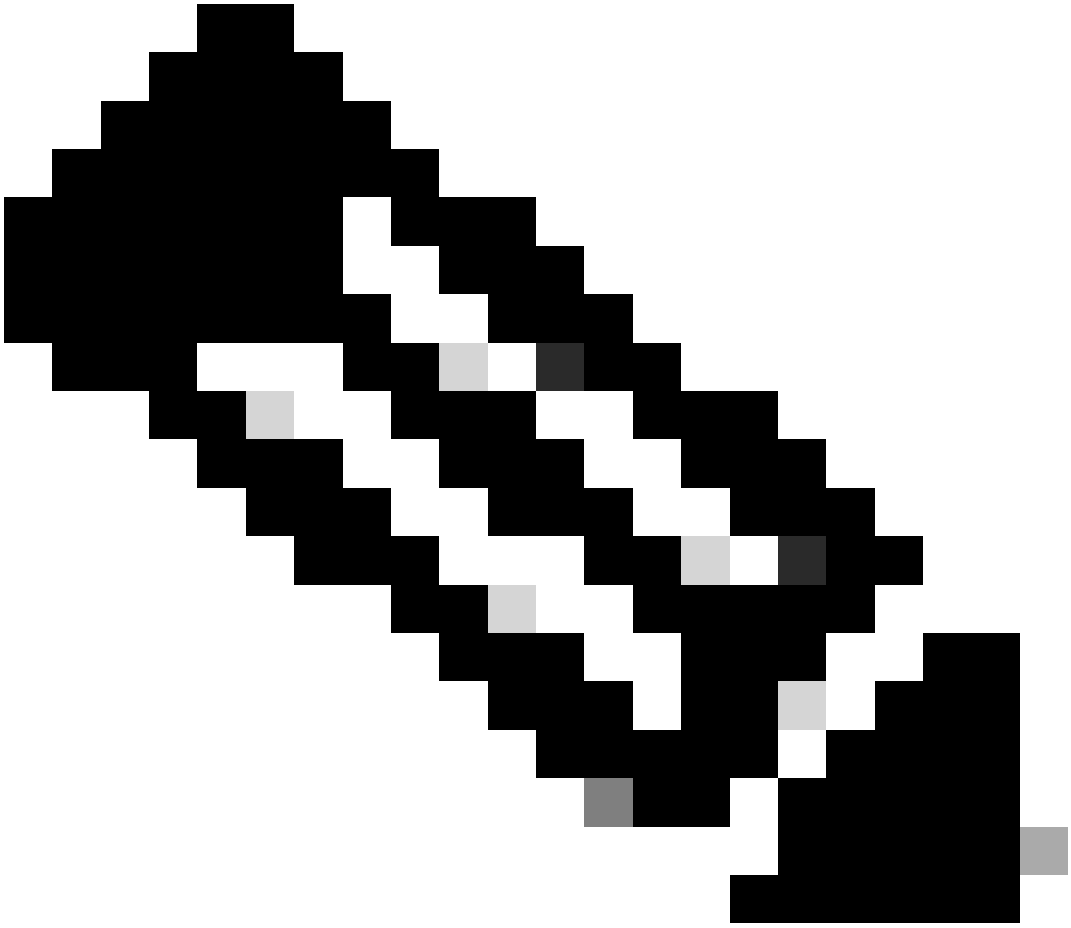


Nota: MGCP incorpora il concetto di SDP, che è utilizzato per lo stesso scopo.

Questo è un esempio di messaggio SDP all'interno di un protocollo 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
```



Nota: Alcuni messaggi SDP contengono questi parametri nell'esempio:

++c-IN IP4: Indirizzo IP del server multimediale

++m=audio: Ciò indica che il tipo di supporto è audio.

++8266: Questo è il numero della porta sulla quale viene inviato il flusso audio.

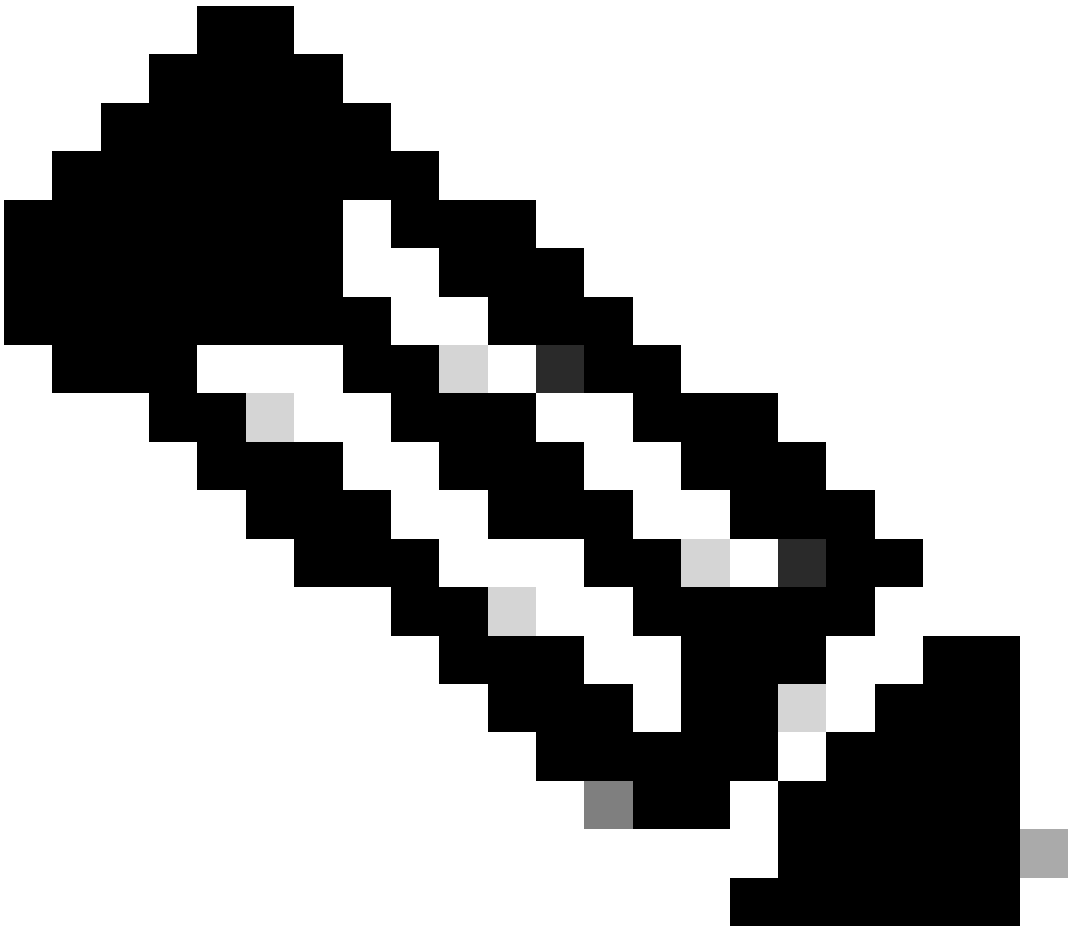
++RTP/AVP: Specifica il protocollo di trasporto, ovvero il protocollo RTP che utilizza il profilo audio/video (AVP).

++18 127: Questi sono i tipi di payload per i codec audio. Il tipo di payload 18 corrisponde in genere al codec G.729 e 127 è un tipo di payload dinamico che può essere assegnato a un codec in base alla negoziazione tra gli endpoint.

Il protocollo SDP (Session Description Protocol) è disponibile all'interno di diversi messaggi SIP, ad esempio: INVITE, 183 Session in Progress, 200 OK, ACK e così via. SDP è un metodo di risposta per lo scambio di funzionalità voce e/o video tra le parti. Per risolvere i problemi relativi

alle chiamate, è essenziale comprendere tre concetti principali:

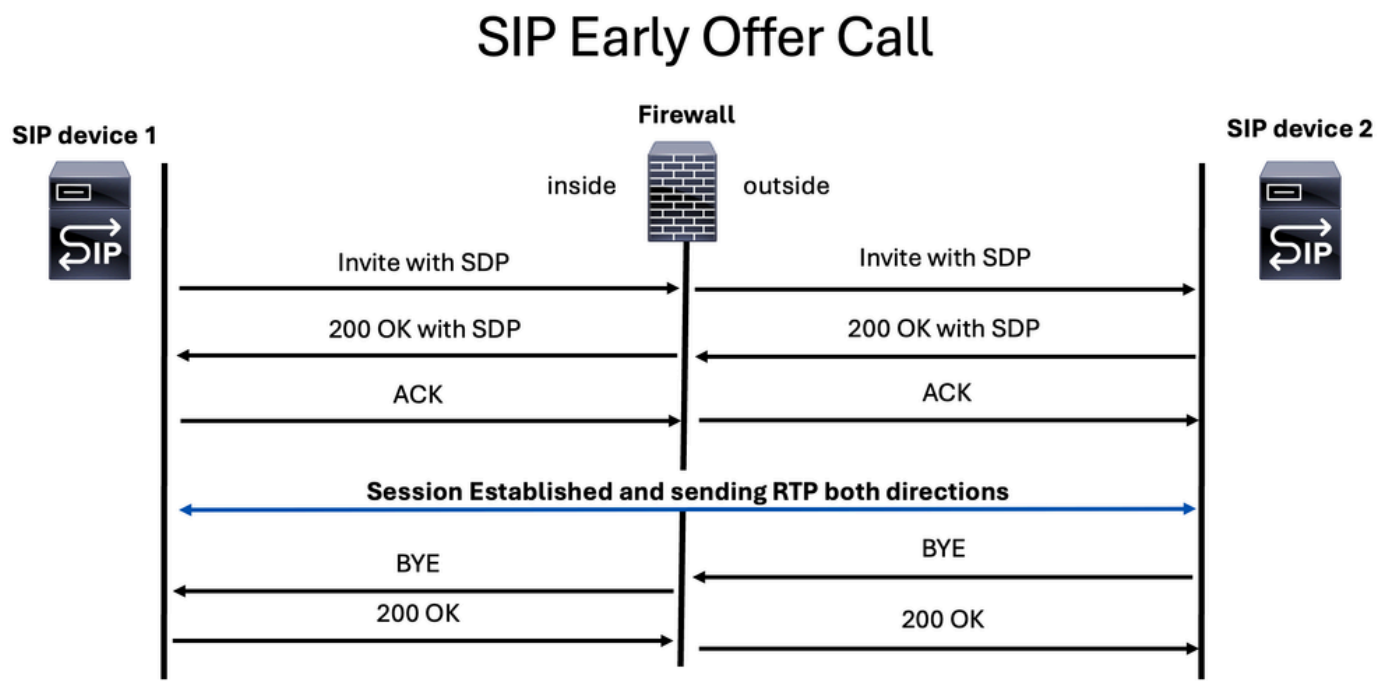
1. Offerta anticipata
2. Ritarda offerta
3. Early Media



> Nota: È fondamentale comprendere la destinazione dei messaggi SDP, in quanto la funzione di ispezione sul firewall può modificare gli indirizzi IP non solo nelle intestazioni SIP ma anche nella sezione SDP.

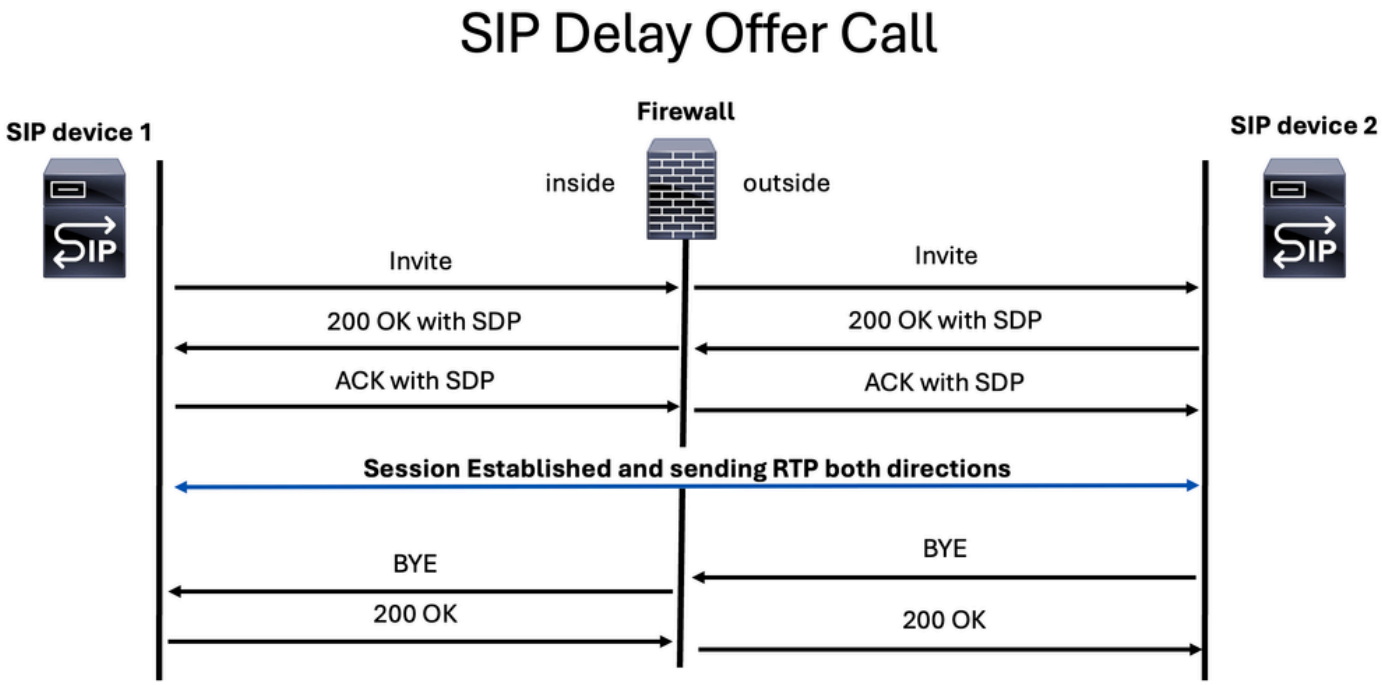
Offerta anticipata

Qui i parametri multimediali su SDP si trovano nei messaggi INVITE e 200 OK SIP.



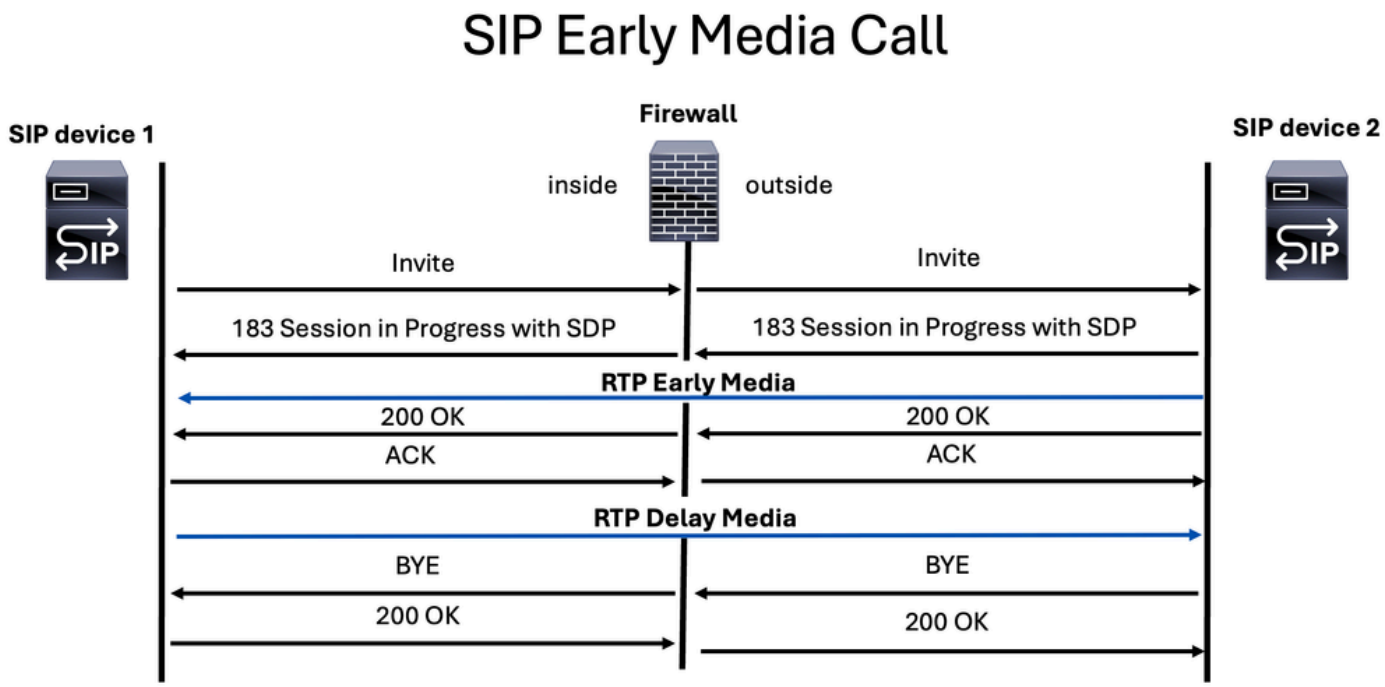
Ritarda offerta

Con questo metodo, l'SDP si trova su 200 messaggi OK e ACK SIP.



Early Media

I primi file multimediali vengono trasmessi tramite uno specifico messaggio SIP noto come risposta 183 Session Progress. Questo messaggio include il protocollo SDP (Session Description Protocol) contenente i parametri multimediali per il destinatario della chiamata. Viene comunemente utilizzato dai gestori telefonici e dai provider SIP per inviare messaggi vocali automatici o altri supporti al chiamante prima che la chiamata venga connessa ufficialmente.

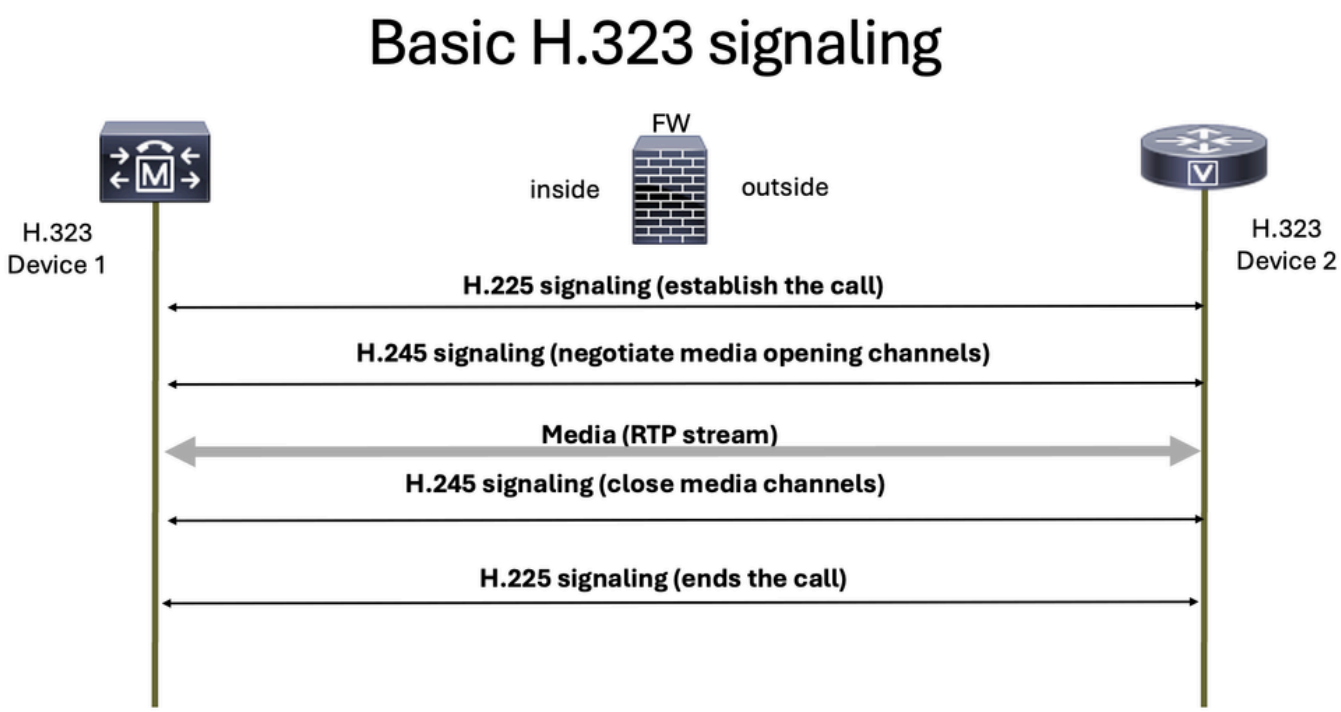


H.323

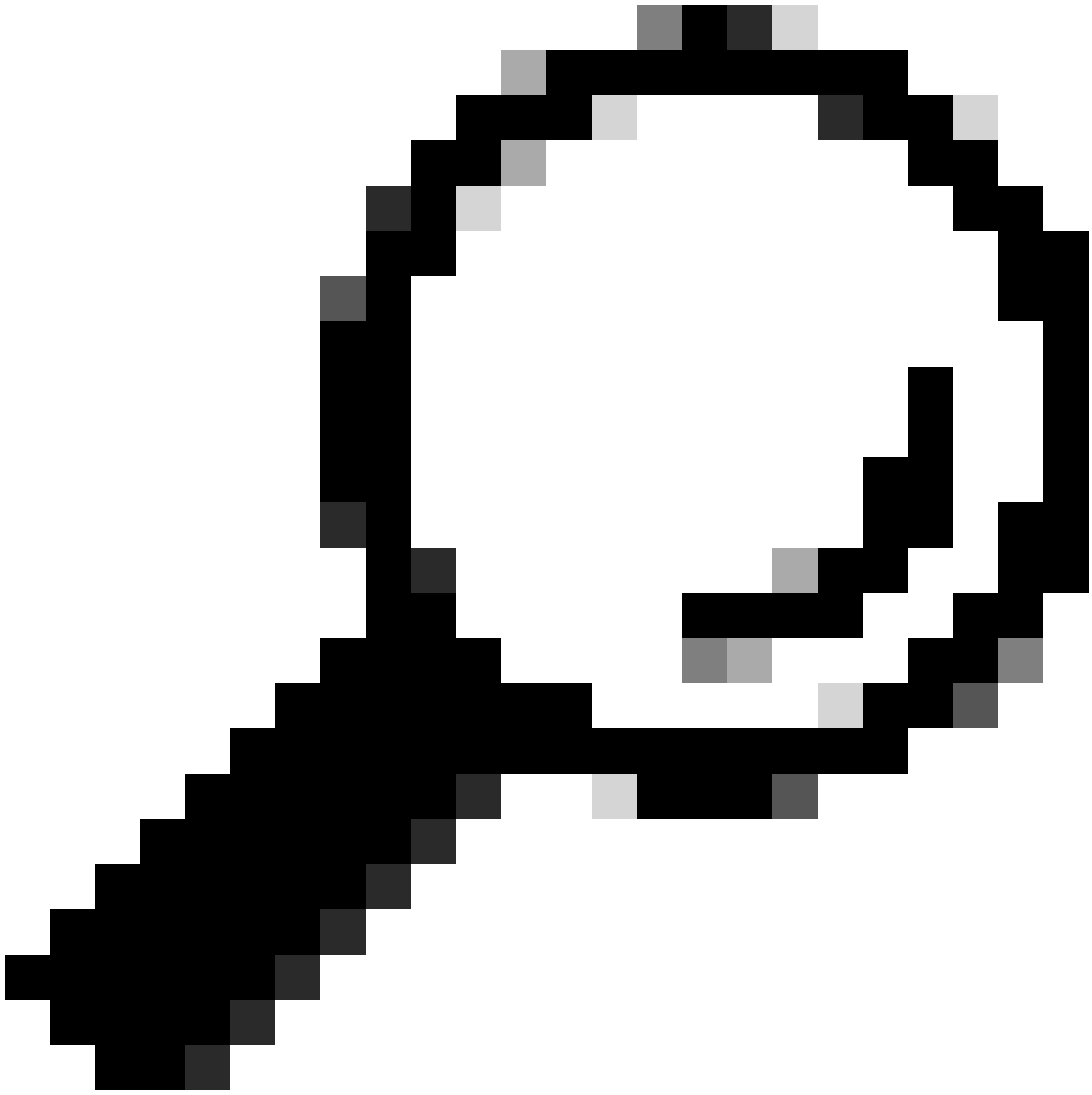
H.323 è un set di protocolli definiti dall'Unione Internazionale delle Telecomunicazioni (ITU) per la comunicazione voce, video e dati su reti a commutazione di pacchetto, come Internet.

Il protocollo H.323 è composto da due componenti principali:

1. H.225: Gestisce la segnalazione delle chiamate, incluse la configurazione e la terminazione delle chiamate.
2. H.245: Questa funzione è responsabile dello scambio di funzionalità e dell'apertura e chiusura dei canali audio e video.



Le porte utilizzate dal protocollo di segnalazione H.323 sono 1718, 1719 e 1720.

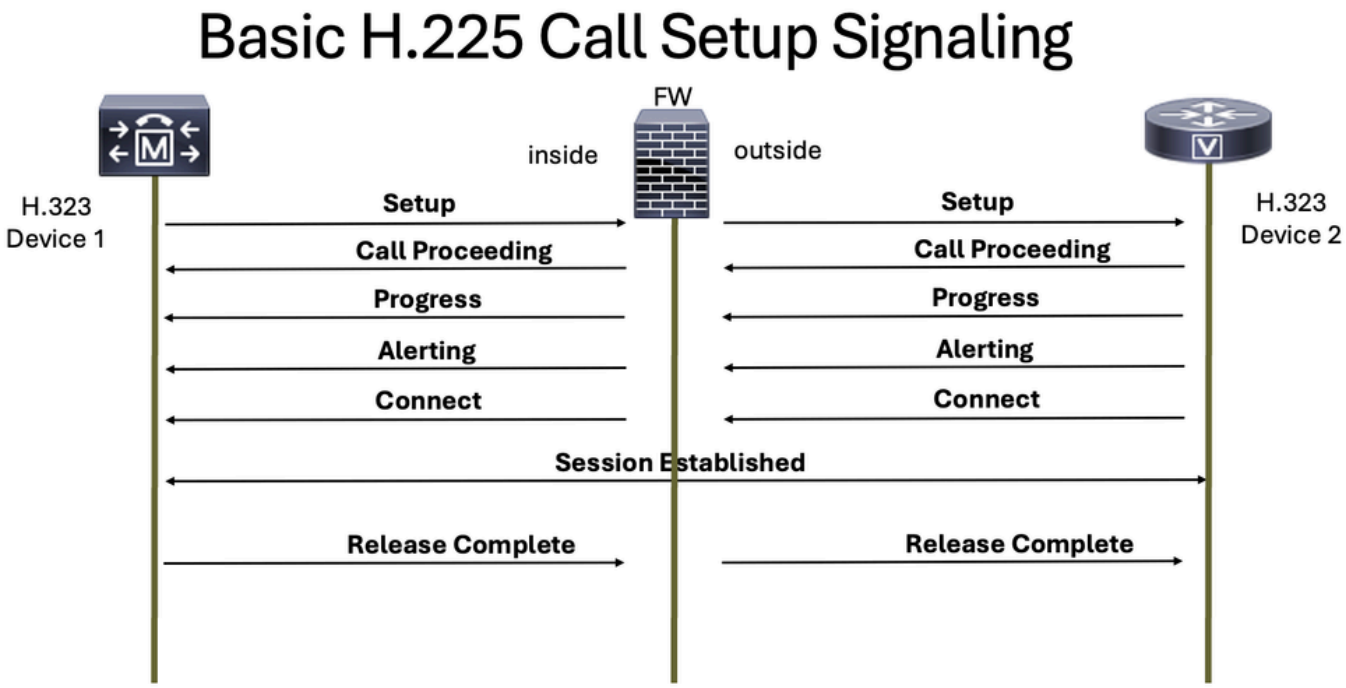


Suggerimento: Le comunicazioni sicure basate sul protocollo H.323 possono presentare problemi nel passaggio da UDP a TCP a causa dell'uso di TLS per la crittografia, che può causare il blocco erroneo della connessione da parte di un firewall come attività sospetta. Per questo motivo è fondamentale configurare il firewall in modo da consentire traffico UDP e TCP sia per gli endpoint o i server H.323.

H.323 è un protocollo che ha due modalità operative: avvio lento e avvio rapido.

H.225

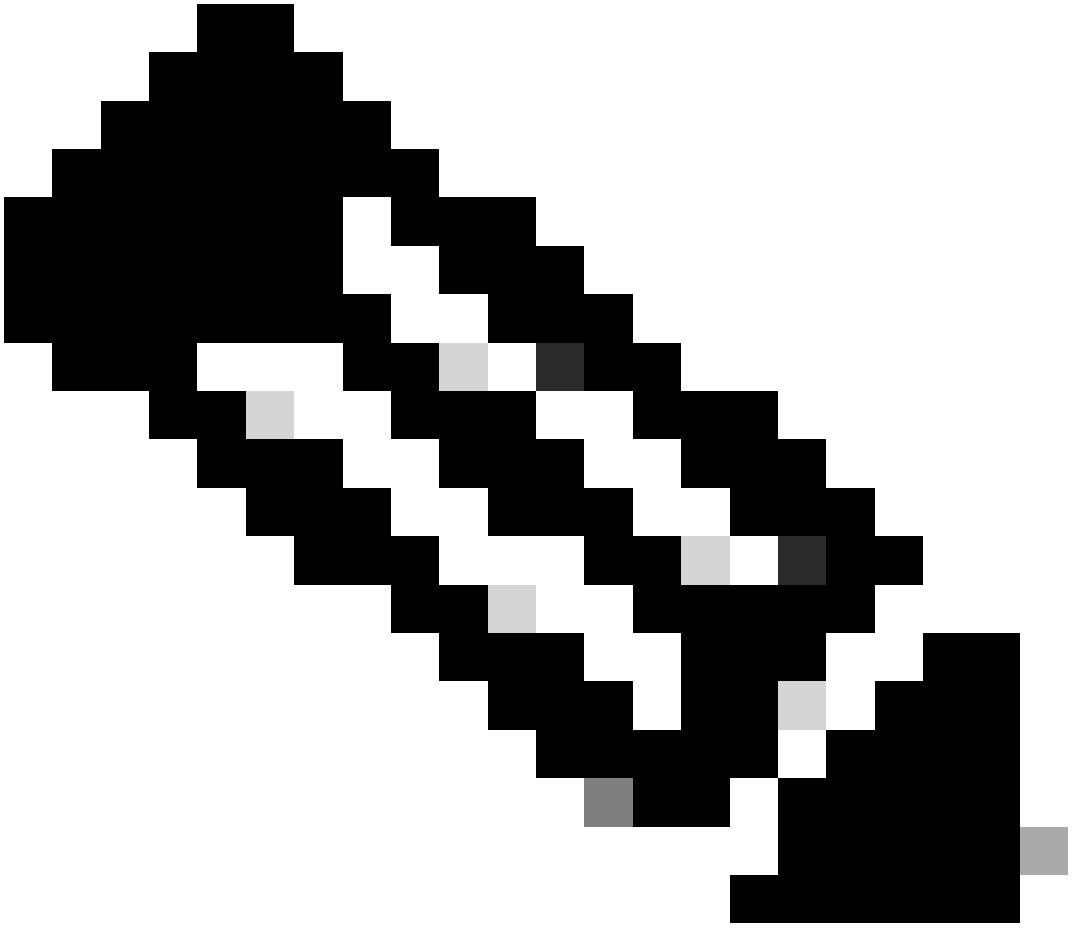
Questo protocollo è responsabile dell'impostazione della chiamata e dell'interruzione di una chiamata vocale quando una delle parti si blocca.



H.245

H.245 offre le seguenti funzionalità:

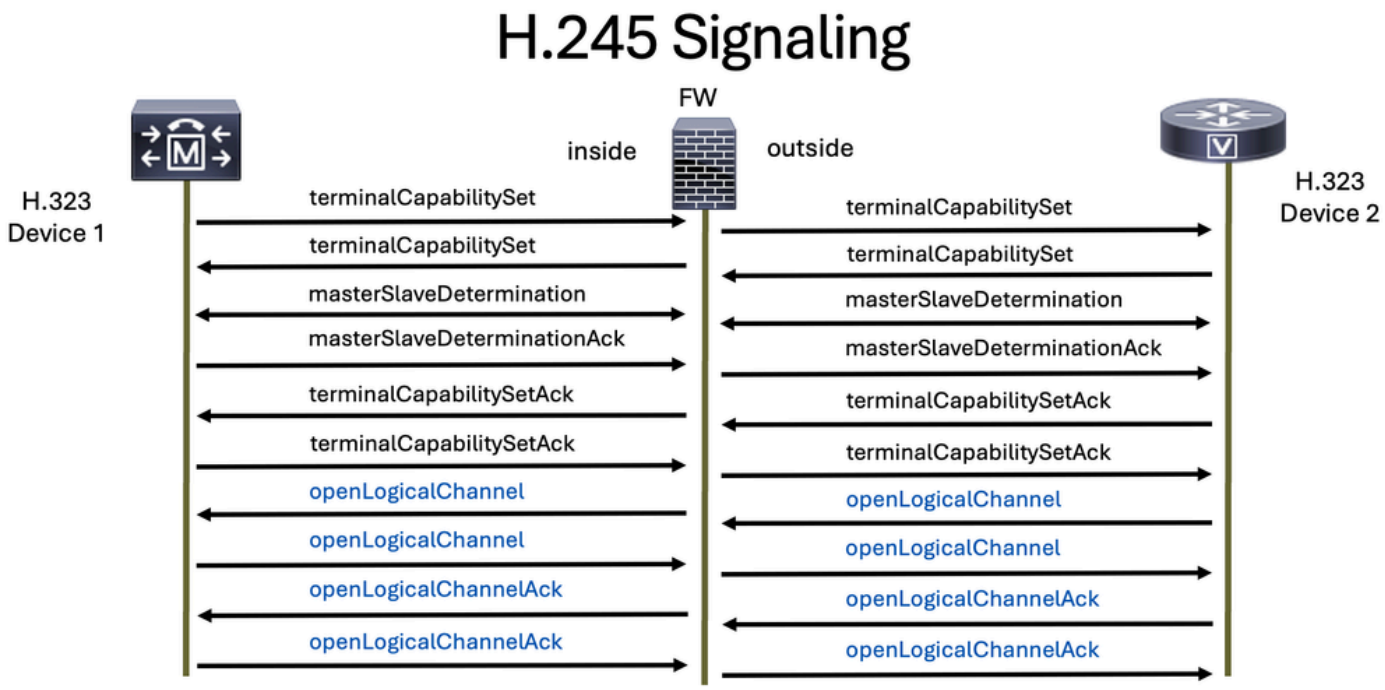
- Scambio funzionalità terminale
- Determinazioni master/slave
- Segnalazione canale logico



Nota: I termini Master e Slave utilizzati in questo documento sono codificati nel protocollo originale H.323 e non riflettono le politiche o i valori della nostra azienda. Ci impegniamo a promuovere un linguaggio inclusivo e rispettoso.

Il protocollo H.245 viene inviato dopo aver ricevuto il messaggio di connessione H.225.

Questo protocollo aiuta a determinare quale protocollo vocale viene utilizzato per il protocollo RTP e viene specificato sul canale logico di apertura e di chiusura dei relativi messaggi.

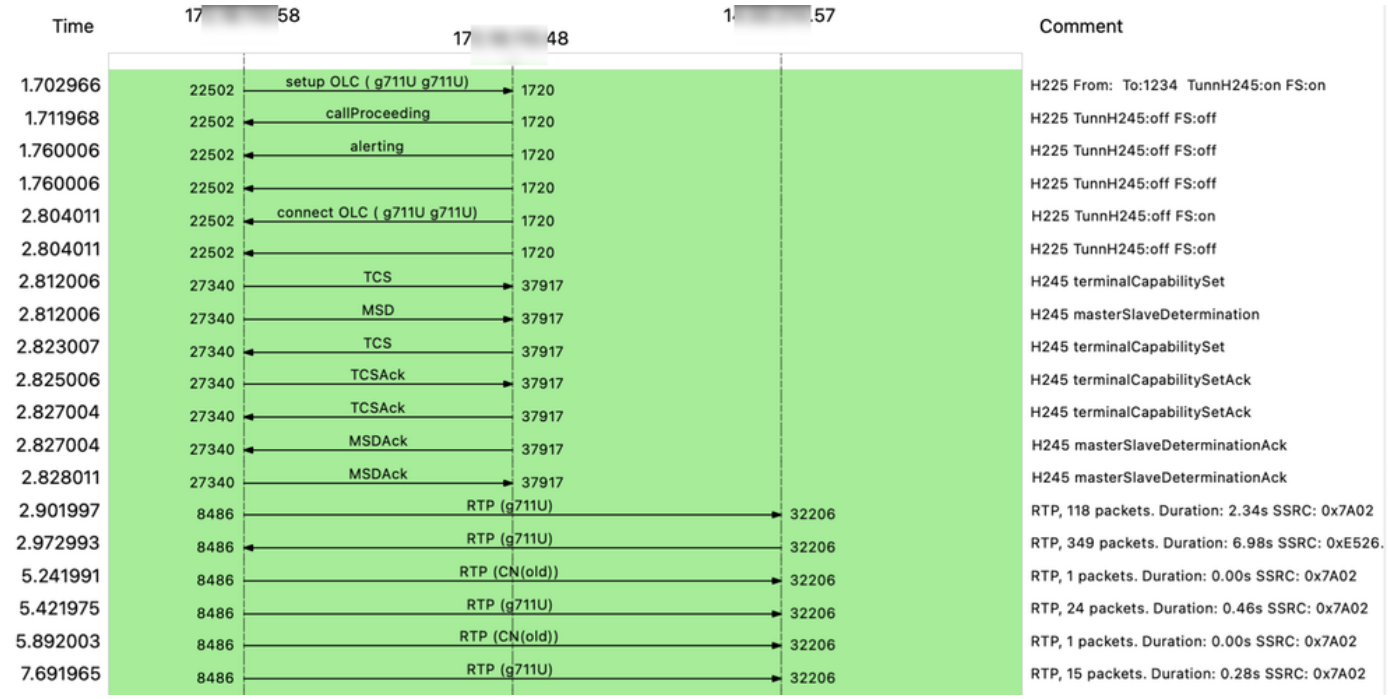


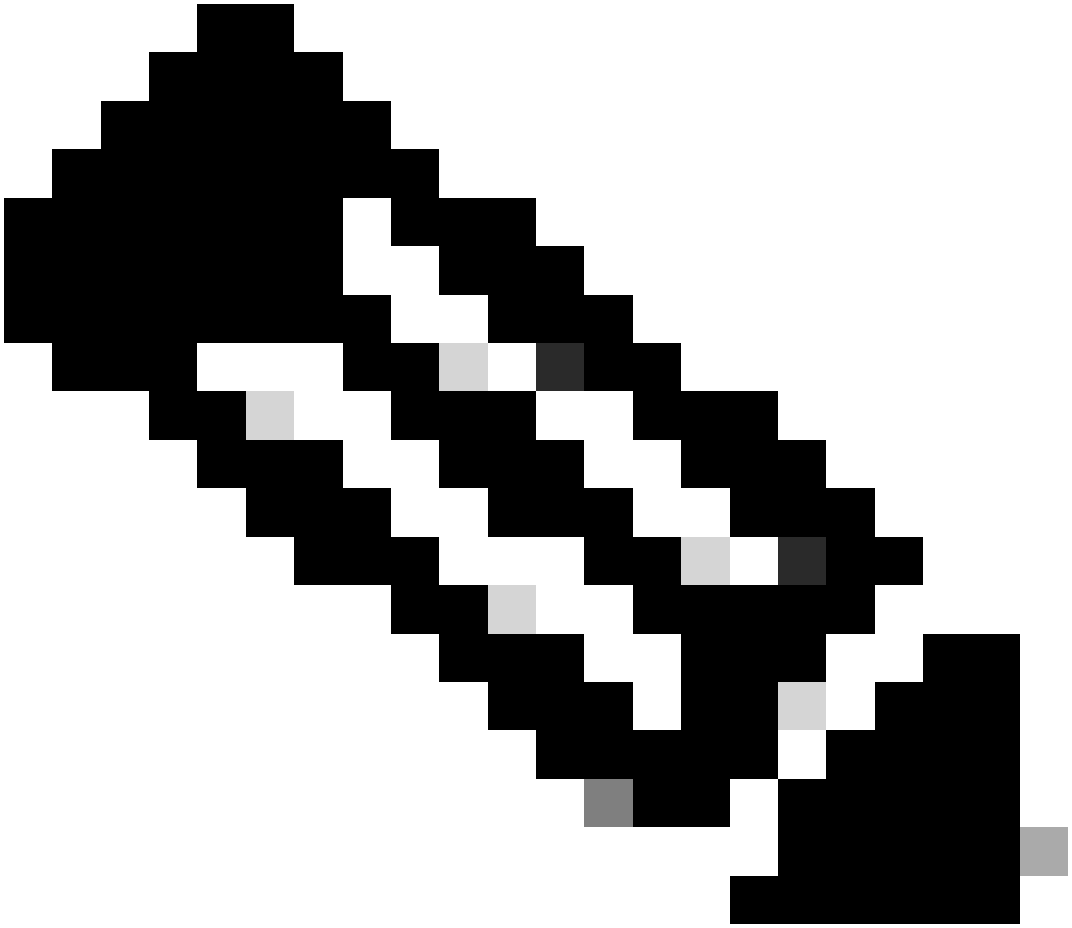
Questa acquisizione mostra le richieste e le risposte da due dispositivi H.323 con H.225 e H.245 e il traffico (voce) dei supporti:

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
```

Questo è un esempio di flusso di segnali H.323 con H.225 e H.245 e supporti RTP (voce):

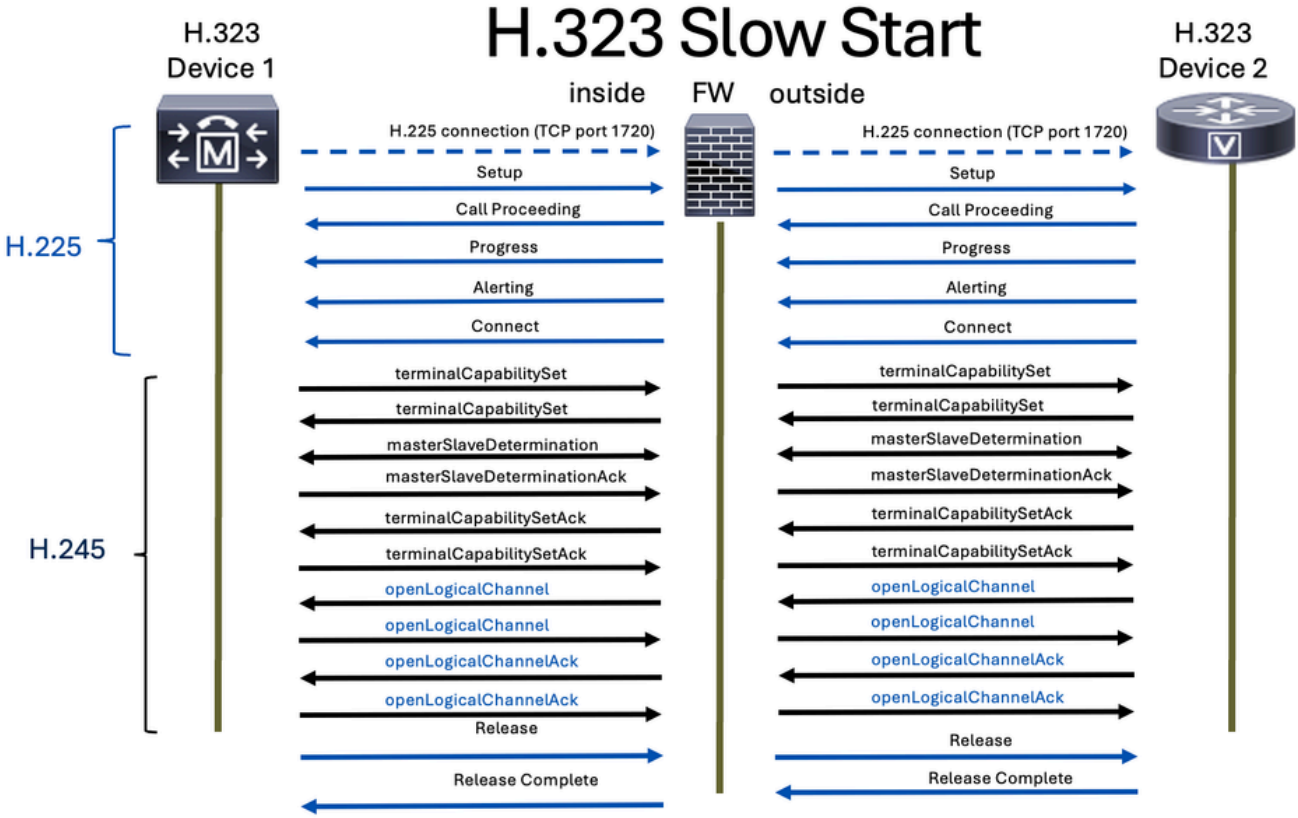

Time
Comment
1.702966 22502 setup OLC (g711U g711U) 1720 H225 From: To:1234 TunnH245:on FS:on
1.711968 22502 callProceeding 1720 H225 TunnH245:off FS:off
1.760006 22502 alerting 1720 H225 TunnH245:off FS:off
1.760006 22502 1720 H225 TunnH245:off FS:off
2.804011 22502 connect OLC (g711U g711U) 1720 H225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



Nota: L'ispezione H.323 è abilitata per impostazione predefinita su Cisco Secure Firewall Threat Defense (FTD) e Secure Firewall Adaptive Security Appliance (ASA).

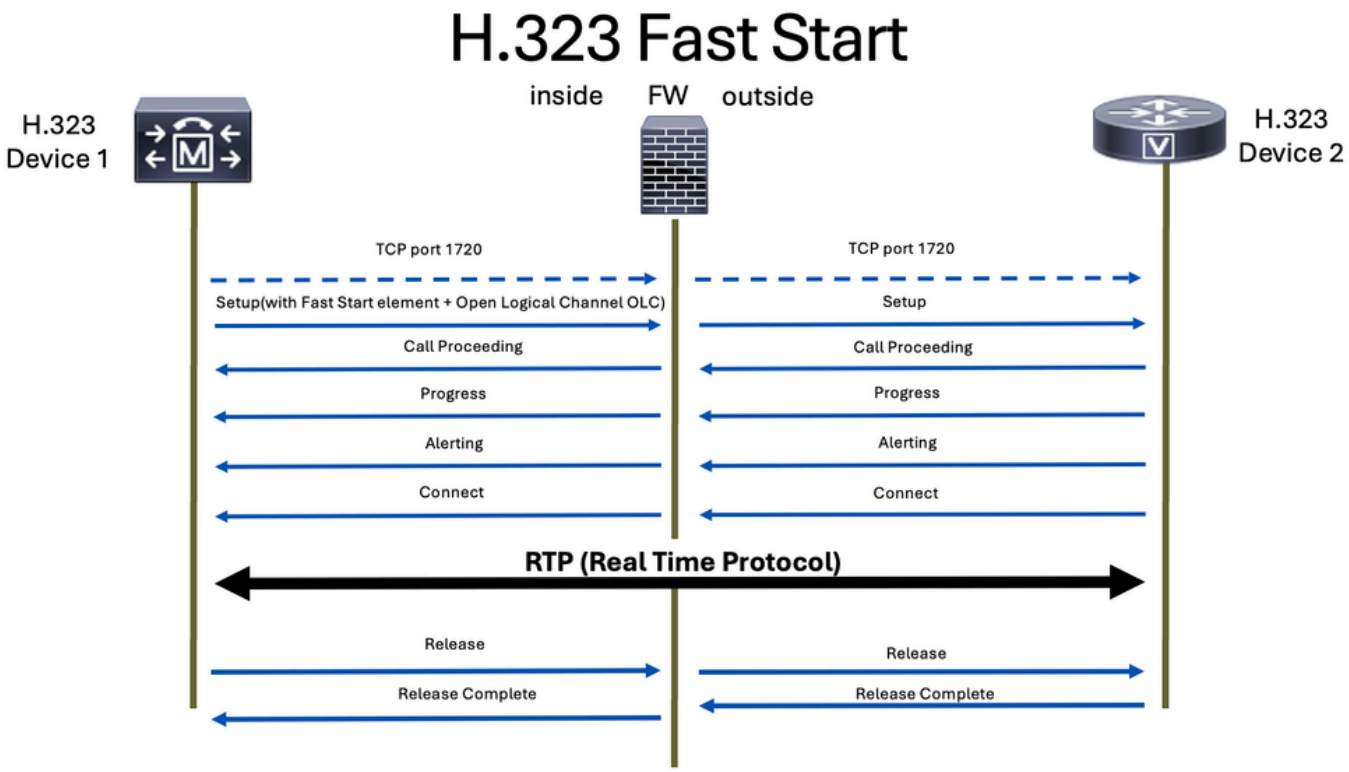
Avvio lento

In modalità di avvio lento, il processo di configurazione delle chiamate prevede diverse fasi di segnalazione prima che i canali multimediali vengano stabiliti. Le fasi includono l'installazione, l'elaborazione delle chiamate, gli avvisi e la connessione. Dopo questa procedura, la negoziazione dei supporti H.245 viene eseguita separatamente. Ciò significa che i canali multimediali non vengono stabiliti fino al completamento della segnalazione di chiamata iniziale, il che può comportare un tempo di configurazione più lungo.



Avvio rapido

Al contrario, la modalità di avvio rapido consente di eseguire la negoziazione dei supporti all'interno del messaggio di installazione iniziale. Ciò significa che i canali multimediali possono essere stabiliti più rapidamente, poiché la negoziazione viene effettuata nell'ambito della configurazione iniziale della chiamata. Fast Start semplifica il processo riducendo il numero di messaggi scambiati e la quantità di elaborazione necessaria prima che i canali multimediali vengano stabiliti.

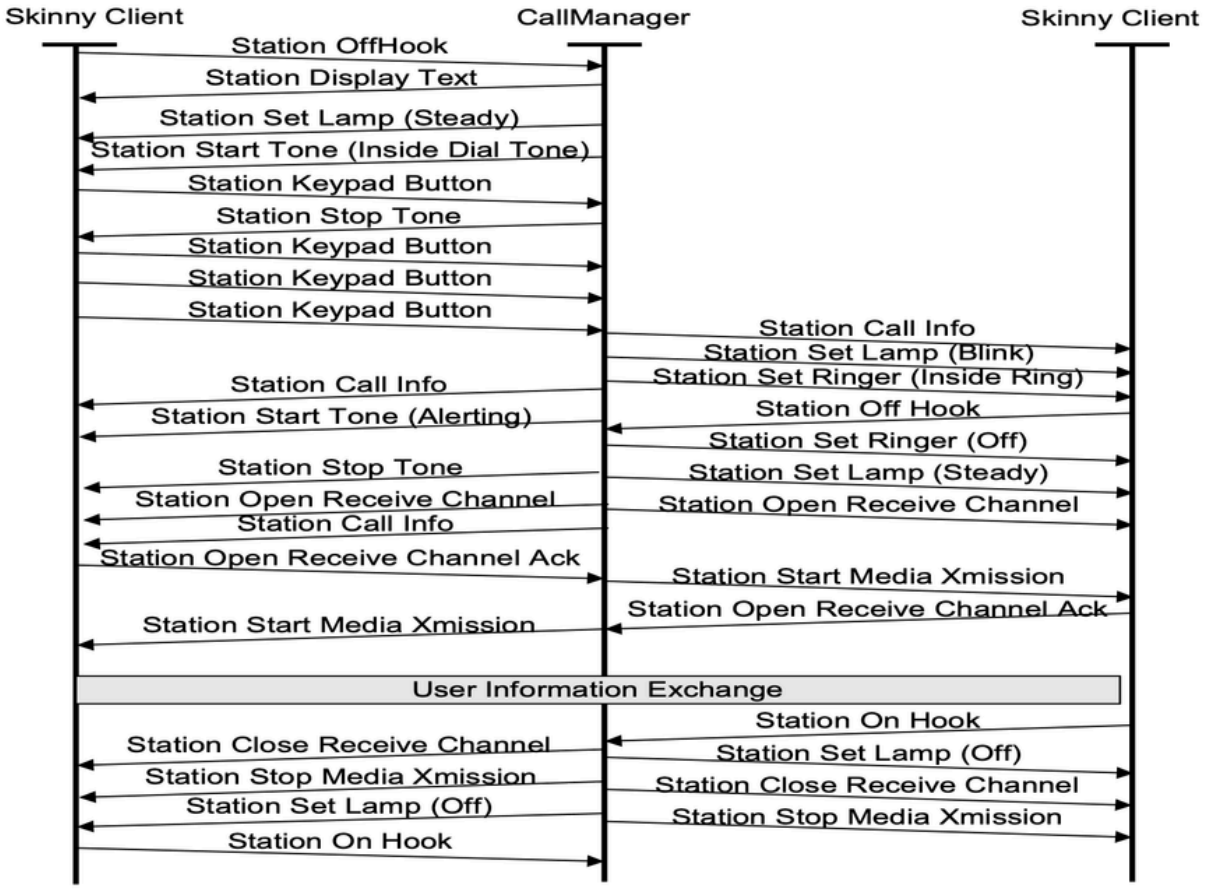


SCCP

Il protocollo SCCP (Skinny Client Control Protocol), spesso denominato semplicemente Skinny, è un protocollo di segnalazione proprietario di Cisco. È utilizzato principalmente dai router Cisco Unified Communications Manager (CUCM), Cisco Unified Communications Manager Express (CME) e dai telefoni IP Cisco per facilitare la configurazione e il controllo delle chiamate.

Il protocollo SCCP usa il protocollo TCP sulla porta 2000 per il protocollo SCCP non sicuro e la porta 2443 per il protocollo SCCP sicuro.

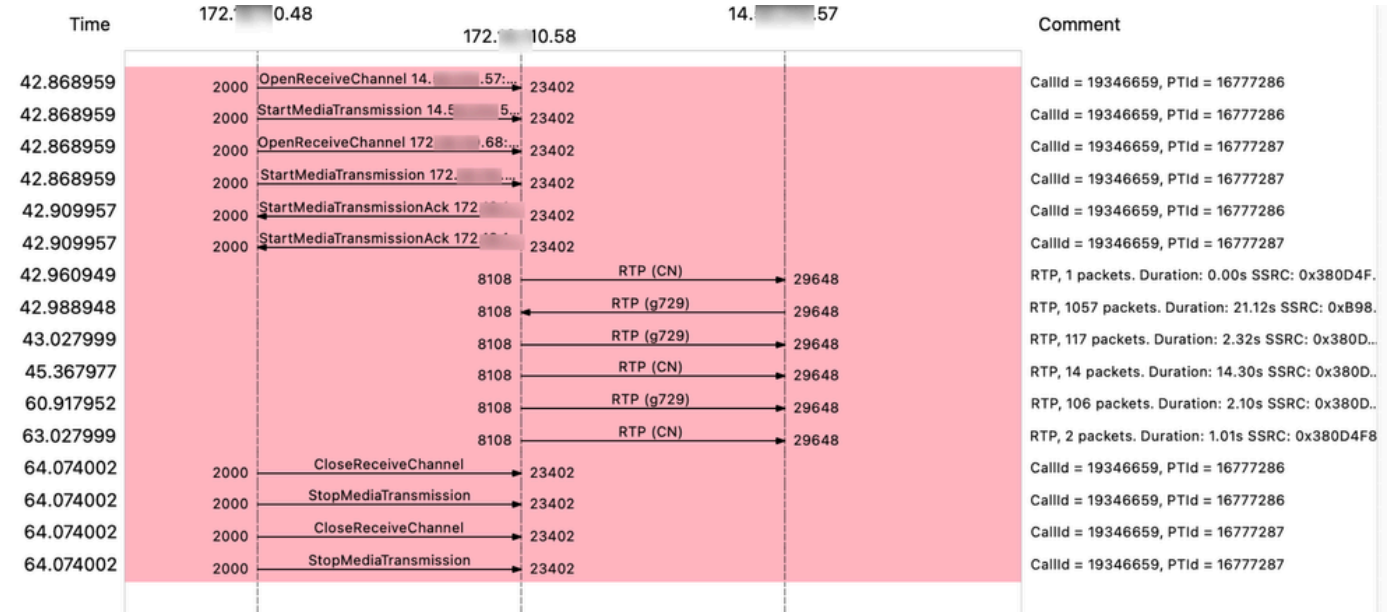
Di seguito sono riportati i messaggi SCCP comuni che è possibile trovare in una chiamata SCCP:

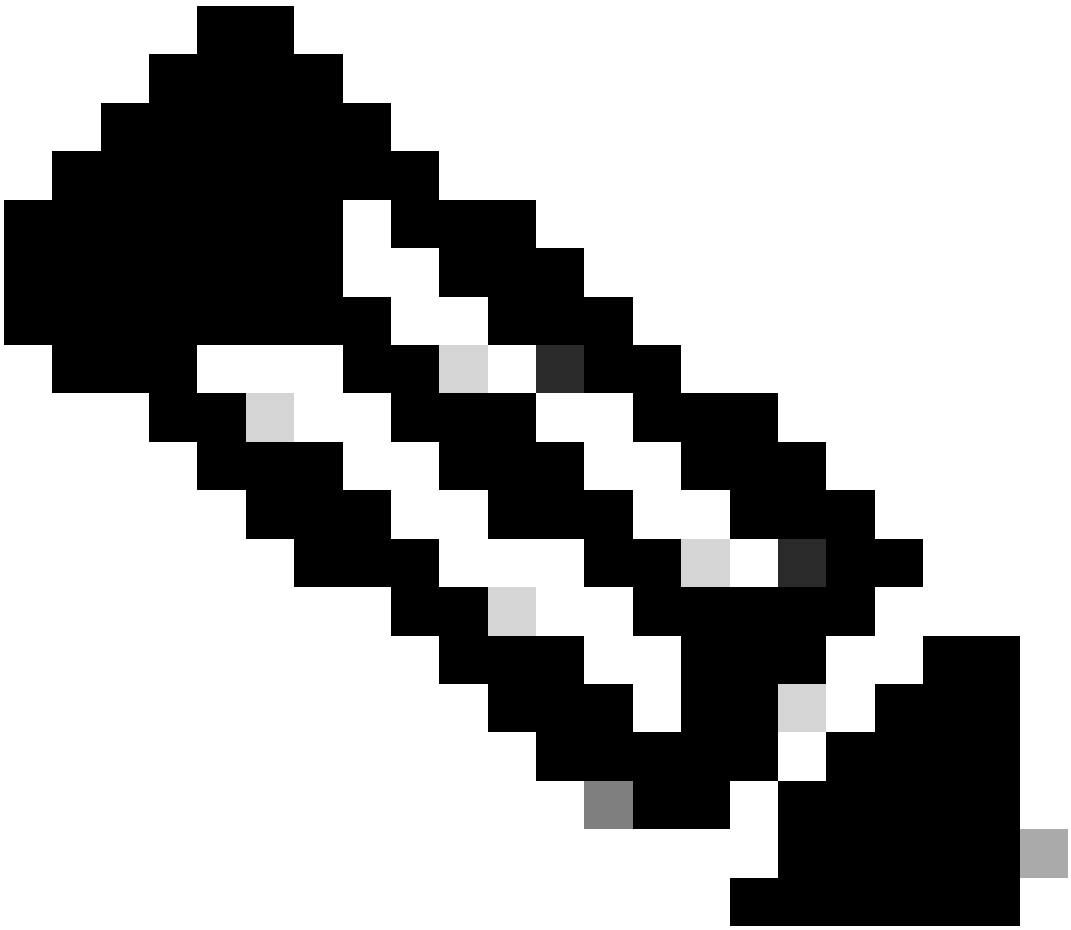


Questa acquisizione mostra le richieste e le risposte da due dispositivi SCCP e il traffico (voce) multimediale:

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

Questo è un esempio di flusso di segnali SCCP e supporti RTP (voce):





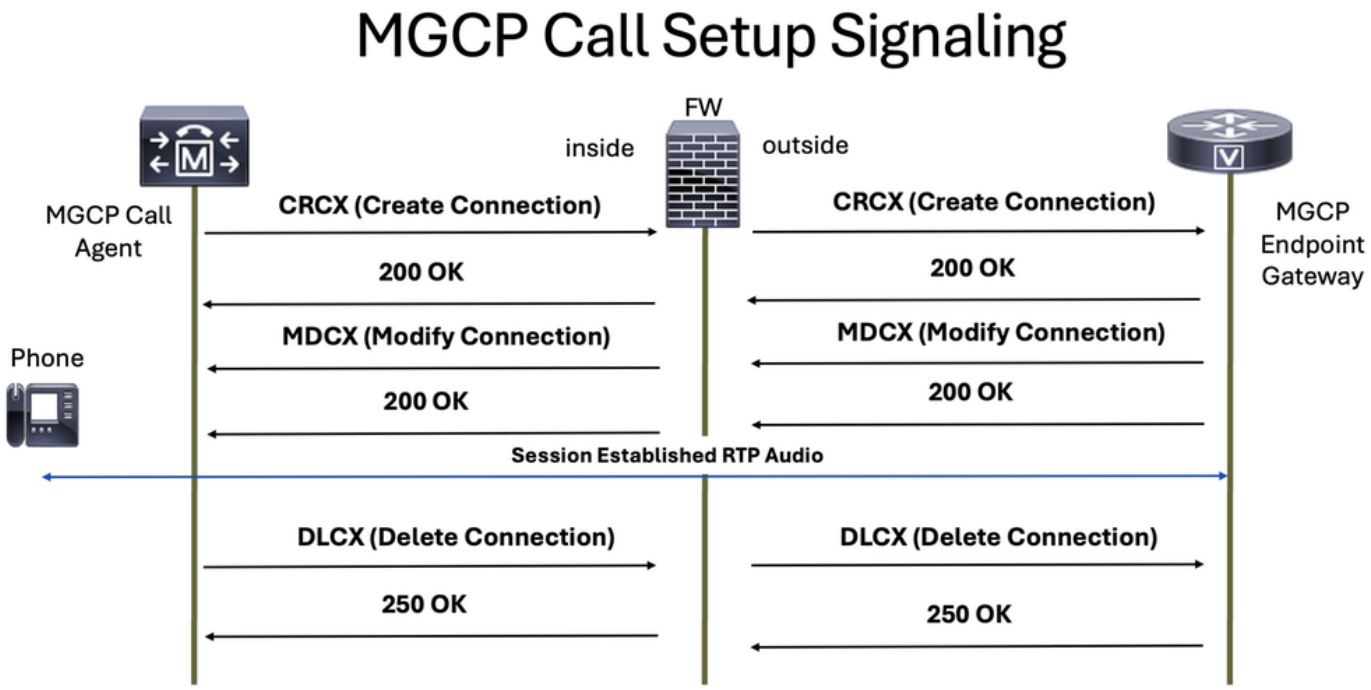
Nota: L'ispezione SCCP è abilitata per impostazione predefinita su Cisco Secure Firewall Threat Defense (FTD) e Secure Firewall Adaptive Security Appliance (ASA).

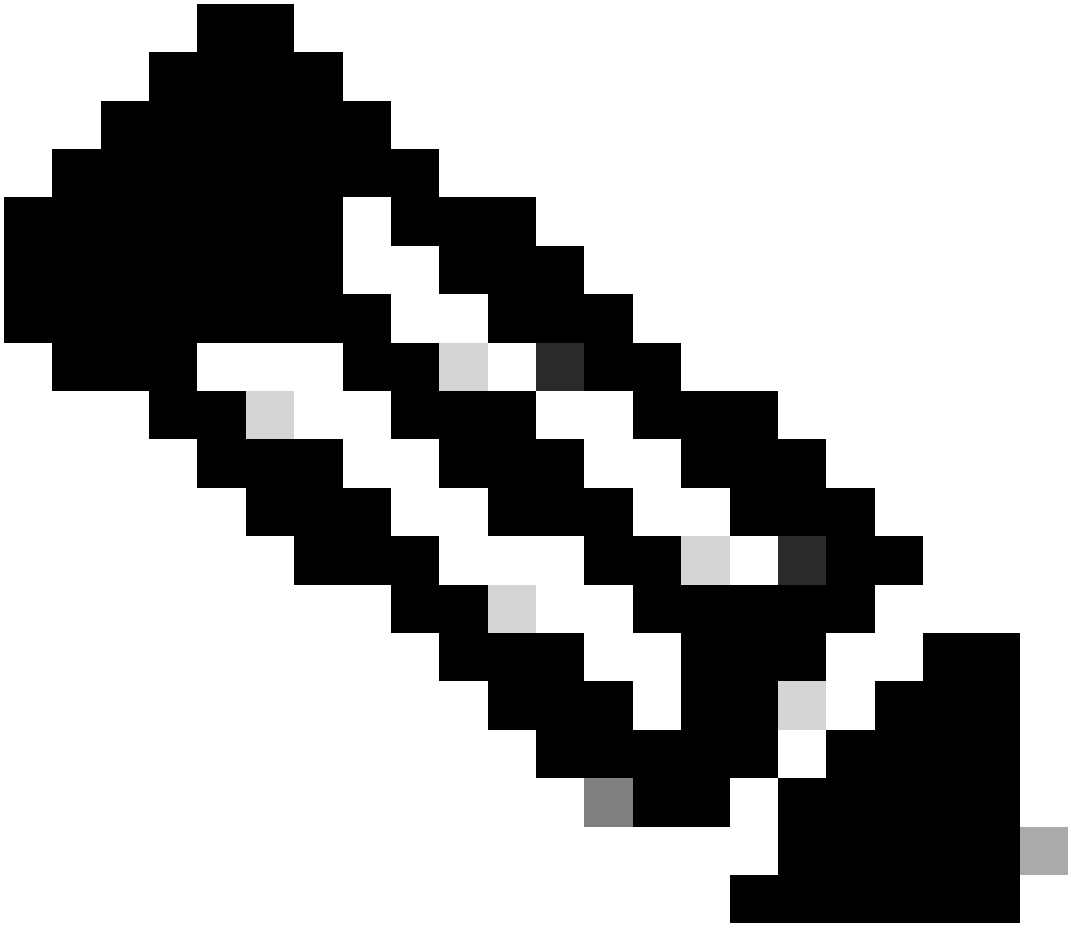
MGCP

MGCP (Media Gateway Control Protocol) è un protocollo utilizzato per il controllo delle chiamate VoIP da un dispositivo di controllo delle chiamate, ad esempio CUCM.

Il protocollo di segnalazione MGCP è definito sulla RFC 2705 e usa le porte TCP 2428 e UDP 2427 per la comunicazione.

I pacchetti normali MGCP che ci si aspetta di ricevere per la comunicazione di una chiamata sono:



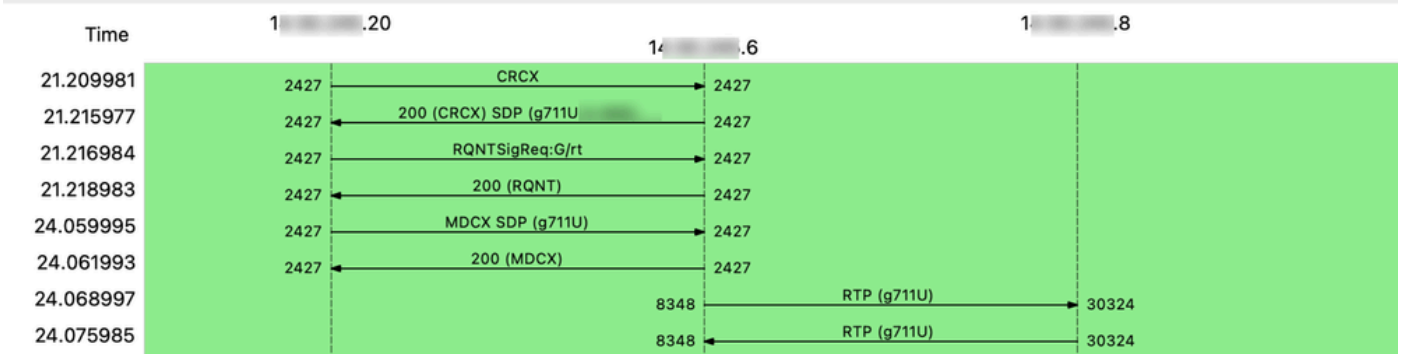


> Nota: L'ispezione MGCP non è abilitata nei criteri di ispezione predefiniti su Cisco Secure Firewall Threat Defense (FTD) e Secure Firewall Adaptive Security Appliance (ASA), quindi è necessario abilitarla se è necessaria questa ispezione.

Questa acquisizione mostra le richieste e le risposte di due dispositivi MGCP e anche il traffico (voce) dei supporti:

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

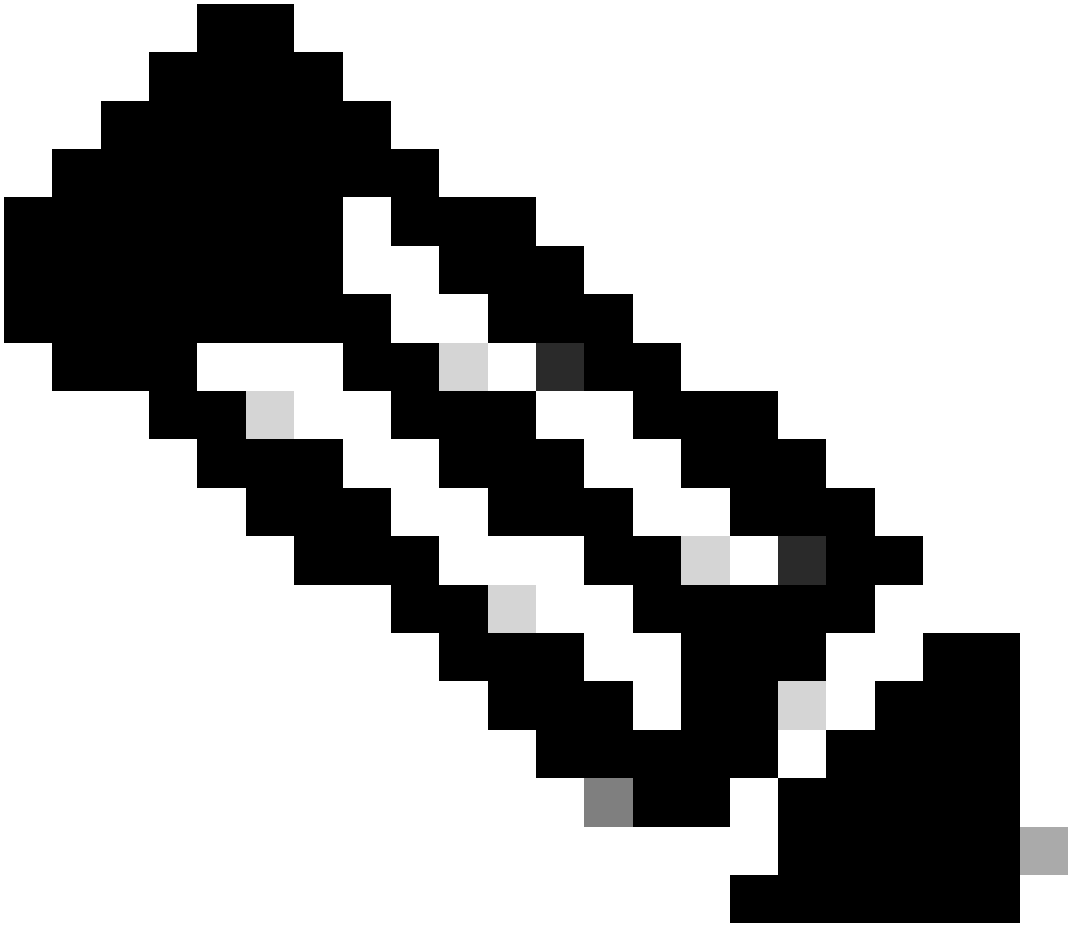
Questo è un esempio di flusso di segnali MGCP e supporti RTP (voce):



Procedure ottimali

Per ASA:

- Utilizzare una regola di autorizzazione che consenta il traffico da e verso i due componenti di segnalazione (dispositivi o server). Questa condizione può essere limitata dalle porte utilizzate sul protocollo VoIP di segnalazione specificato.
- Consente l'intervallo di porte RTP tra i dispositivi multimediali in grado di inviare e/o ricevere flussi audio e/o video.



Nota: Tenere presente che questi dispositivi audio o multimediali potrebbero essere diversi dai componenti di segnalazione (dispositivi o server).

Per FTD:

- Definire le regole di prefiltro per i componenti di segnalazione (dispositivi o server) e definire la porta specifica per limitare solo il traffico per il protocollo di segnalazione specificato.
- Configurare il prefiltro per il protocollo RTP audio e/o video.

Risoluzione dei problemi

Quando si risolvono i problemi relativi alla voce, è necessario sapere se il problema riguarda la segnalazione o i supporti (voce o video) o entrambi. Di seguito sono riportati alcuni esempi che possono aiutare a distinguerli:

Esempio di problemi di segnalazione:

++L'utente segnala che la chiamata non è stabilita.

++L'utente non può chiamare altri utenti o numeri.

++Il trunk SIP non è in arrivo, perché il messaggio SIP OPTIONS non riceve risposta.

++Il dispositivo non è in grado di eseguire la registrazione.

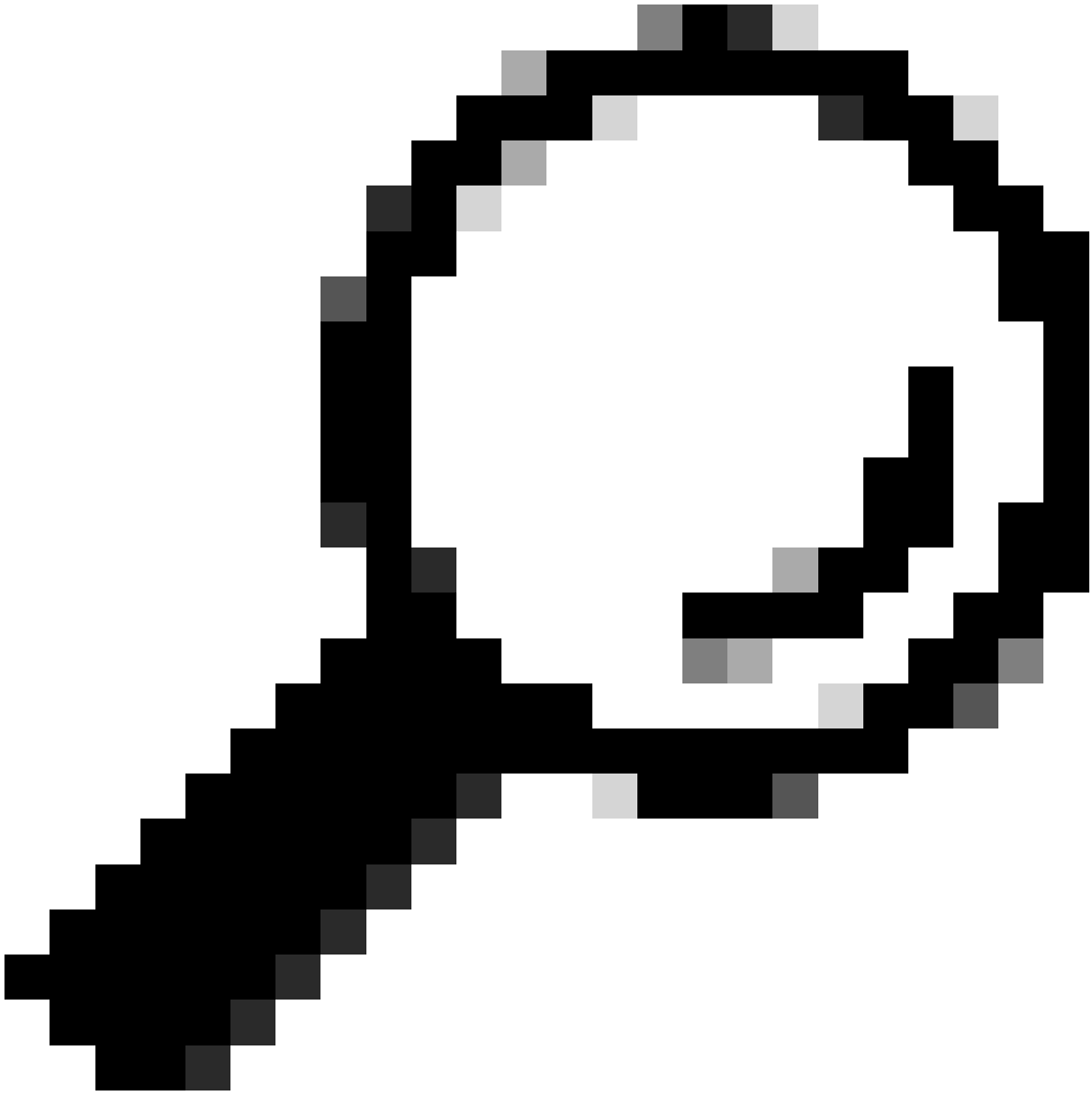
Esempio di problemi relativi ai supporti (voce o video):

++Esiste un problema audio unidirezionale.

++L'audio non è in chiamata.

++Non esiste alcun video.

++La chiamata tace.



Suggerimento: Durante una videochiamata, l'SDP può negoziare fino a tre linee multimediali (m-line): audio, video e immagine. Ogni linea m corrisponde a un flusso RTP (Real-Time Transport Protocol) separato per ogni tappa della chiamata, ovvero possono esistere fino a tre flussi RTP distinti, uno per ogni tipo di supporto, in ogni tappa della chiamata.

Risoluzione dei problemi di segnalazione sul firewall

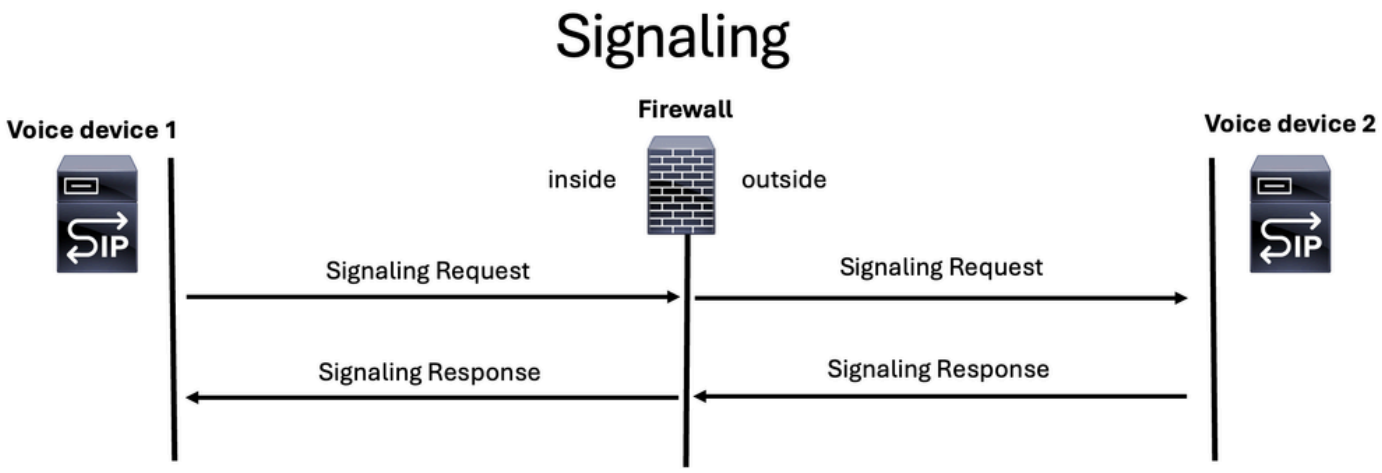
Per la risoluzione dei problemi relativi alla parte di segnalazione, è necessario verificare quanto segue:

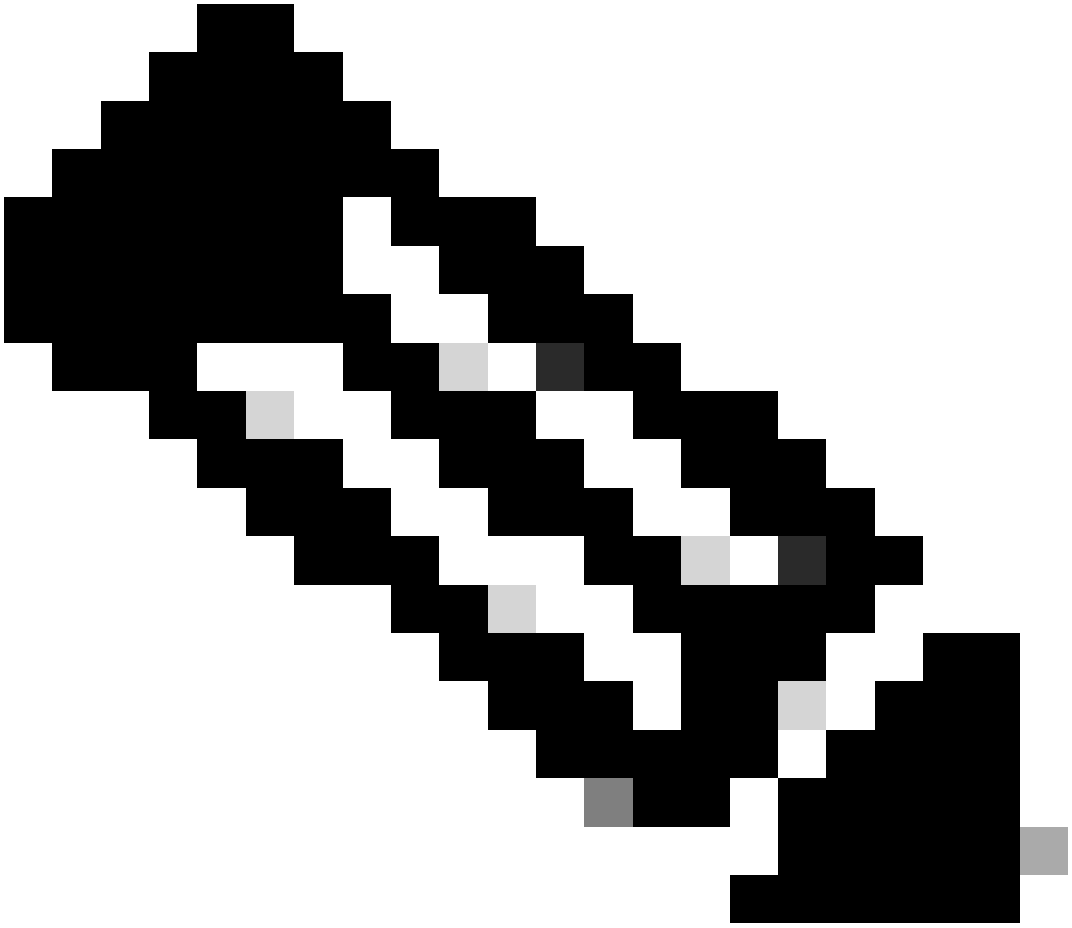
++Identificare tutti i componenti di segnalazione (dispositivi o server) coinvolti nella chiamata sia dall'interfaccia in entrata che da quella in uscita e configurare i criteri di corrispondenza appropriati sulle acquisizioni dei pacchetti sulla CLI di Secure FW.

++Ricordare che il numero di messaggi di segnalazione sull'interfaccia in entrata deve corrispondere all'interfaccia in uscita.

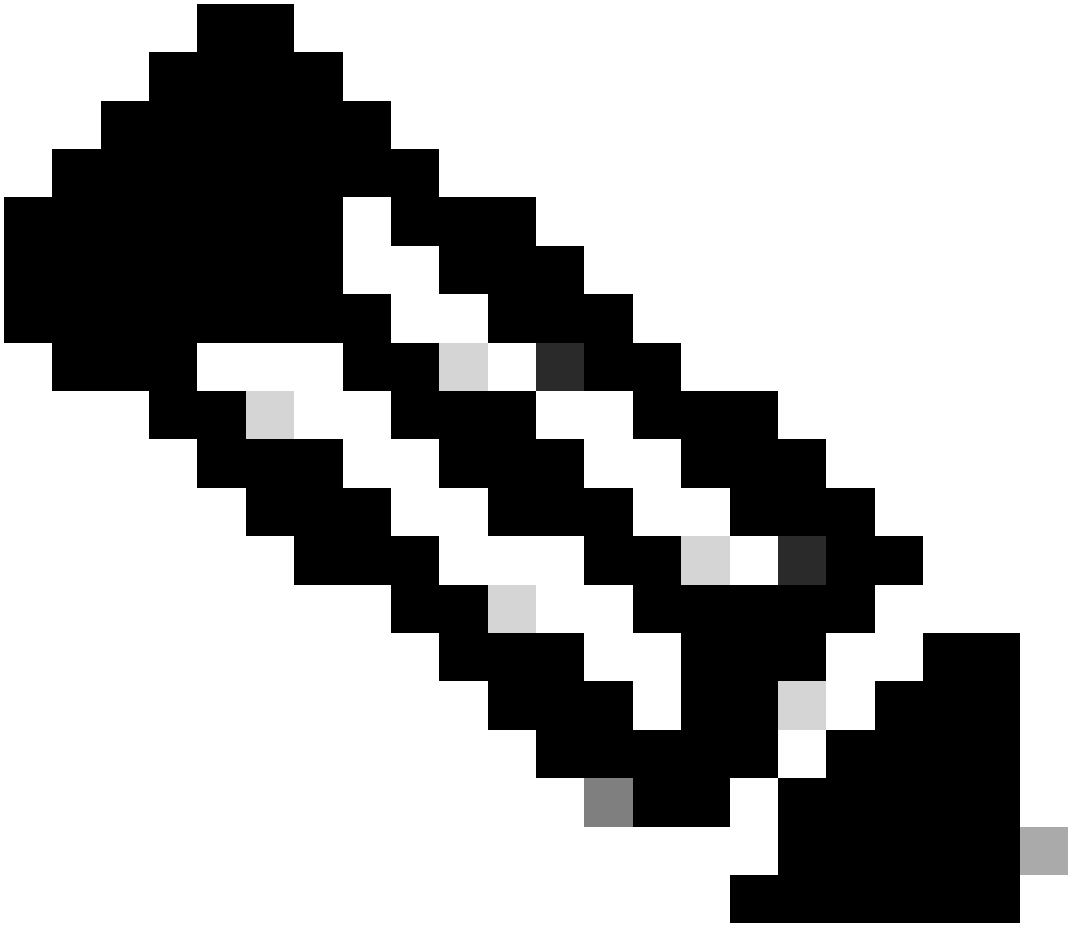
++L'acquisizione dei pacchetti può essere resa più efficiente specificando se il protocollo di segnalazione utilizza TCP o UDP e filtrando il numero di porta previsto. Poiché tutti i protocolli di segnalazione operano su IP, l'applicazione di questi filtri sulla CLI aiuta a limitare la quantità di traffico visualizzata nelle clip.

++Solo per le interfacce in uscita, verificare che l'indirizzo IP NAT assegnato al traffico in uscita sia specificato nel filtro di acquisizione pacchetti. In questo modo, è possibile catturare il traffico corretto così come viene visualizzato sull'interfaccia di uscita.





Nota: tenere presente che, a prescindere dal protocollo di segnalazione utilizzato per la voce, devono sempre esistere una richiesta e una risposta coerenti sulle interfacce in entrata e in uscita.

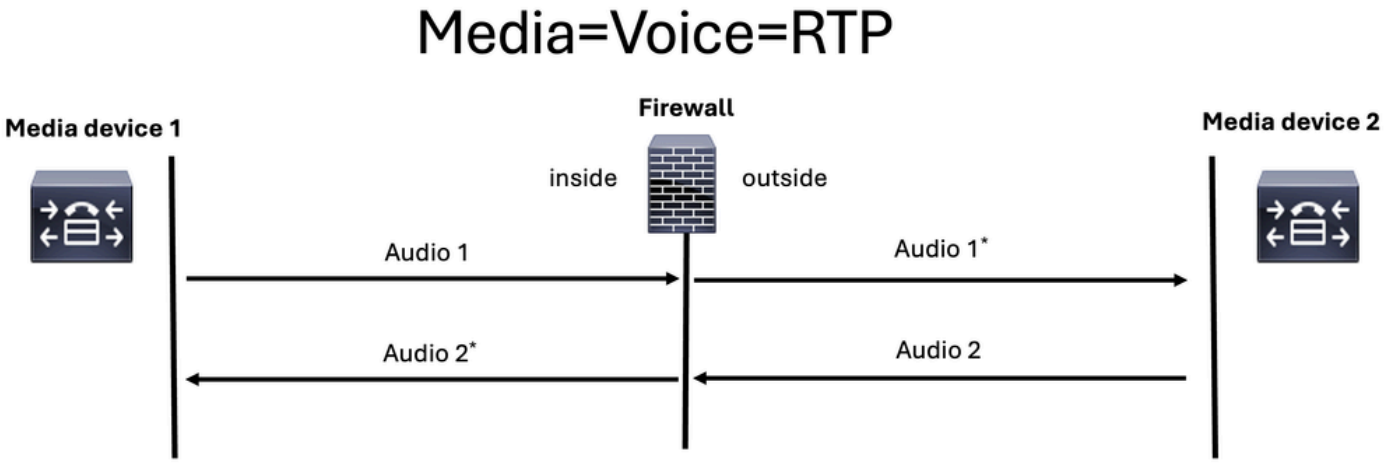


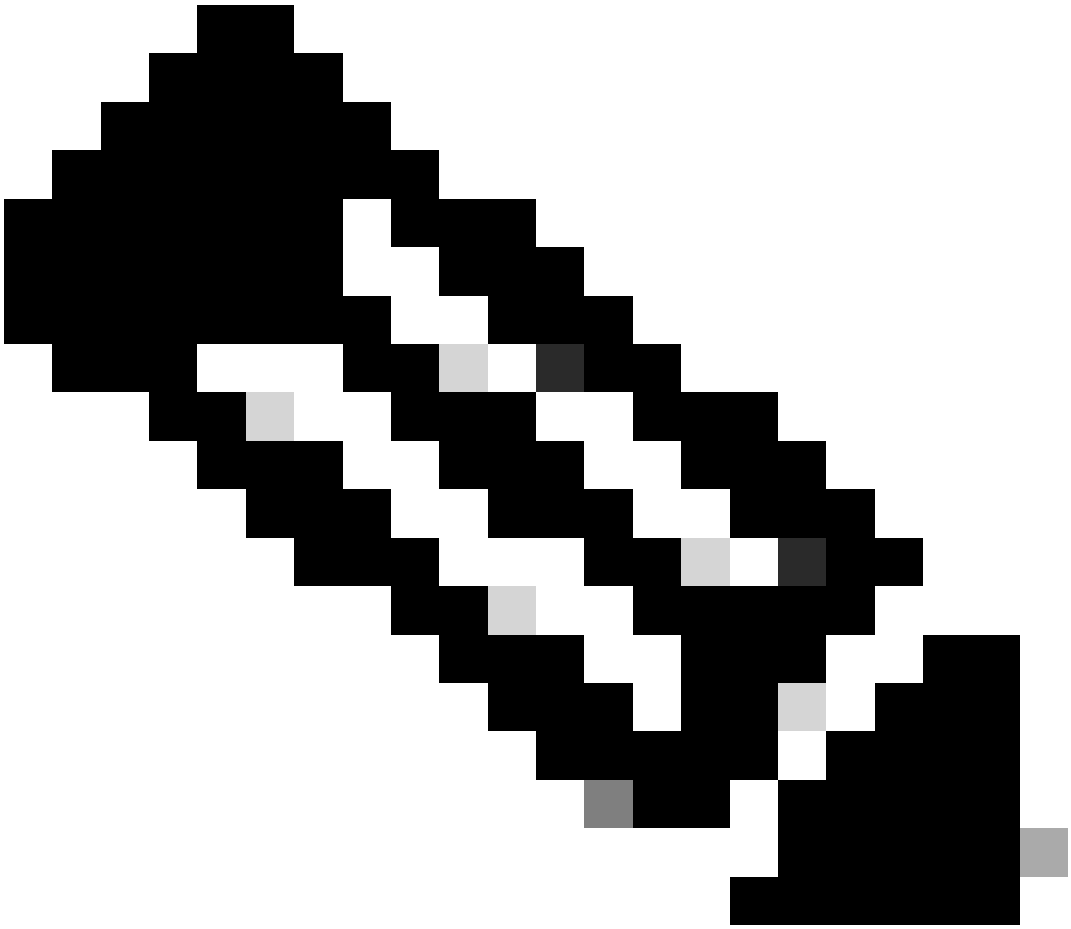
Nota: se possibile, verificare che solo un firewall sia coinvolto nel percorso di comunicazione. In alcune distribuzioni, la segnalazione vocale e i flussi multimediali possono attraversare firewall distinti. In questi casi, assicurarsi di includere tutti i firewall rilevanti nel processo di risoluzione dei problemi

Risoluzione dei problemi relativi ai supporti sul firewall

Dal punto di vista dei flussi, saranno 4 i flussi da analizzare quando si risolvono problemi di audio unidirezionale, problemi di audio bidirezionale o nessun audio:

1. Flusso RTP da chiamante a destinatario chiamata (interfaccia in ingresso).
2. Flusso RTP da chiamante a destinatario chiamata (interfaccia in uscita).
3. Flusso RTP da destinatario chiamata a chiamante (interfaccia in uscita).
4. Flusso RTP da destinatario chiamata a chiamante (interfaccia in ingresso).



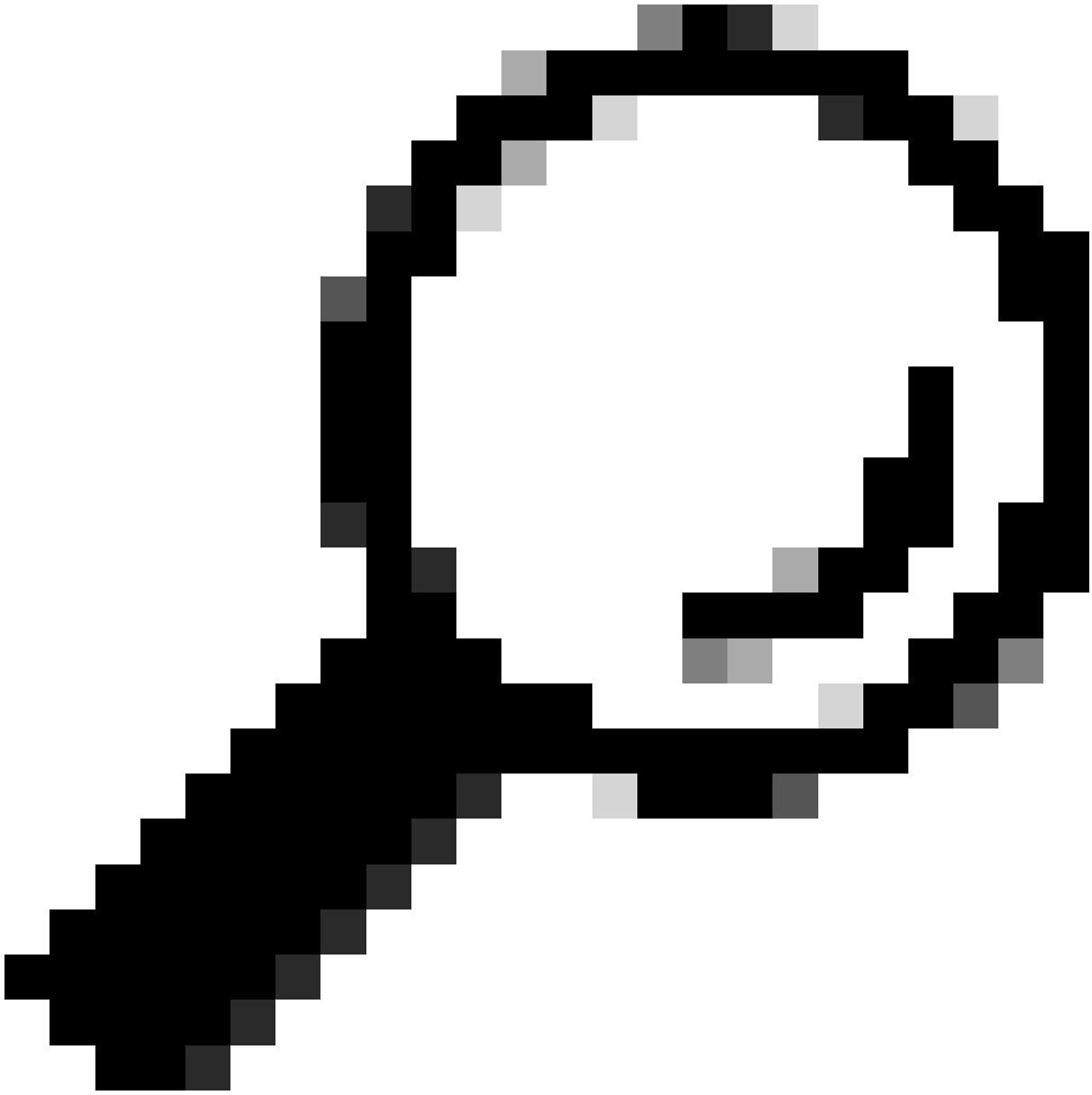


Nota: accertarsi di eseguire la risoluzione dei problemi utilizzando le acquisizioni dei pacchetti CLI in modalità ASA o LINA sull'FTD, in quanto ciò fornisce una maggiore flessibilità per applicare più corrispondenze all'interno di una singola acquisizione.

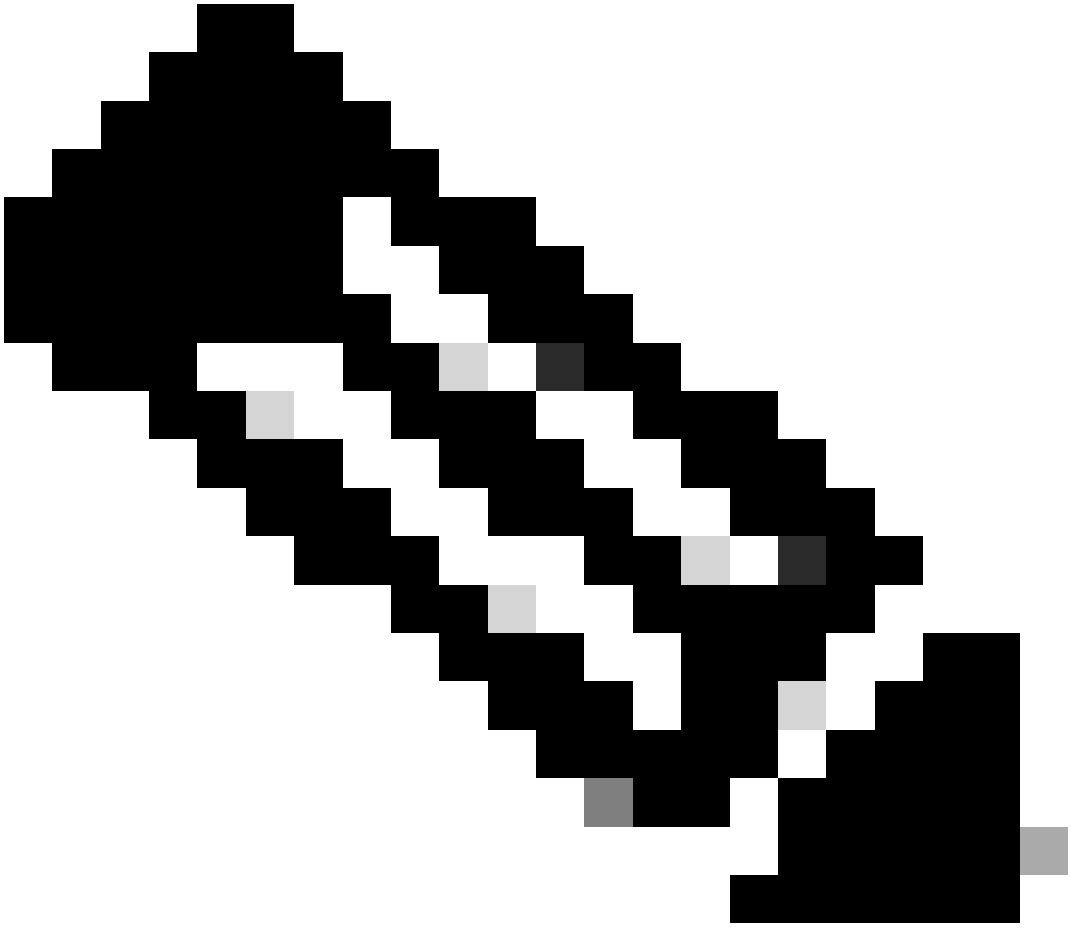
Risoluzione dei problemi delle chiamate SIP

Per risolvere i problemi relativi alla voce su Secure FW (ASA o FTD), effettuare le seguenti operazioni:

1. Assicurarsi di disporre del flusso di chiamate e del diagramma della topologia.
2. Assicurarsi di comprendere il problema dal punto di vista dell'utente.
3. Comprendere il percorso del protocollo di segnalazione.
4. Comprendere il percorso del protocollo Media RTP.
5. Acquisire i pacchetti su entrambe le interfacce in entrata ed in uscita.
6. Esaminare le regole ACL di configurazione e le regole NAT.
7. Verificare che il traffico di segnalazione SIP non sia bloccato dal firewall. Inoltre, confronta le interfacce in entrata e in uscita per analizzare il flusso del traffico vocale.
8. Verificare che il traffico multimediale RTP non venga bloccato dal firewall confrontando il flusso del traffico sulle interfacce in entrata e in uscita.
9. Verificare che i dispositivi di segnalazione supportino l'ispezione e, in caso contrario, disattivarla.



Suggerimento: I messaggi di segnalazione SIP che entrano nel firmware devono essere gli stessi che lasciano il firmware.



Nota: I suggerimenti per la risoluzione dei problemi per il SIP possono essere applicati anche ai protocolli H.323, MGCP e SCCP.

Informazioni correlate

- Configurazione delle acquisizioni di pacchetti ASA con CLI
- Usa acquisizioni Firepower Threat Defense

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).