Conheça os fundamentos dos protocolos de voz sobre IP para firewall seguro

Contents

Introdução

Este documento descreve os fundamentos de vários protocolos VoIP para ajudar os engenheiros a solucioná-los de forma eficaz em firewalls seguros.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento destina-se ao uso em cenários de solução de problemas com estes dispositivos:

- Defesa contra ameaças de firewall (FTD) segura
- Dispositivo de segurança adaptável (ASA) com firewall seguro

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

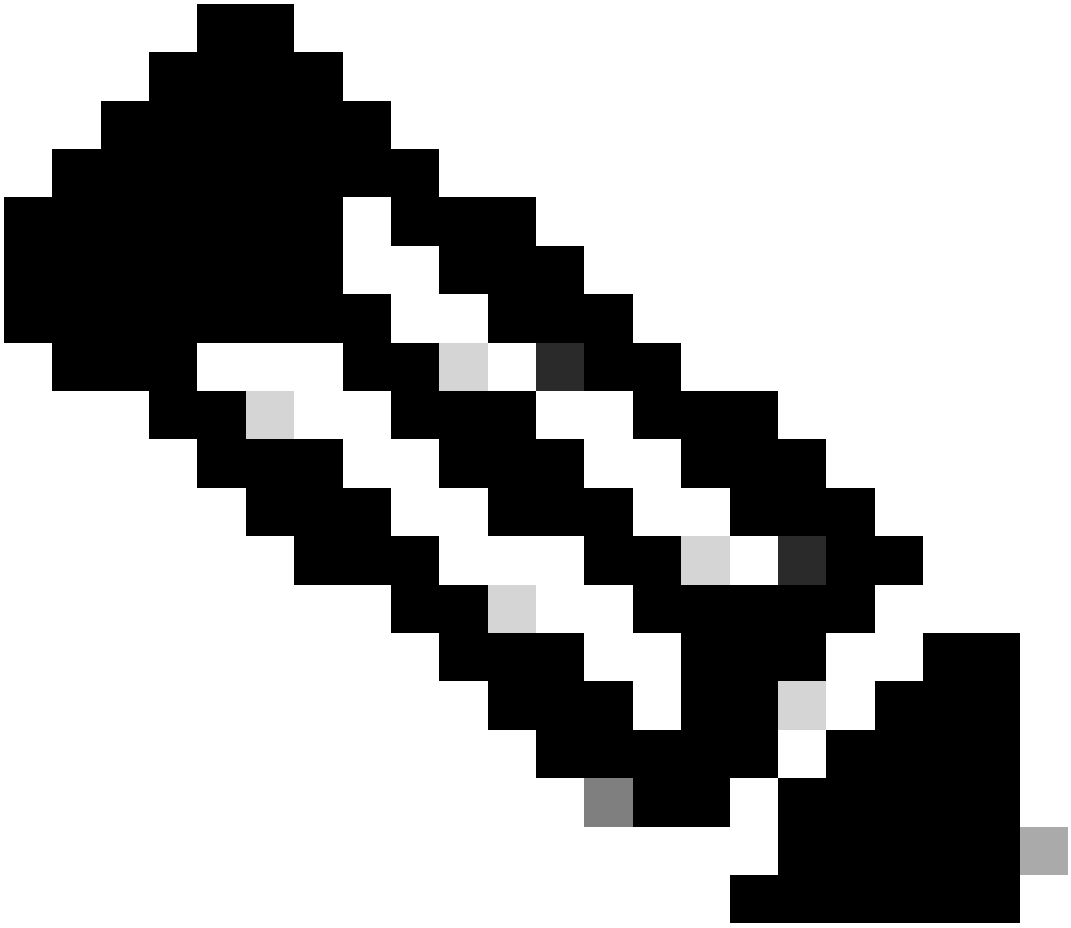
Conceitos básicos de VoIP

A comunicação é fundamental para as interações humanas, os protocolos de Voz sobre IP (VoIP) tornaram-se indispensáveis para a comunicação humana. É por isso que é importante conhecer suas partes ao solucionar problemas de um cenário que inclui um Firewall (FW).

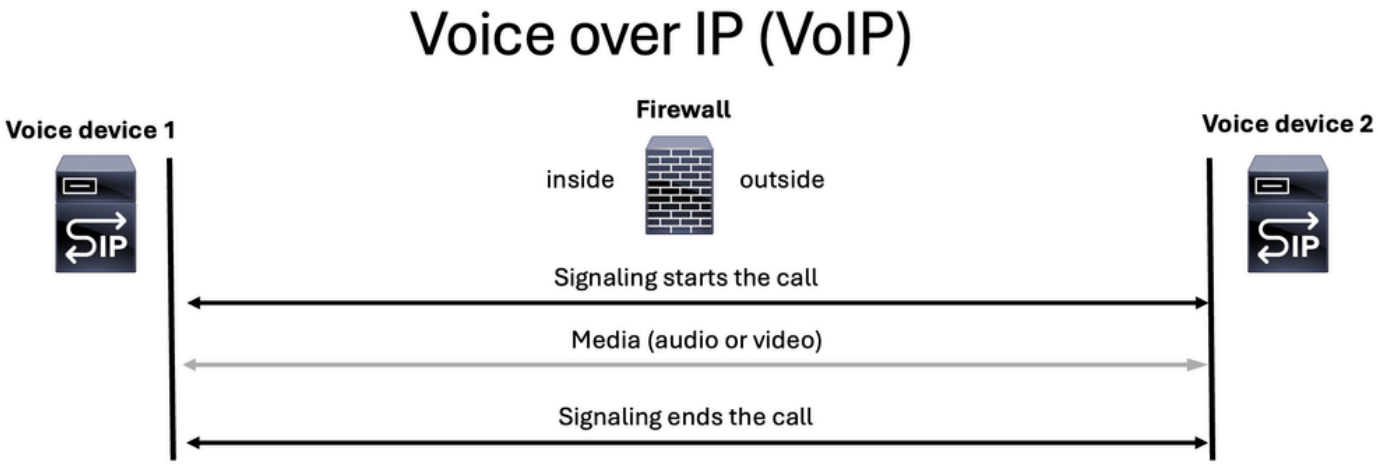
O VoIP é composto de duas partes:

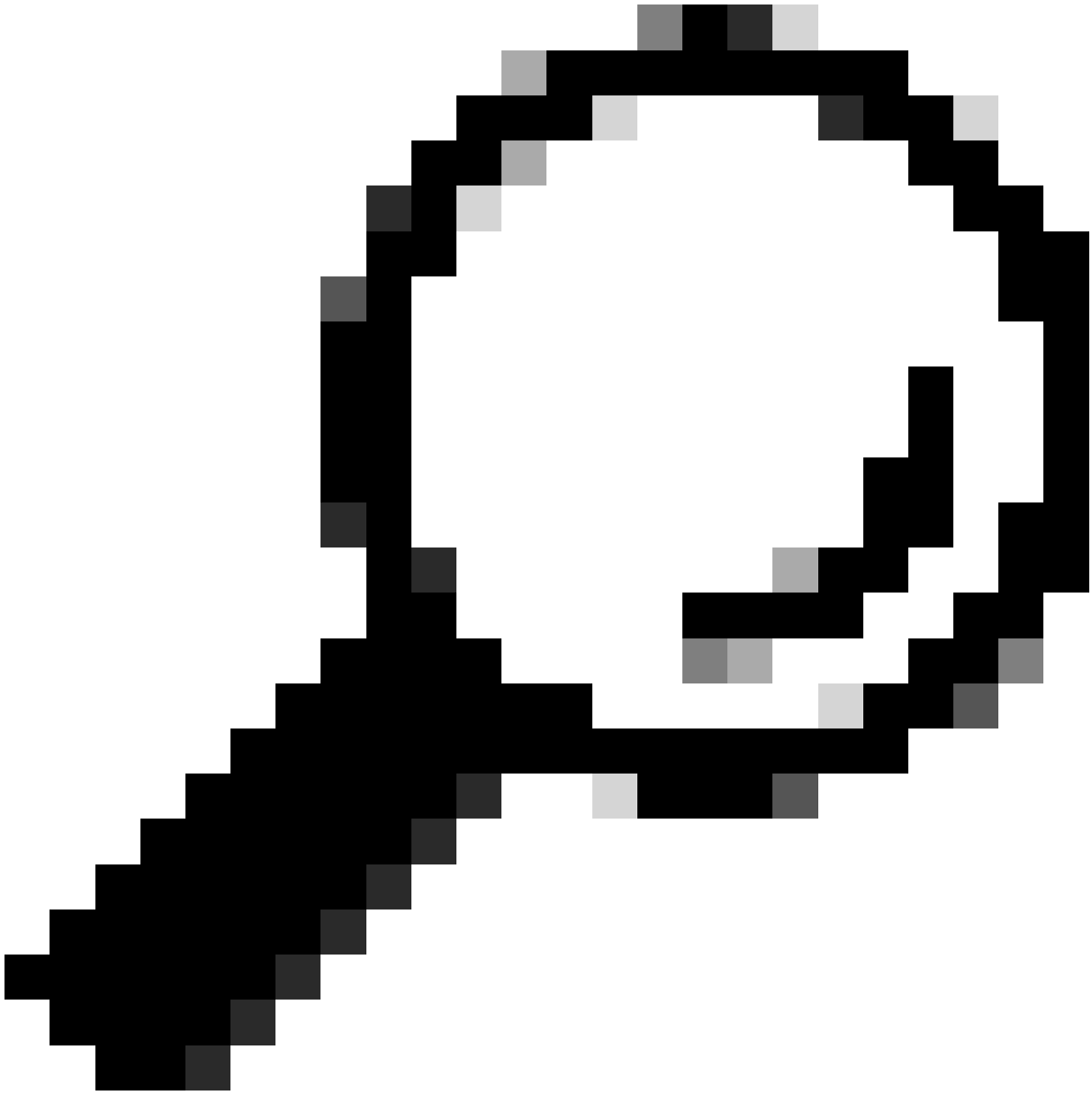
- Sinalização
- Mídia (voz ou vídeo)

As comunicações VoIP sempre começam com uma parte de sinalização para iniciar uma chamada, depois a mídia (voz ou vídeo) é transmitida e, finalmente, a sinalização encerra a chamada.

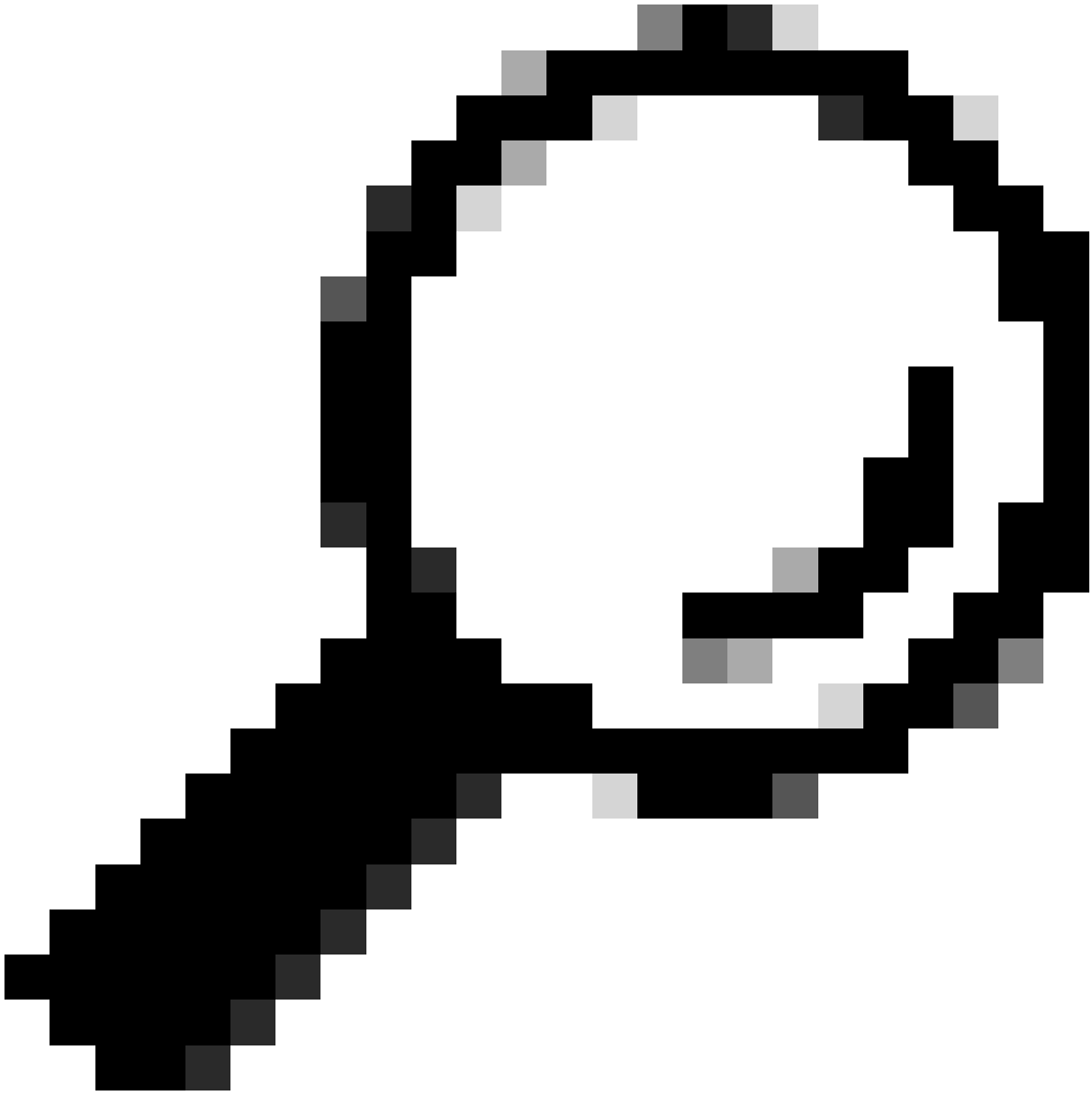


Note: O SIP é o protocolo mais amplamente usado, portanto é representado consistentemente como o ícone do servidor de voz SIP em muitos dos diagramas.





Tip: Ao solucionar um problema de voz do ASA ou do FTD, é crucial considerar o cenário da perspectiva do usuário. Você precisa determinar se a chamada foi estabelecida ou se não há áudio ou áudio unidirecional. Essas informações fornecem pistas valiosas sobre se o problema está no protocolo de sinalização ou no protocolo de mídia (voz ou vídeo).



Tip: Um dispositivo de voz pode gerenciar o tráfego RTP (Real-time Transport Protocol) de voz, o tráfego de sinalização ou ambos simultaneamente. Ao solucionar problemas de voz, é essencial lembrar estes conceitos principais:

++Servidores de sinalização: Esses servidores são responsáveis por lidar apenas com o tráfego de sinalização.

++Servidores de mídia: Esses servidores lidam exclusivamente com o tráfego RTP de voz.

++Alguns dispositivos podem lidar com ambas as tarefas.

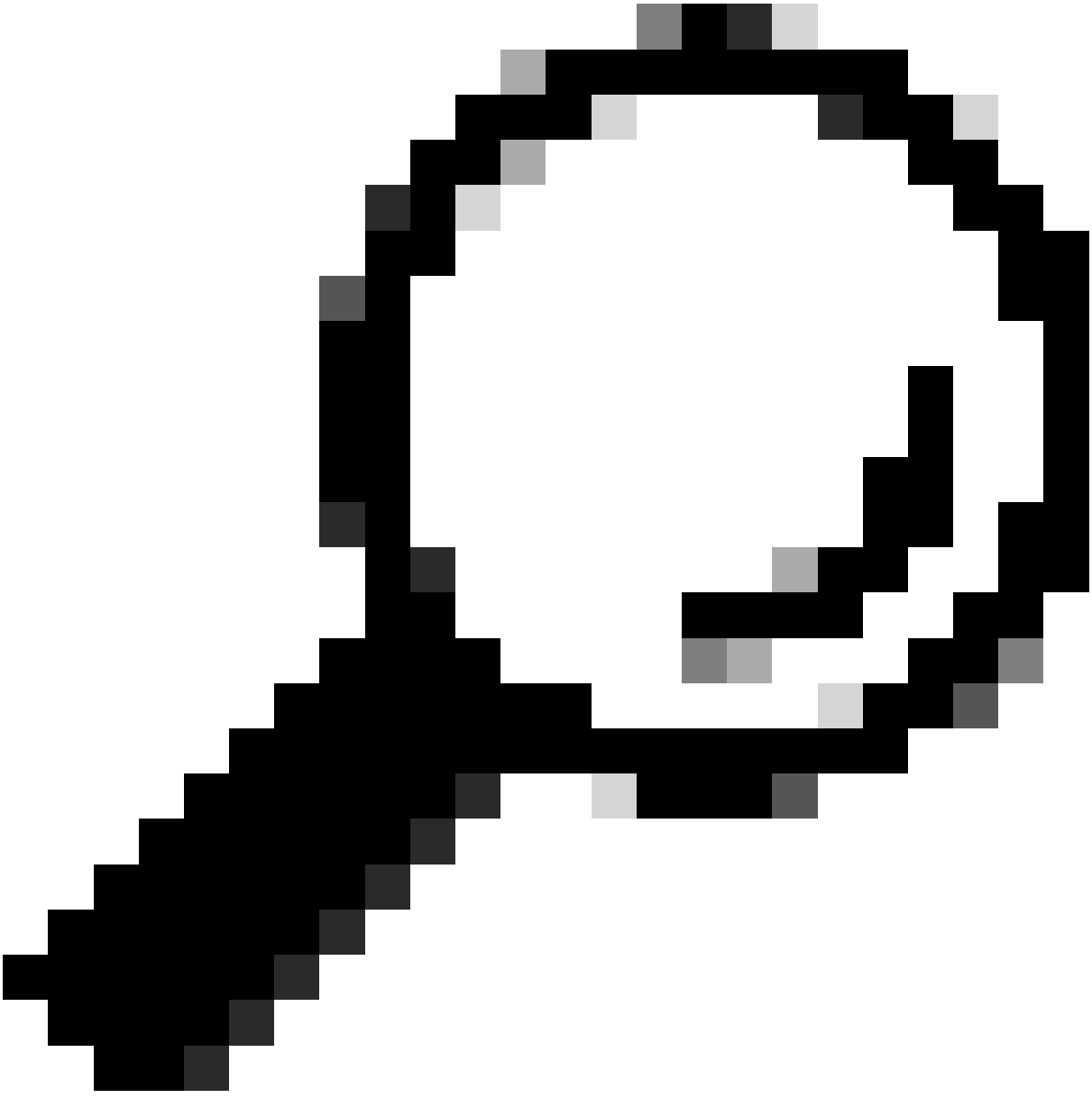
Sinalização

O protocolo de sinalização é a parte de uma chamada que inicia a comunicação de voz, mas não apenas isso, ele também executa estas funções:

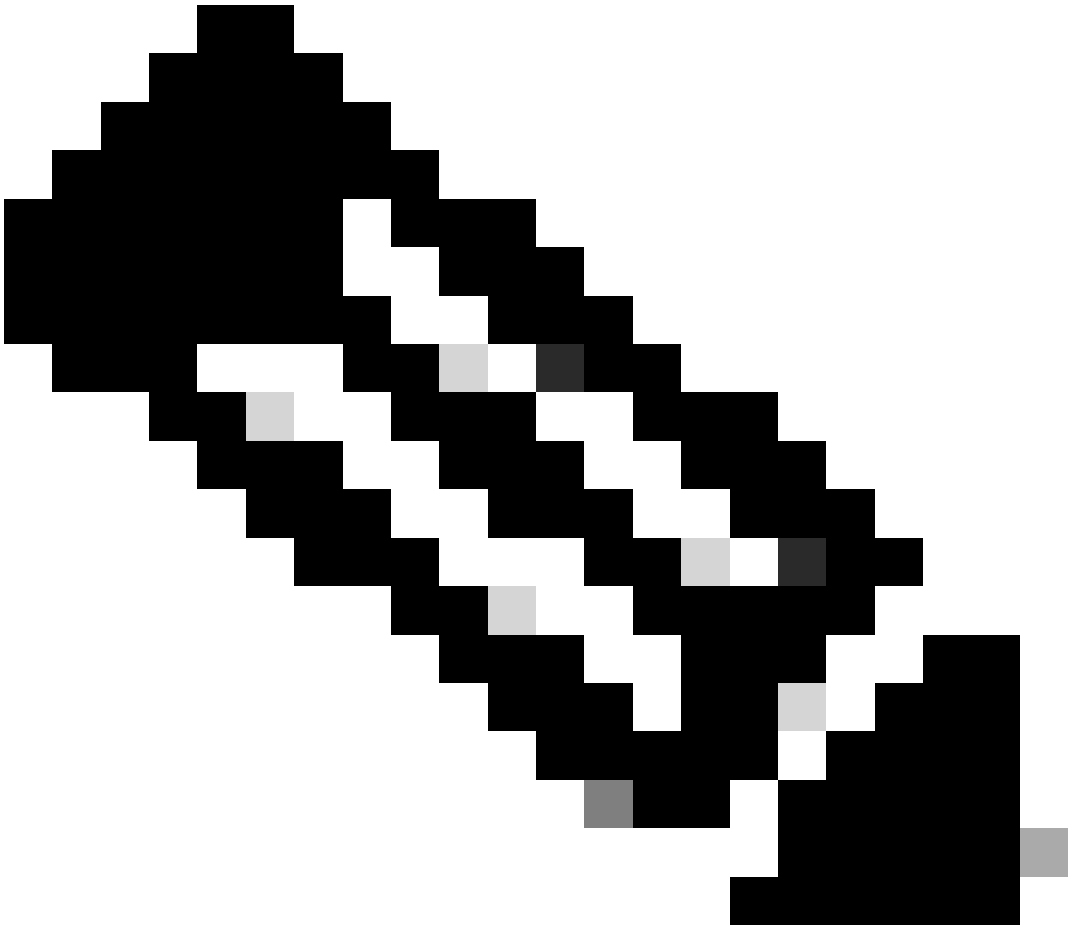
- Mantém a comunicação ativa.
- Modifica a comunicação.
- Finaliza a comunicação.

Tipos diferentes de protocolos de sinalização ajudam uma chamada a ser estabelecida e os mais comuns incluem:

- Protocolo de Iniciação da Sessão (SIP)
- H.323
- Media Gateway Control Protocol (MGCP)
- Skinny Call Control Protocol (SCCP)



Tip: É essencial identificar o protocolo de sinalização em uso para determinar as portas apropriadas para a captura de pacotes no ASA ou FTD. Além disso, ter um fluxo de chamadas e uma topologia de rede é útil para entender o caminho de sinalização.

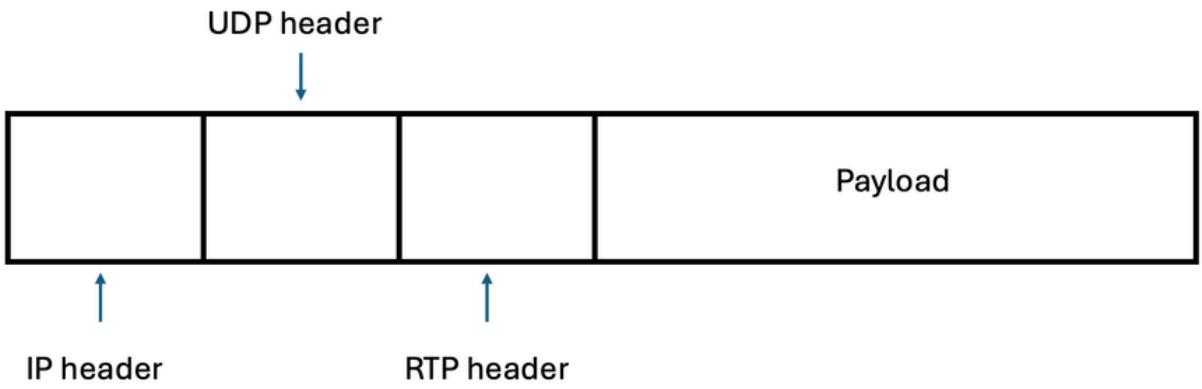


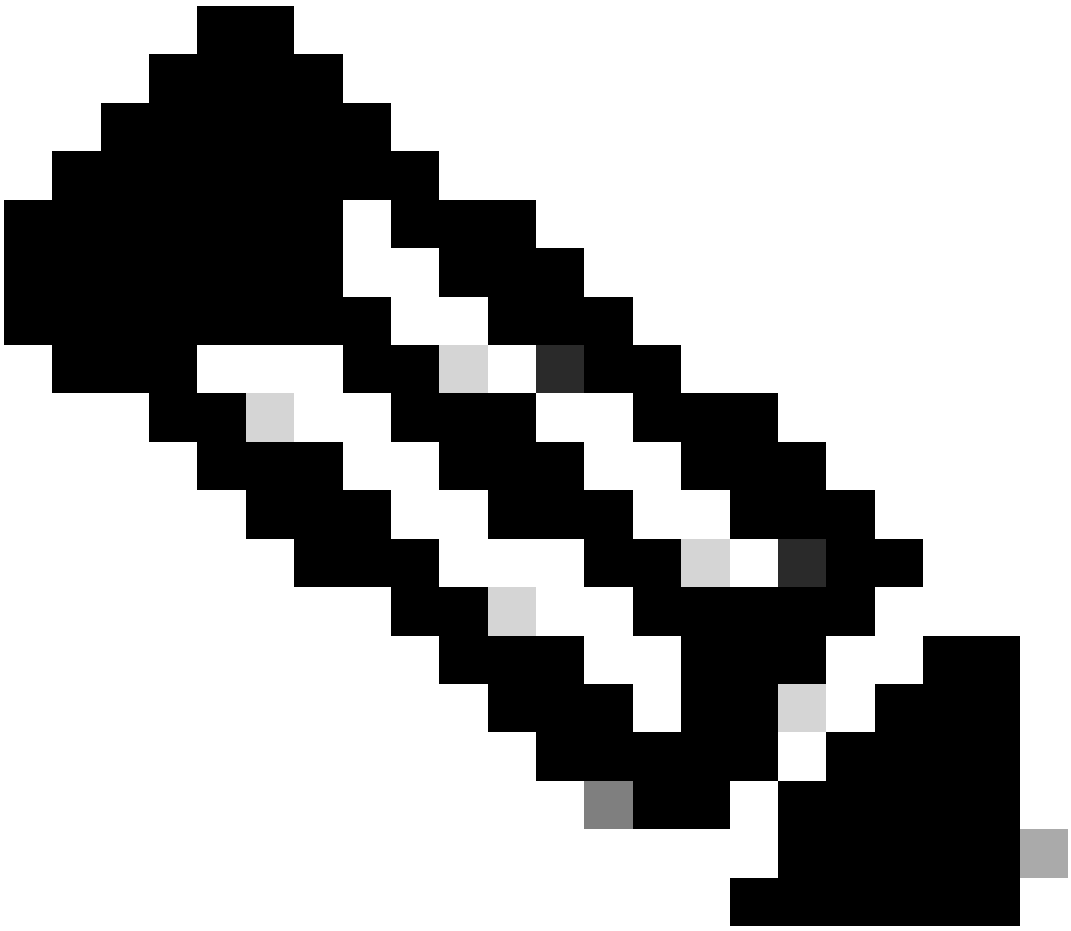
Note: Os pacotes de sinalização incluem endereços IP origem e destino, auxiliando na identificação das partes envolvidas no envio e recebimento do fluxo de mídia RTP.

Mídia

Após a conclusão da sinalização e os componentes de sinalização (dispositivos ou servidores) concordarem sobre o tipo de mídia, o Real Time Protocol (RTP) entra em ação para iniciar o envio de mídia (áudio e/ou vídeo) a todas as partes envolvidas.

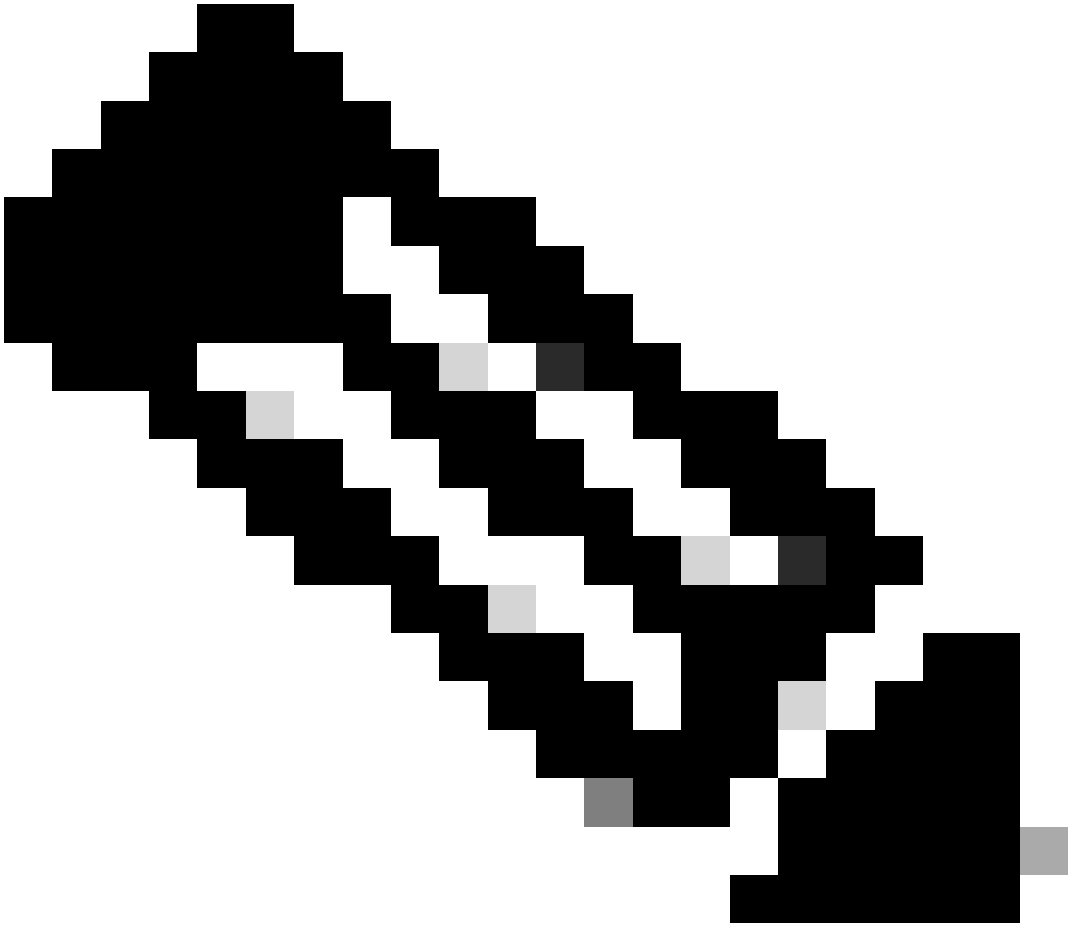
O RTP é um protocolo de Internet usado para mídia de streaming que é enviado somente depois que a chamada é estabelecida e executada sobre o User Datagram Protocol (UDP).



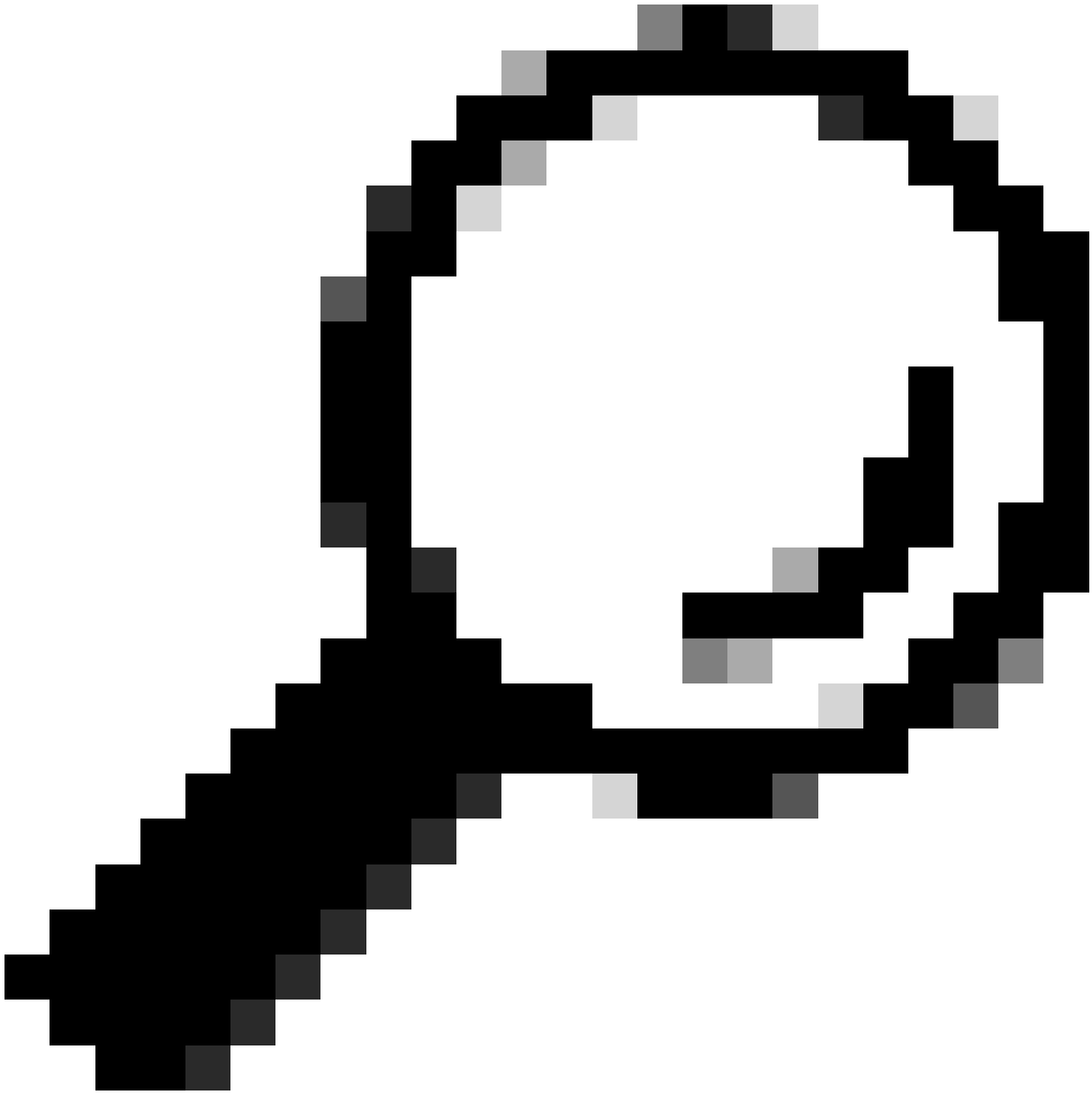


Note: A mídia pode ser voz e/ou vídeo e trafega em pacotes RTP.

Os componentes de sinalização (dispositivos ou servidores) determinam quais portas são usadas para enviar ou receber mídia (áudio e/ou vídeo). O intervalo de portas mais comum para RTP é tipicamente entre 16384 e 32767 para a maioria dos dispositivos.



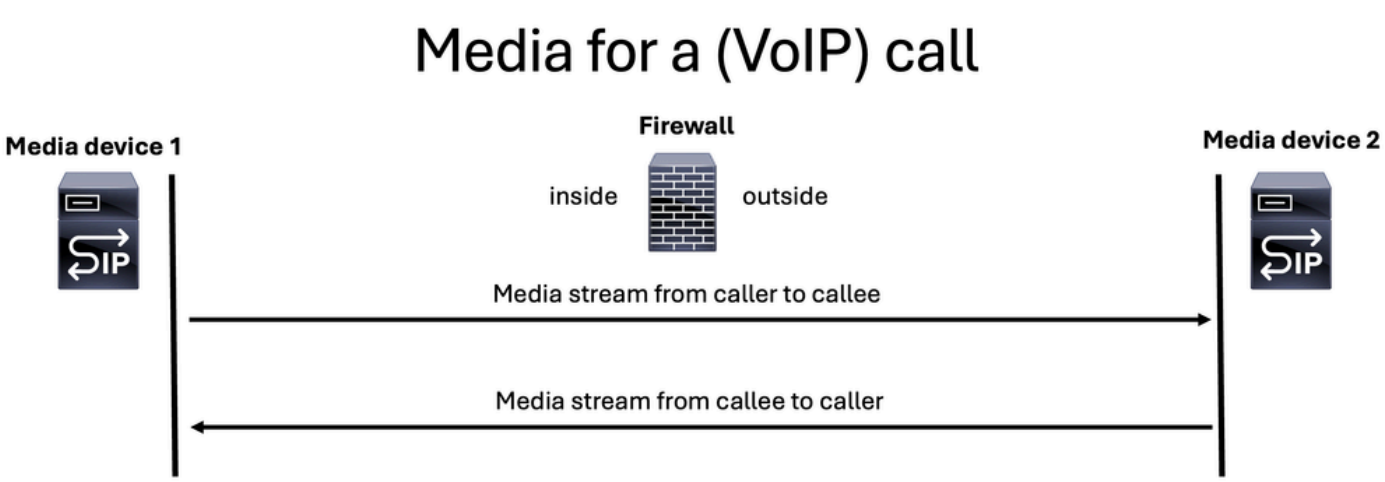
Note: Determinados dispositivos Cisco, como as plataformas ASR e ISR G3, como a plataforma ISR4K, utilizam um intervalo de portas RTP padronizado de 8000 a 48200. É crucial verificar o intervalo de portas RTP específico configurado em seus dispositivos, pois ele pode diferir desses valores padronizados e pode variar entre dispositivos de terceiros.

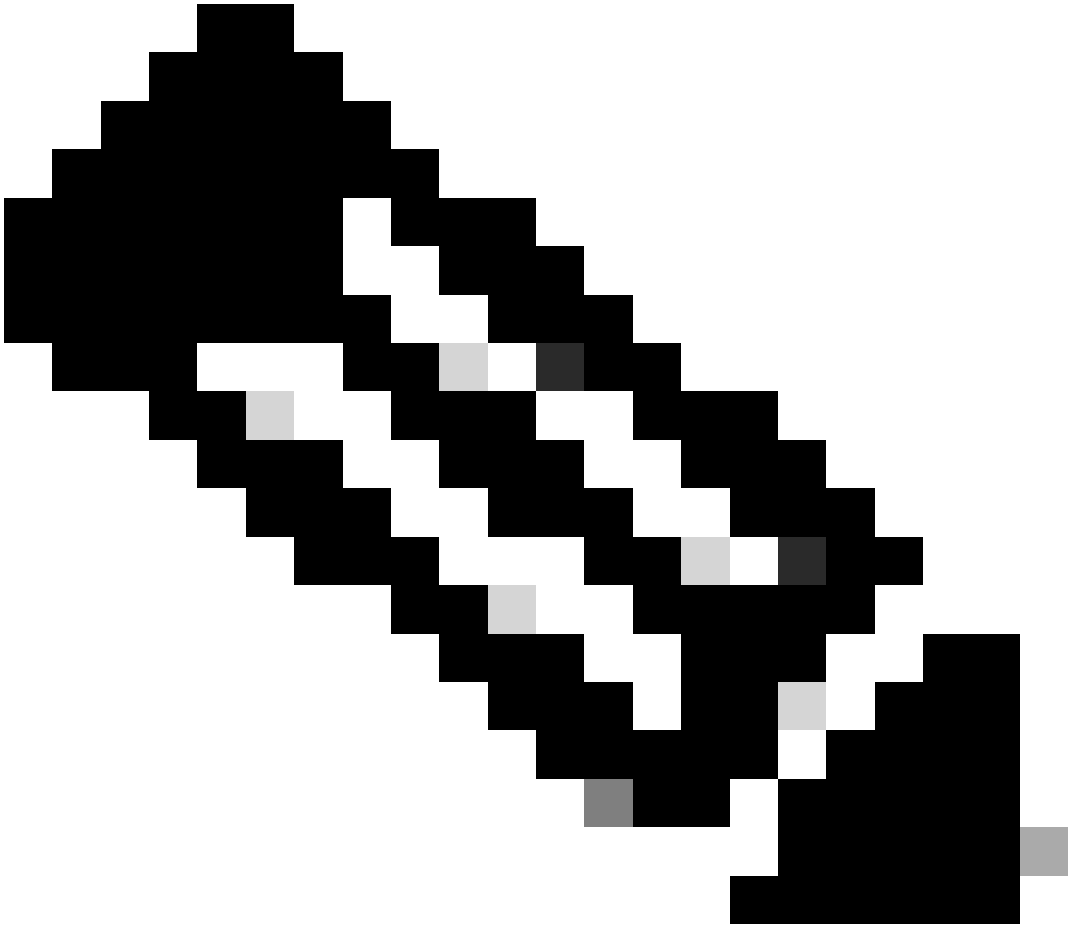


Tip: Às vezes, o caminho RTP difere do caminho de sinalização, tornando crucial identificar os dispositivos responsáveis por enviar e receber pacotes RTP de voz. Isso garante que você capture o tráfego UDP entre os dispositivos que passam pelo ASA ou FTD.

Há dois fluxos de mídia ou fluxos RTP gerados em uma chamada de voz normal:

1. um fluxo de mídia do chamador para o receptor da chamada
2. um fluxo de mídia do receptor da chamada para o chamador





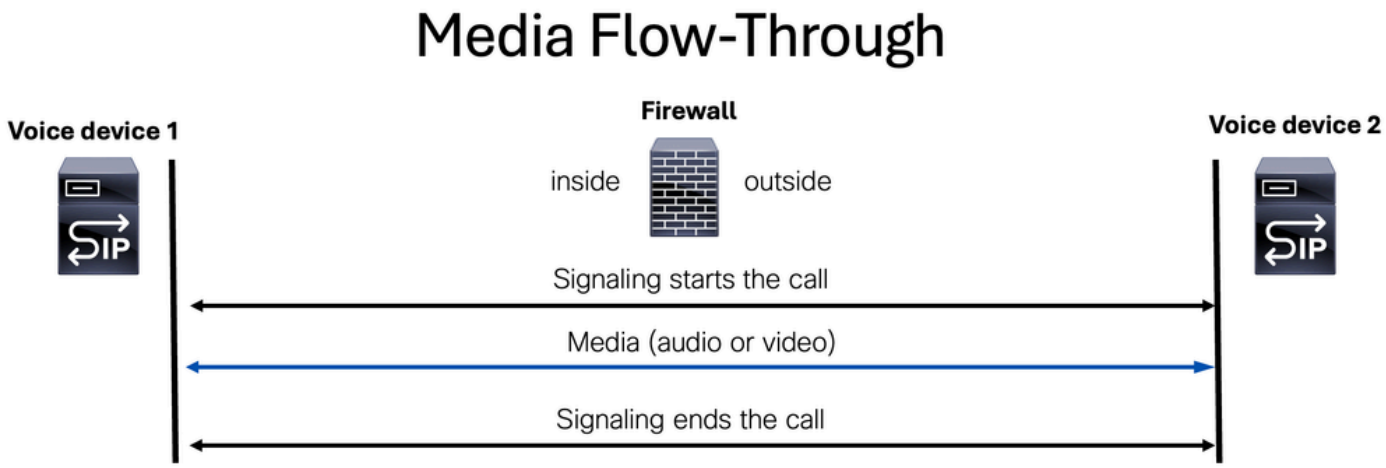
Note: Para fins de ilustração, o ícone do servidor SIP é usado para representar um servidor de sinalização ou um servidor de mídia em todas as imagens.

Ao discutir o streaming de mídia em uma chamada de voz, é importante destacar dois cenários principais:

1. Fluxo de mídia
2. Fluxo de mídia

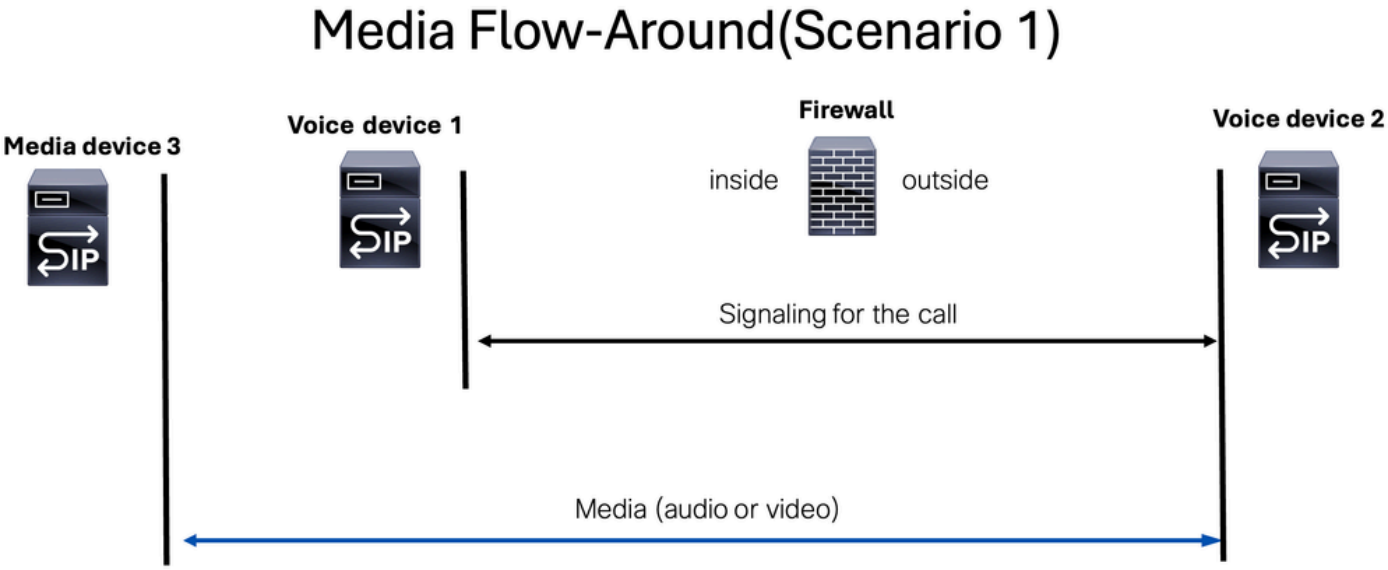
Fluxo de mídia

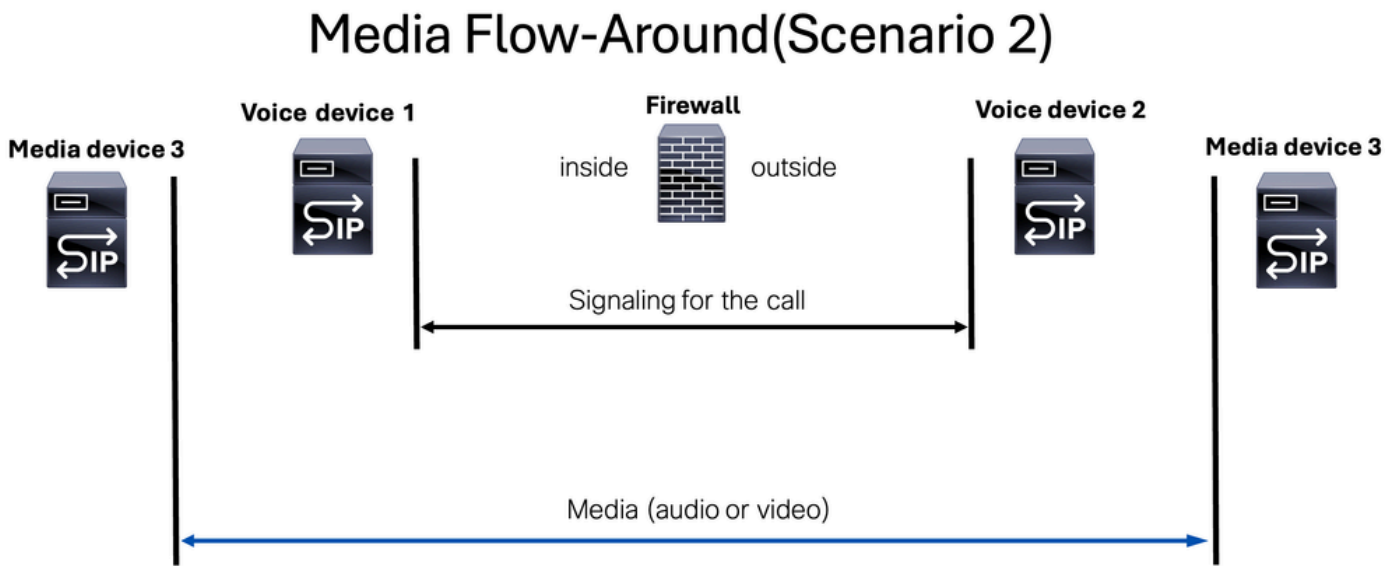
O fluxo de mídia é um modo em que a mídia (voz e/ou vídeo) e os pacotes de sinalização são processados pelo mesmo dispositivo.



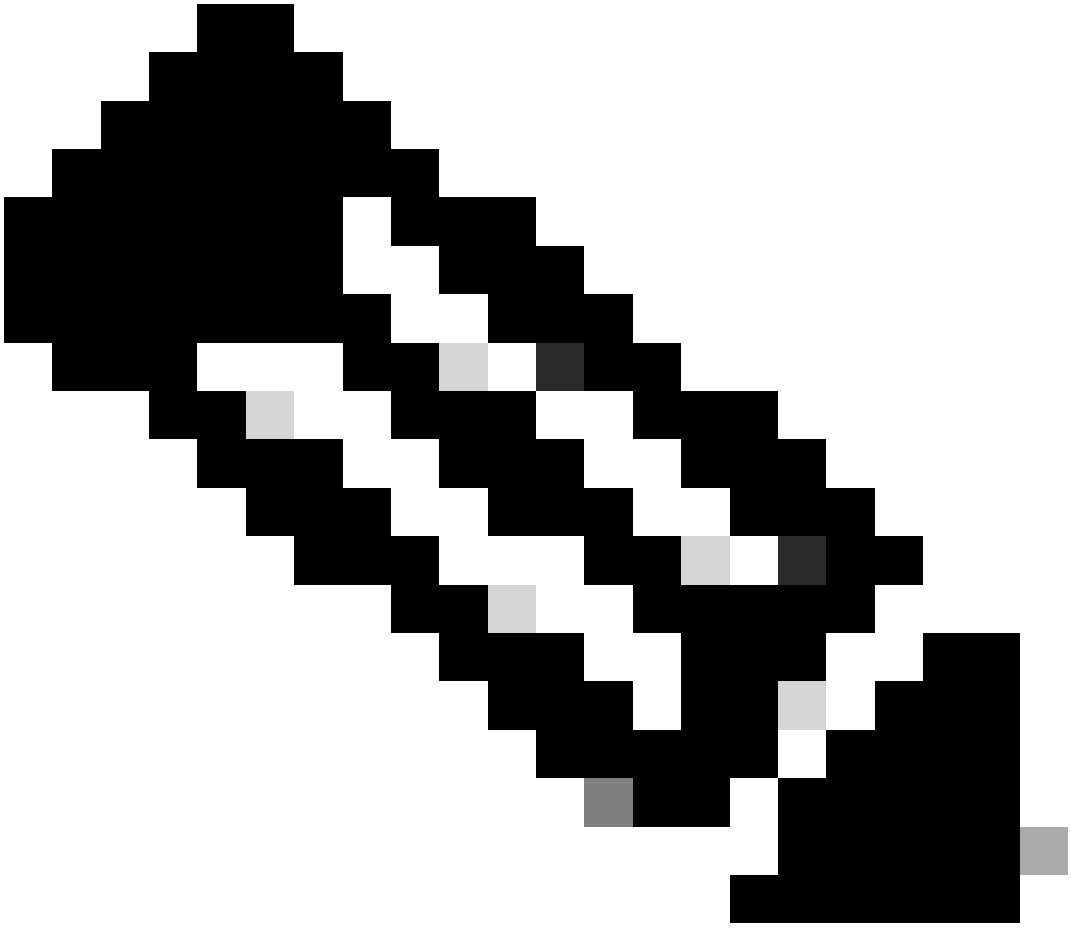
Fluxo de mídia

O fluxo de mídia é um modo em que os pacotes de sinalização são tratados por dois componentes de sinalização separados (dispositivos ou servidores), enquanto o fluxo de mídia (voz ou vídeo) é gerenciado por um terceiro dispositivo conhecido como dispositivo de mídia.





Este modo esclarece as funções dos dispositivos envolvidos e a distinção entre sinais e fluxos de mídia ou dispositivos.



Note: Isso é especialmente importante para mencionar quando a solução de problemas da lista de acesso criada pode permitir os componentes de sinalização (dispositivos ou servidores), mas se o fluxo de mídia estiver usando outro dispositivo de mídia, precisamos permitir isso também na lista de acesso de nosso dispositivo FW.

Protocolo de Iniciação da Sessão (SIP)

O SIP é um protocolo de controle da camada de aplicação definido pela Internet Engineering Task Force (IETF) no RFC 3261.

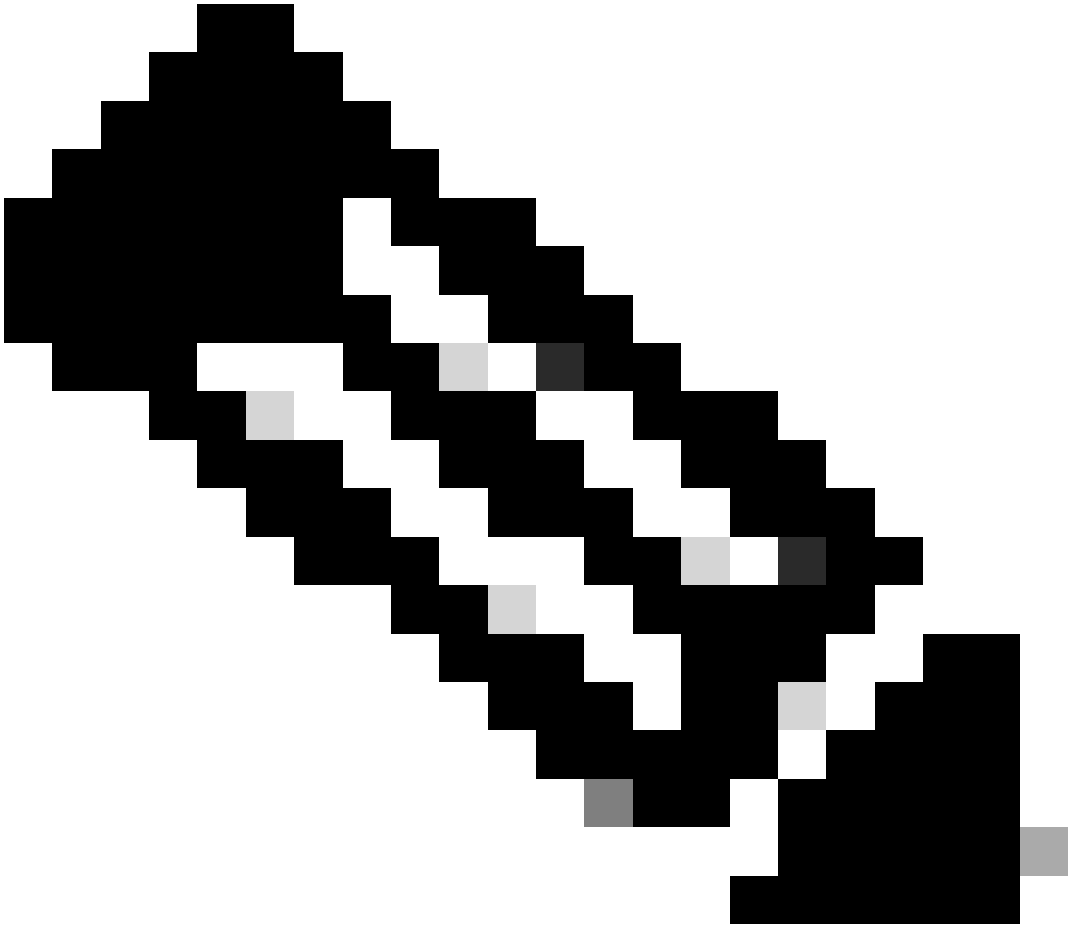
O SIP é um protocolo baseado em texto. Isso significa que as mensagens SIP são compostas de texto legível, semelhante à forma como o HTTP opera.

O SIP é projetado para lidar com as funções de sinalização e gerenciamento de sessão dentro de uma rede de telefonia por pacotes.

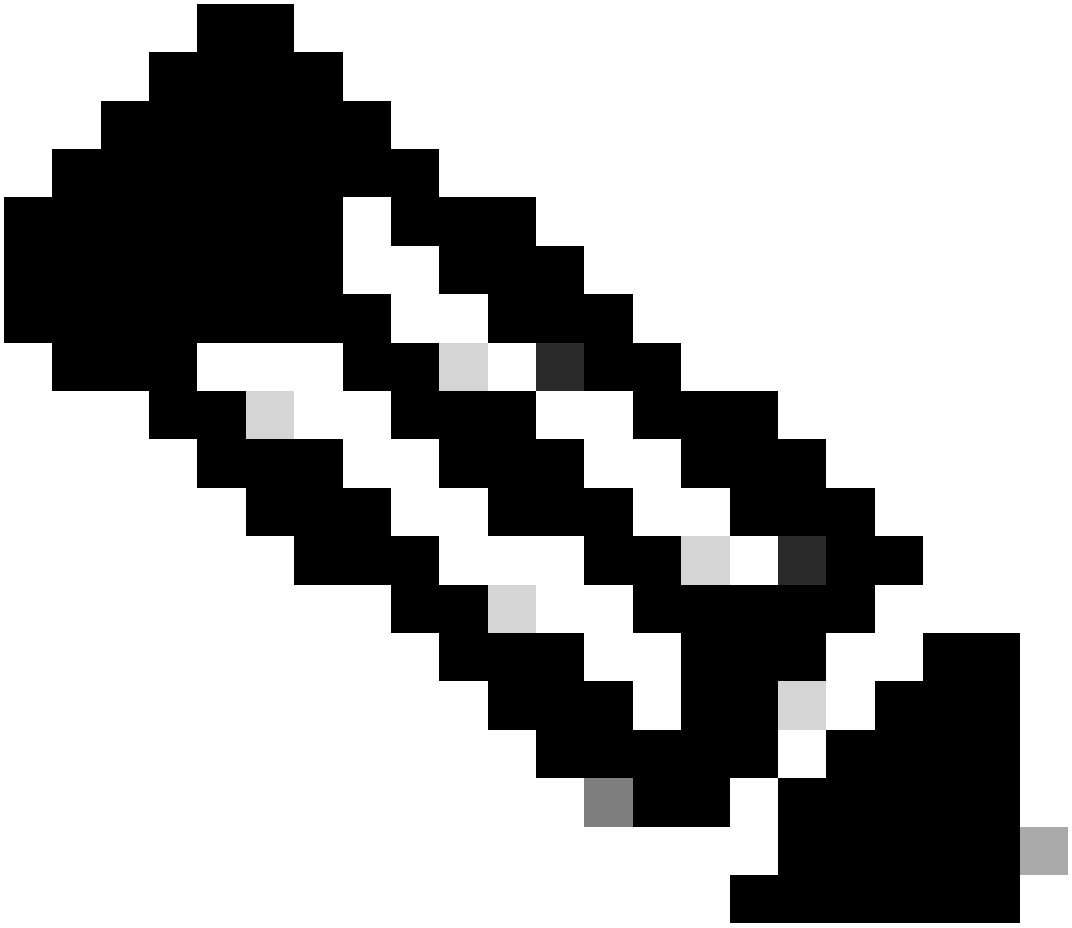
O SIP pode:

- criar uma chamada
- modificar uma chamada
- terminar uma chamada

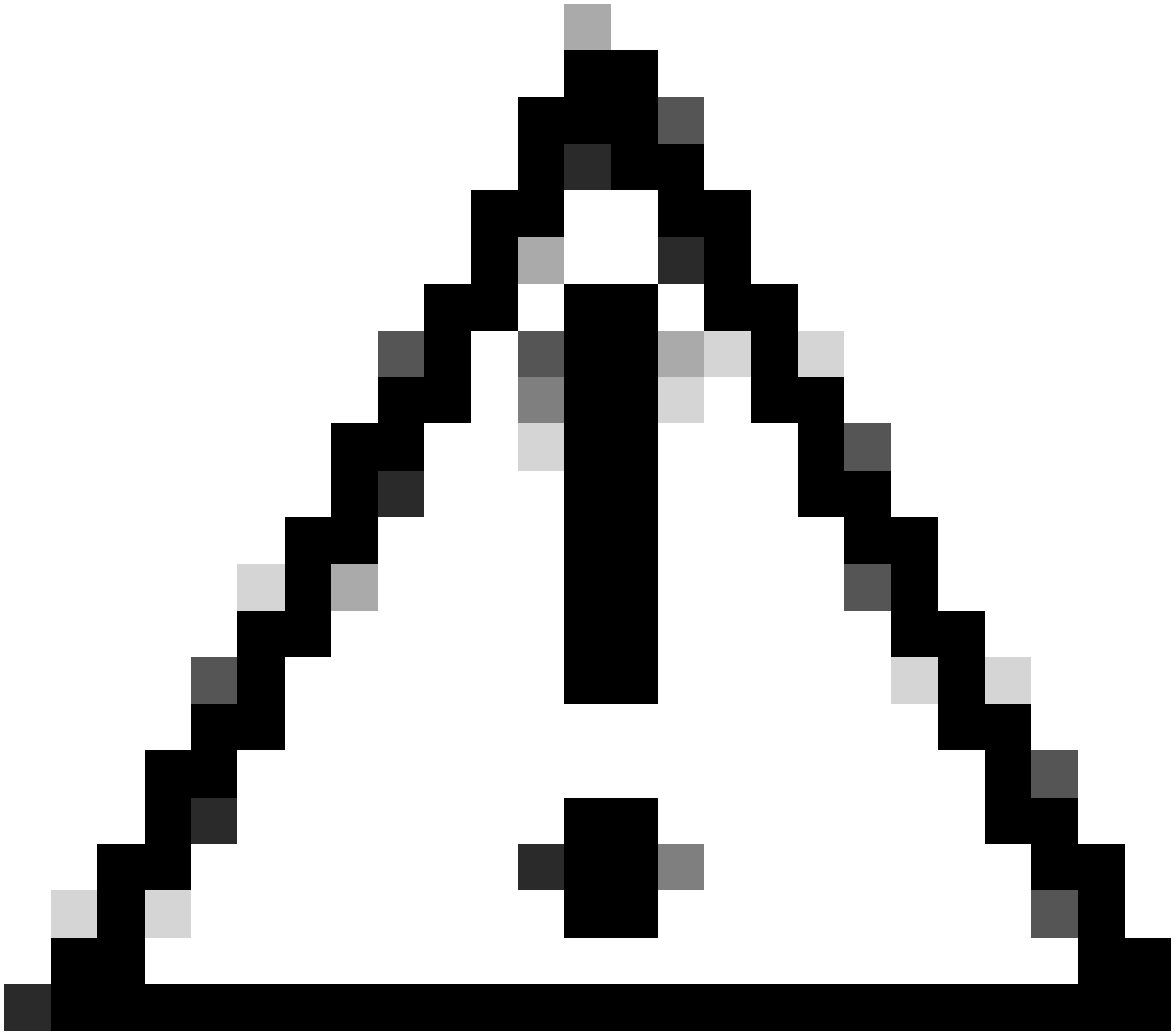
O SIP pode ser usado como UDP ou TCP na porta padronizada 5060. E se o SIP for criptografado usando o protocolo TLS, ele poderá usar a porta padronizada 5061.



Note: Quando a sinalização SIP é criptografada, os pacotes SIP reais não são visíveis em capturas de pacotes em dispositivos ASA ou FTD. No entanto, você ainda poderá observar o handshake TCP seguido pelo handshake TLS entre os clientes SIP e os dispositivos de servidor SIP.



Note: A inspeção de SIP é ativada por padrão no Cisco Secure Firewall Threat Defense (FTD) e no Secure Firewall Adaptive Security Appliance (ASA).



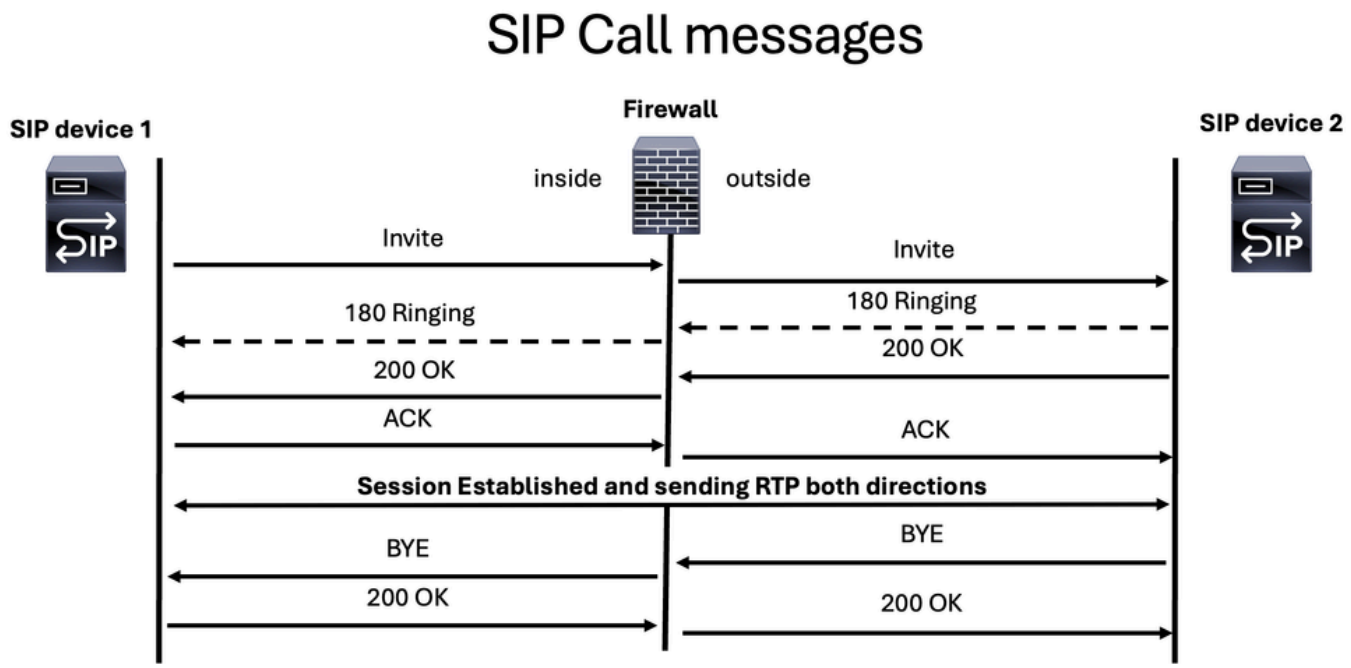
Caution: Sempre confirme quais portas são usadas para sinalização. Lembre-se de que o protocolo SIP geralmente usa as portas 5060 ou 5061, mas algumas implantações podem desviar-se desses padrões e utilizar portas diferentes para o protocolo SIP.

Há três cenários que podem ser encontrados durante a identificação e solução de problemas de sinalização SIP:

- Mensagens de sinalização de chamada SIP
- Mensagens SIP OPTION
- mensagens SIP REGISTER

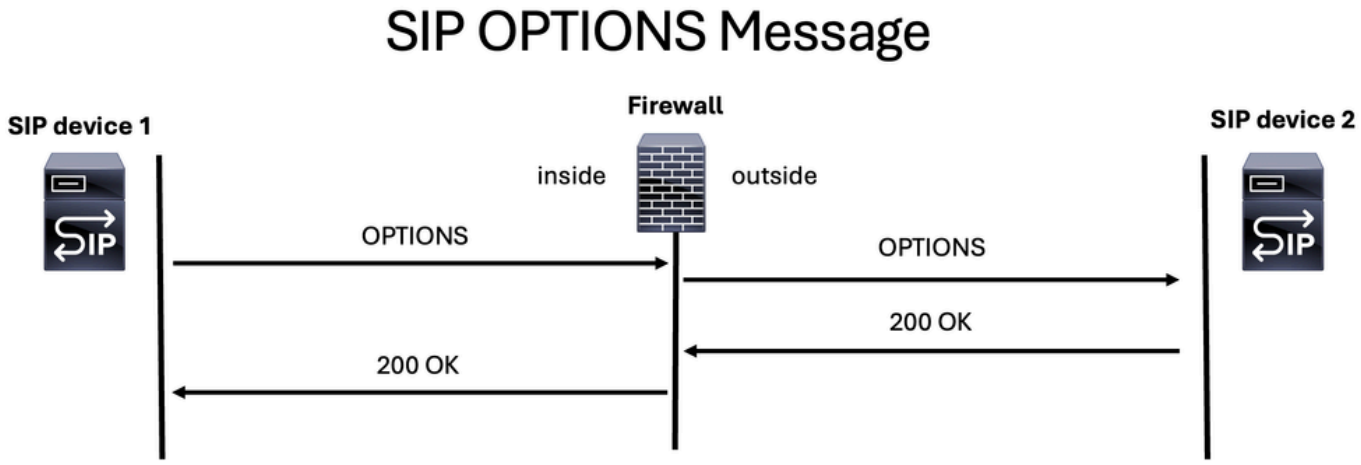
Mensagens de chamada SIP

As principais mensagens SIP para estabelecer e encerrar uma chamada de voz são:



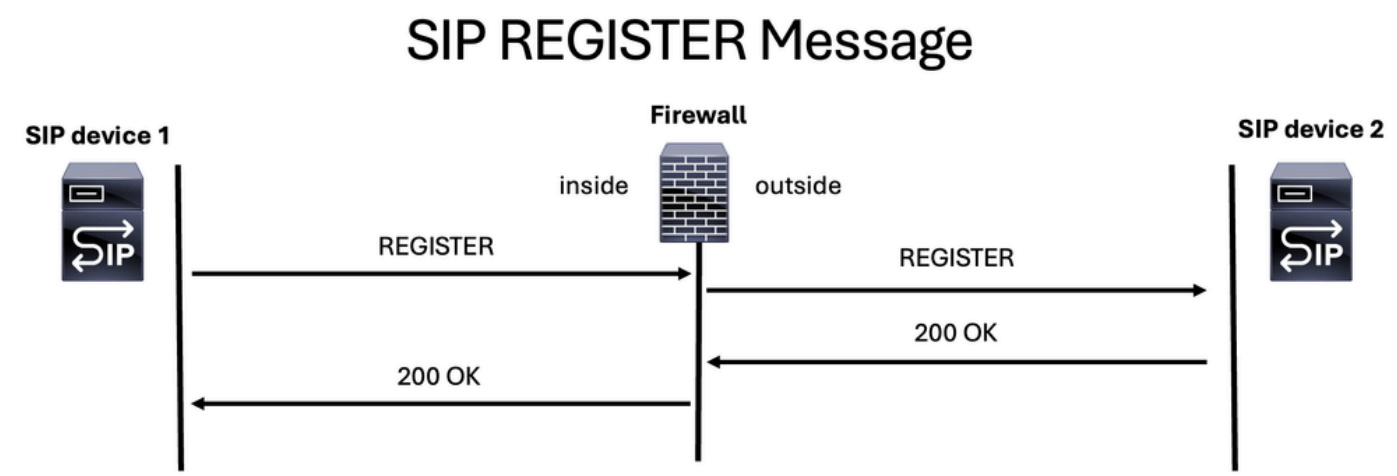
Mensagens SIP OPTION

As mensagens OPÇÕES SIP são importantes para determinar se um dispositivo SIP está on-line e é capaz de responder. É como uma mensagem ICMP de ping, mas no mundo SIP.

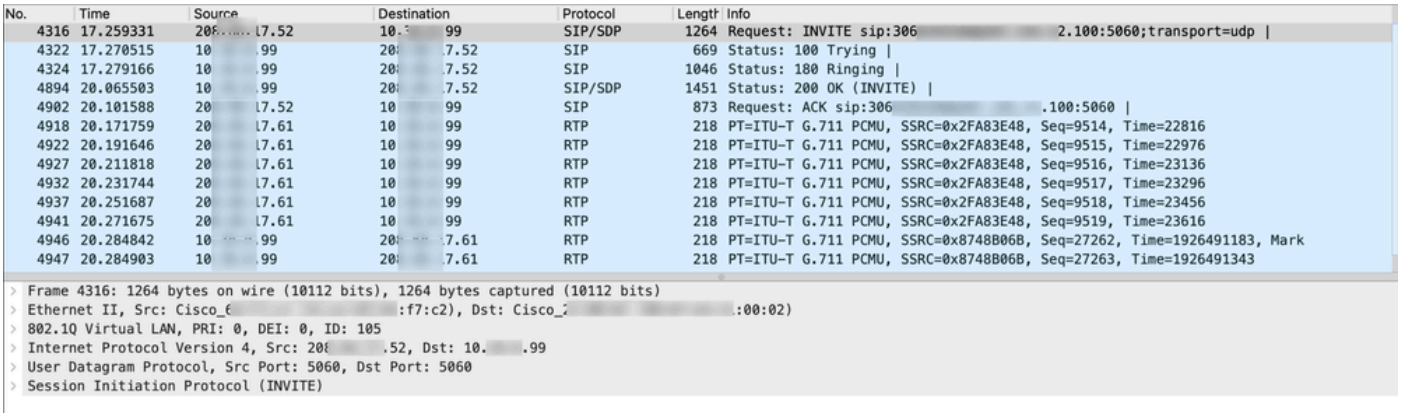


Mensagem SIP REGISTER

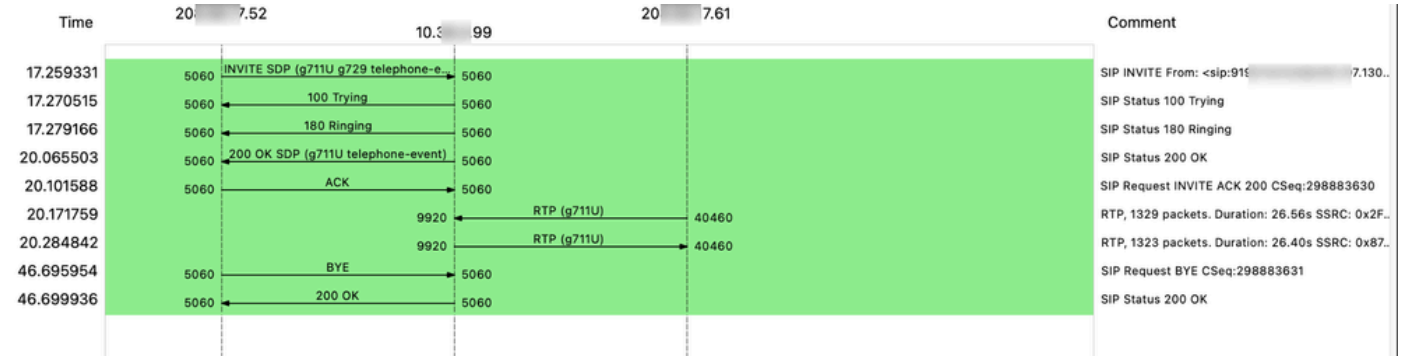
Outra mensagem SIP que você pode encontrar durante uma sessão de solução de problemas de firewall é a mensagem SIP REGISTER, que permite que um dispositivo se registre em um servidor SIP.



Esta captura de pacote mostra solicitações e respostas de dois dispositivos SIP e também o tráfego de mídia (voz):

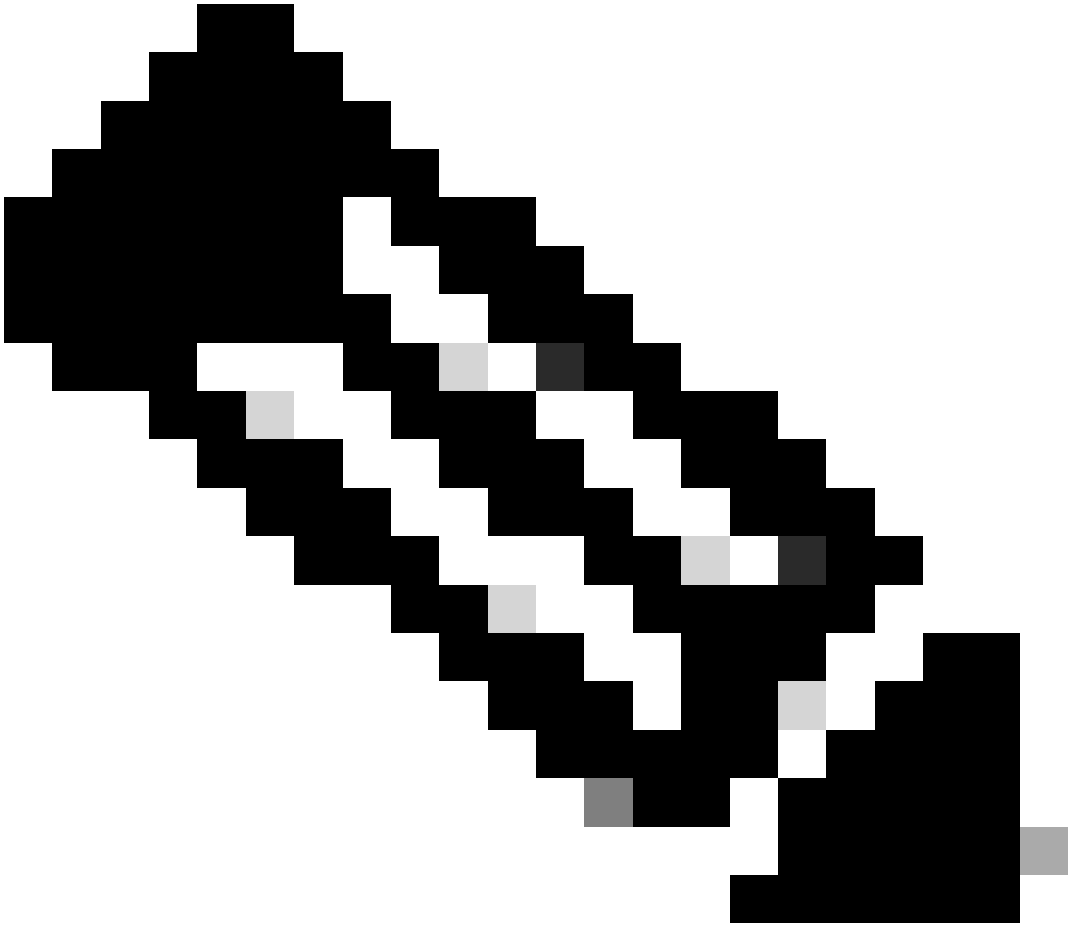


Este é um exemplo de um fluxo de sinalização SIP e mídia RTP (voz):



Protocolo de Descrição de Sessão (SDP - Session Description Protocol)

O Session Description Protocol (SDP) é uma representação padrão usada para descrever fluxos de mídia para sessões multimídia. Ele não transporta mídia em si, mas é usado para negociar o tipo de mídia e o formato entre pontos finais. O SDP é usado em conjunto com o Session Initiation Protocol (SIP) para gerenciar e negociar características de mídia para uma sessão.

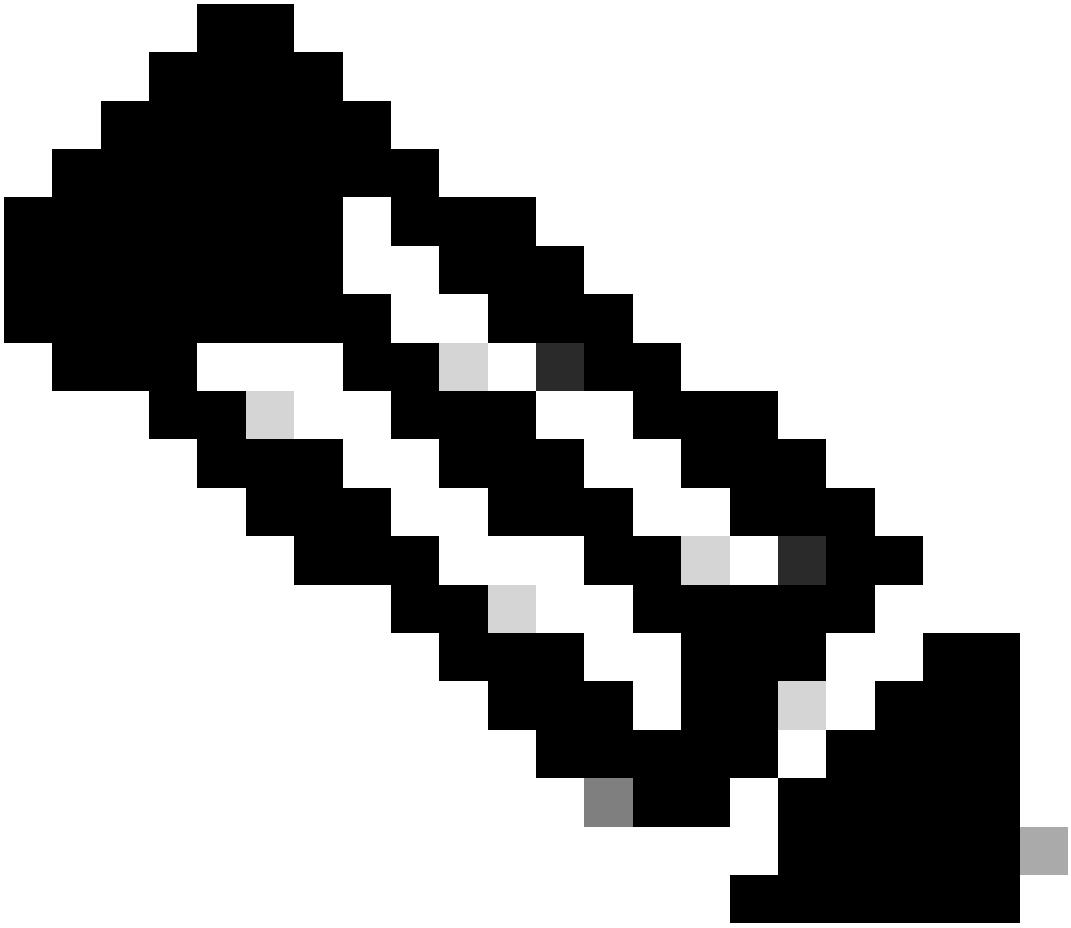


Note: O MGCP incorpora o conceito de SDP, que é utilizado para a mesma finalidade.

Este é um exemplo de mensagem SDP dentro de um protocolo 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
```



Note: Algumas das mensagens SDP contêm estes parâmetros no exemplo:

IP4 ++c-IN: Endereço IP do servidor de mídia

++m=áudio: Isso indica que o tipo de mídia é áudio.

++8266: Esse é o número da porta na qual o fluxo de áudio deve ser enviado.

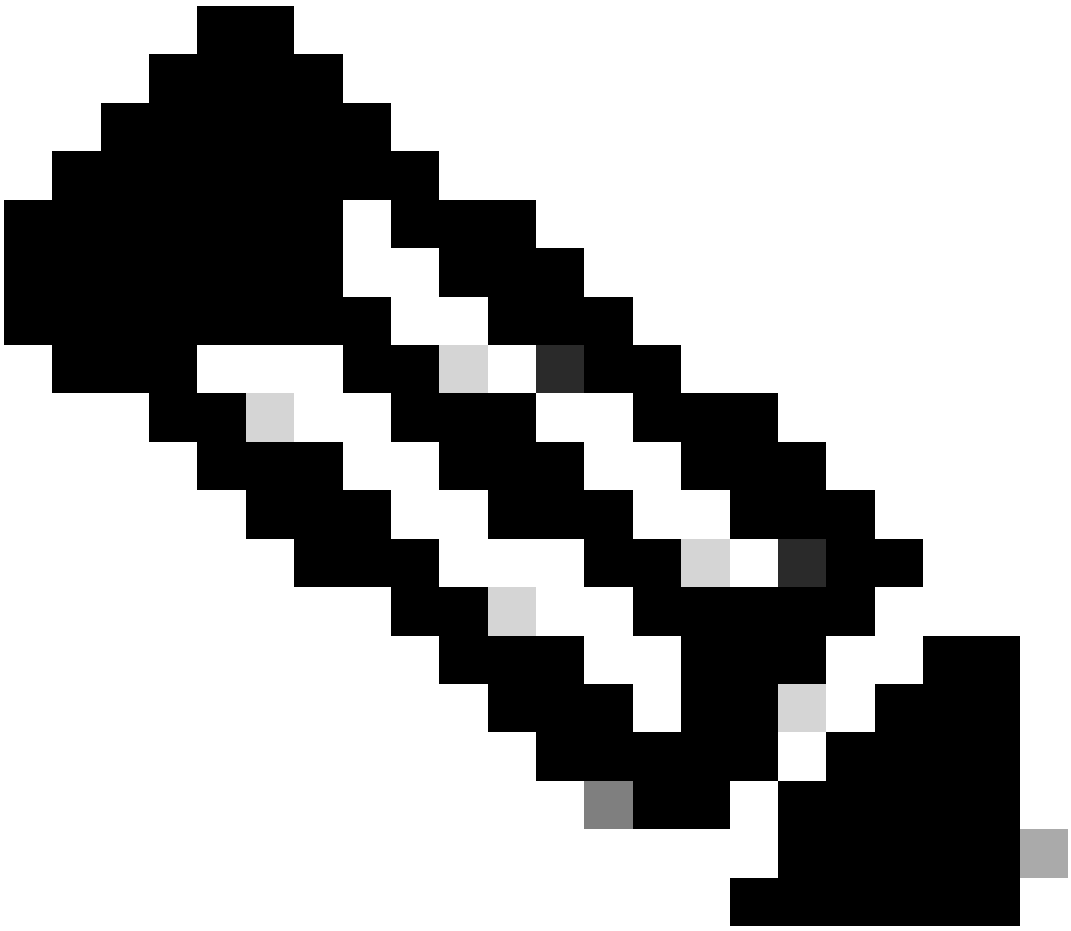
++RTP/AVP: Especifica o protocolo de transporte, que é o RTP usando o perfil de áudio/vídeo (AVP).

++18 127: Esses são os tipos de payload dos codecs de áudio. O tipo de payload 18 normalmente corresponde ao codec G.729, e 127 é um tipo de payload dinâmico que pode ser atribuído a um codec de acordo com a negociação entre os pontos finais.

O Session Description Protocol (SDP) pode ser encontrado dentro de várias mensagens SIP, como: CONVITE, 183 Sessão em Andamento, 200 OK, ACK e assim por diante. O SDP serve como um método de resposta para trocar recursos de voz e/ou vídeo entre as partes. Ao

solucionar problemas de chamada, é essencial compreender três conceitos principais:

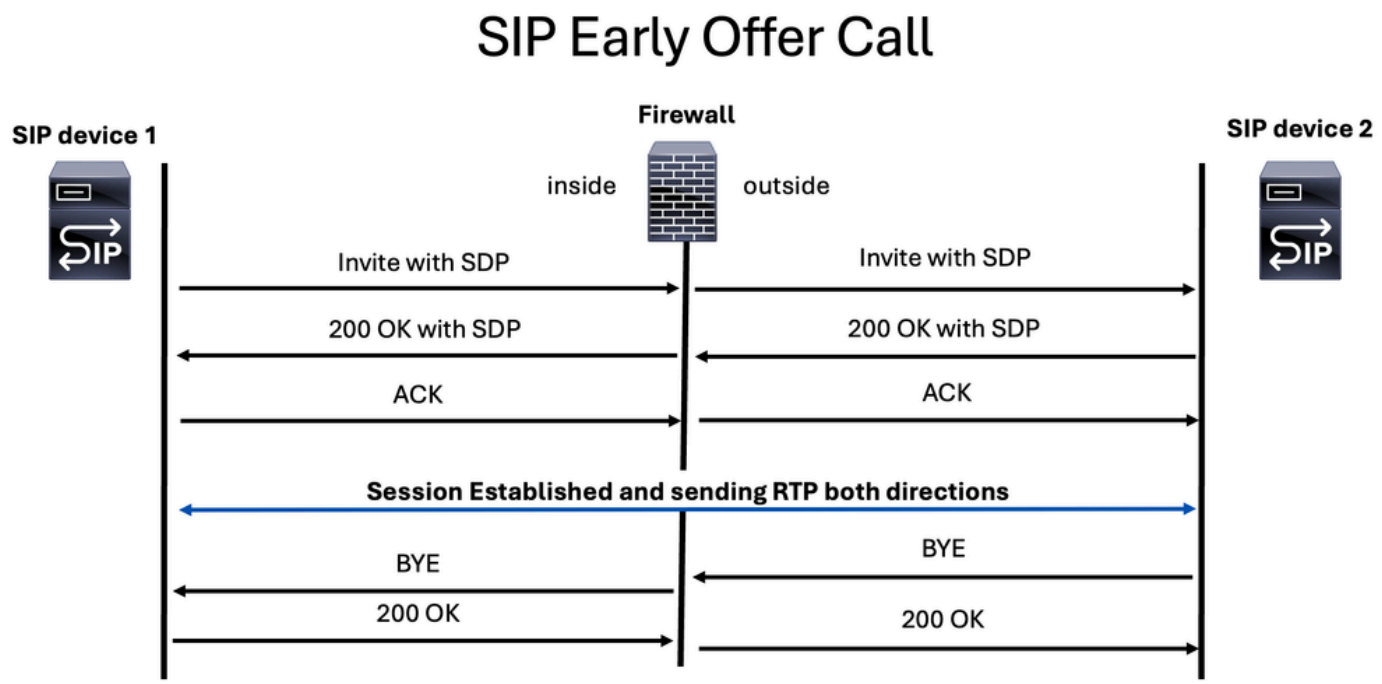
1. Oferta antecipada
2. Atrasar oferta
3. Mídia inicial



Note: É crucial entender o destino das mensagens SDP, pois o recurso de inspeção no firewall pode modificar endereços IP não apenas dentro de cabeçalhos SIP, mas também na seção SDP.

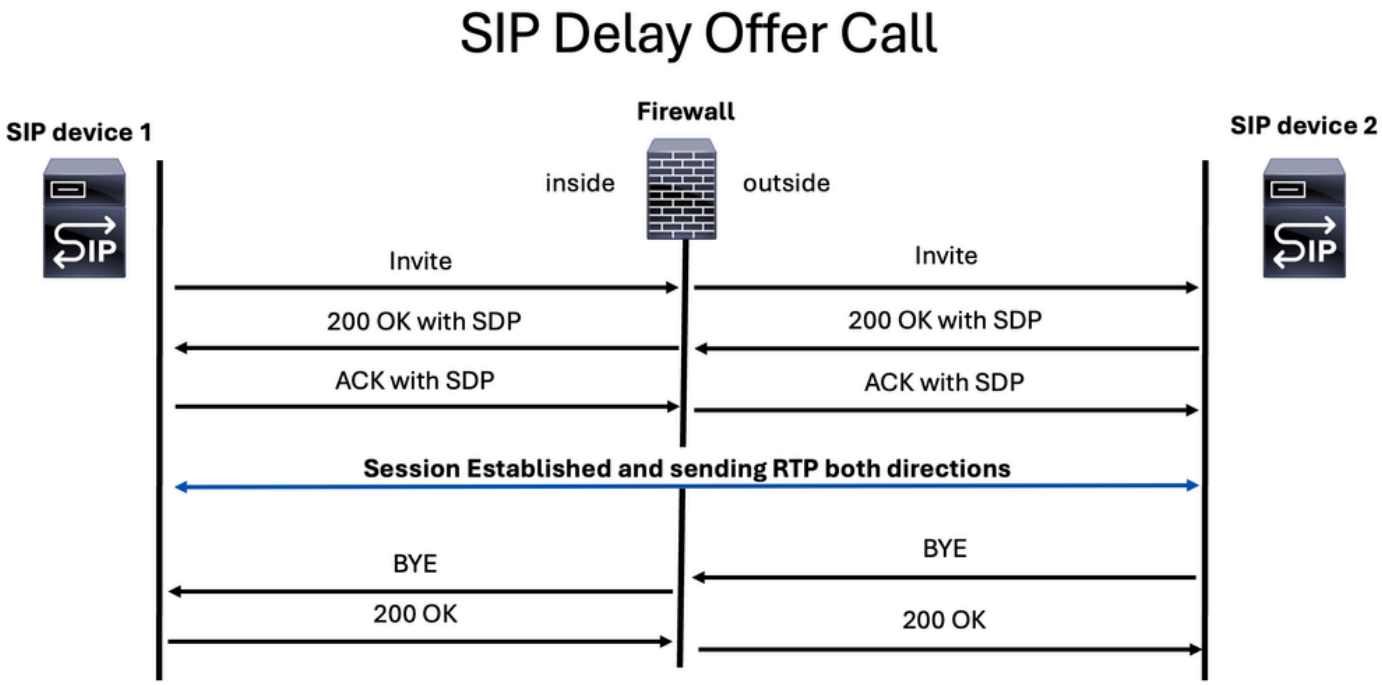
Oferta antecipada

Aqui os parâmetros de mídia no SDP são encontrados dentro das mensagens SIP INVITE e 200 OK.



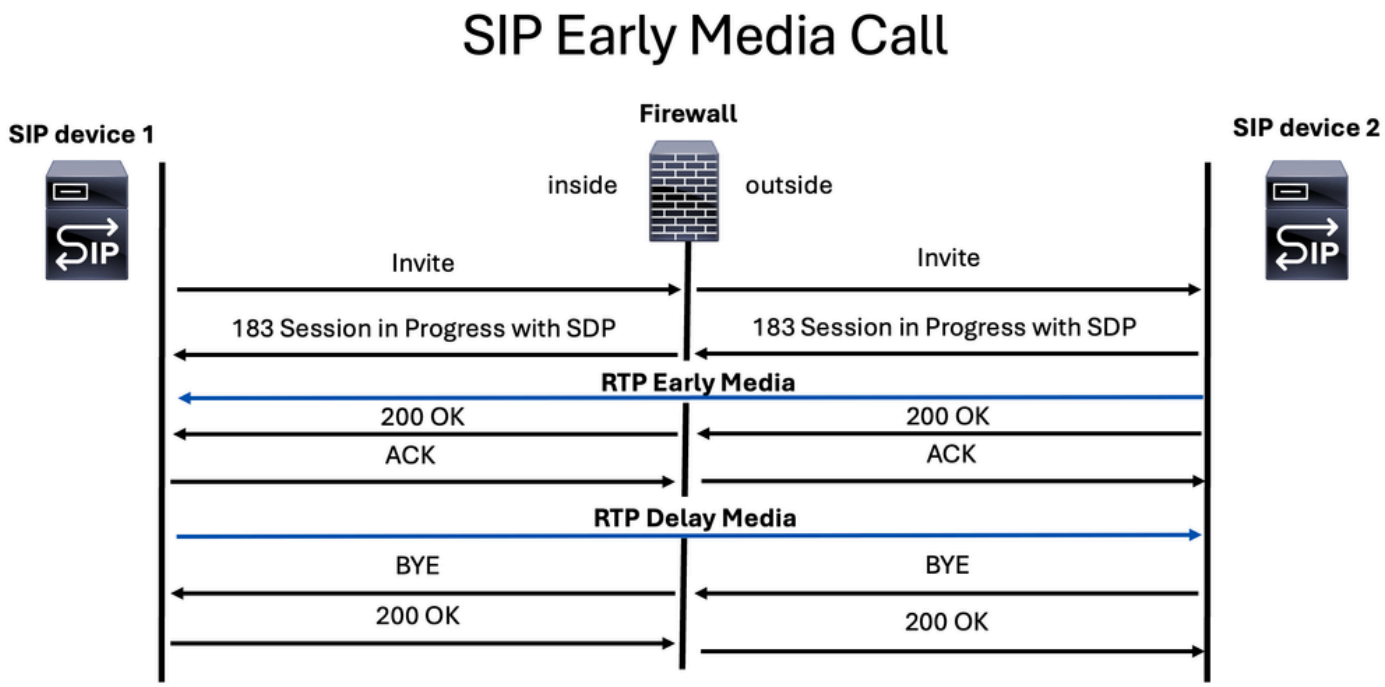
Atrasar oferta

Nesse método, o SDP é encontrado em 200 mensagens SIP OK e ACK.



Mídia inicial

A mídia inicial é transmitida por meio de uma mensagem SIP específica conhecida como resposta 183 Session Progress. Essa mensagem inclui o Session Description Protocol (SDP) que contém parâmetros de mídia para a parte chamada. Geralmente, é usado por operadoras e provedores SIP para enviar mensagens de voz automatizadas ou outras mídias para o chamador antes que a chamada seja oficialmente conectada.

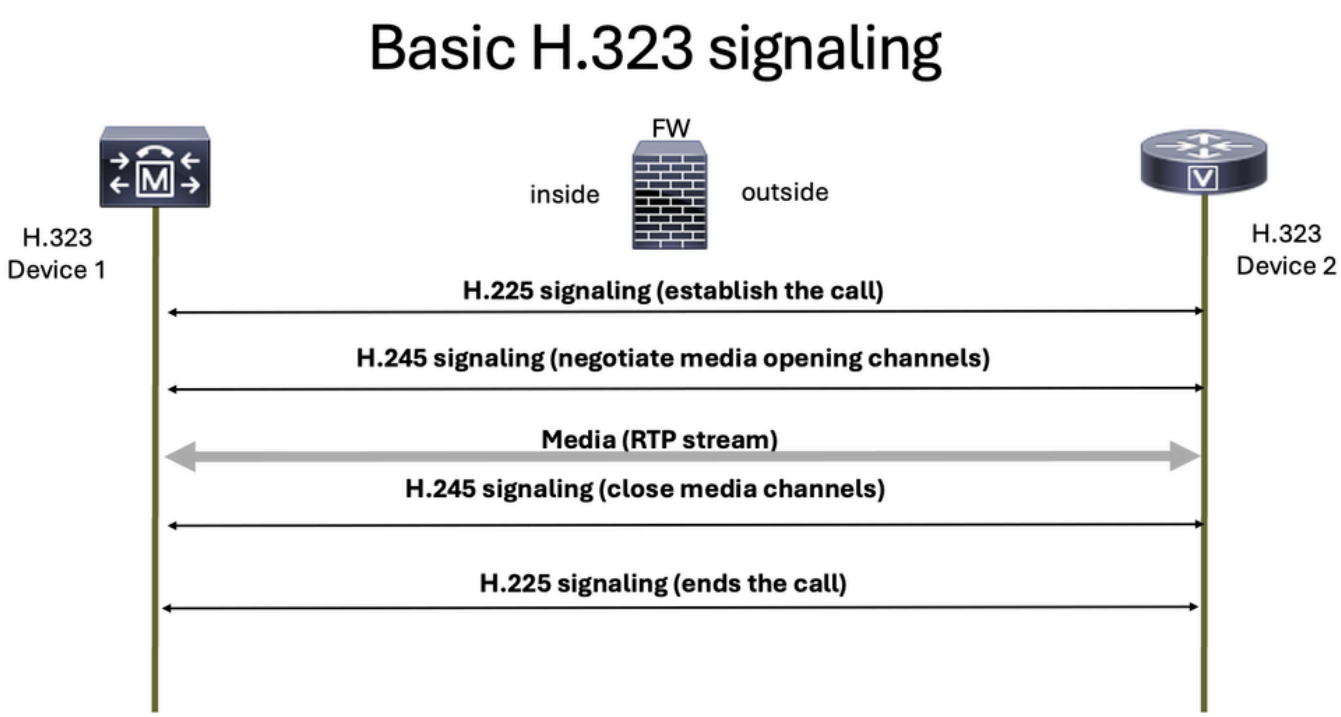


H.323

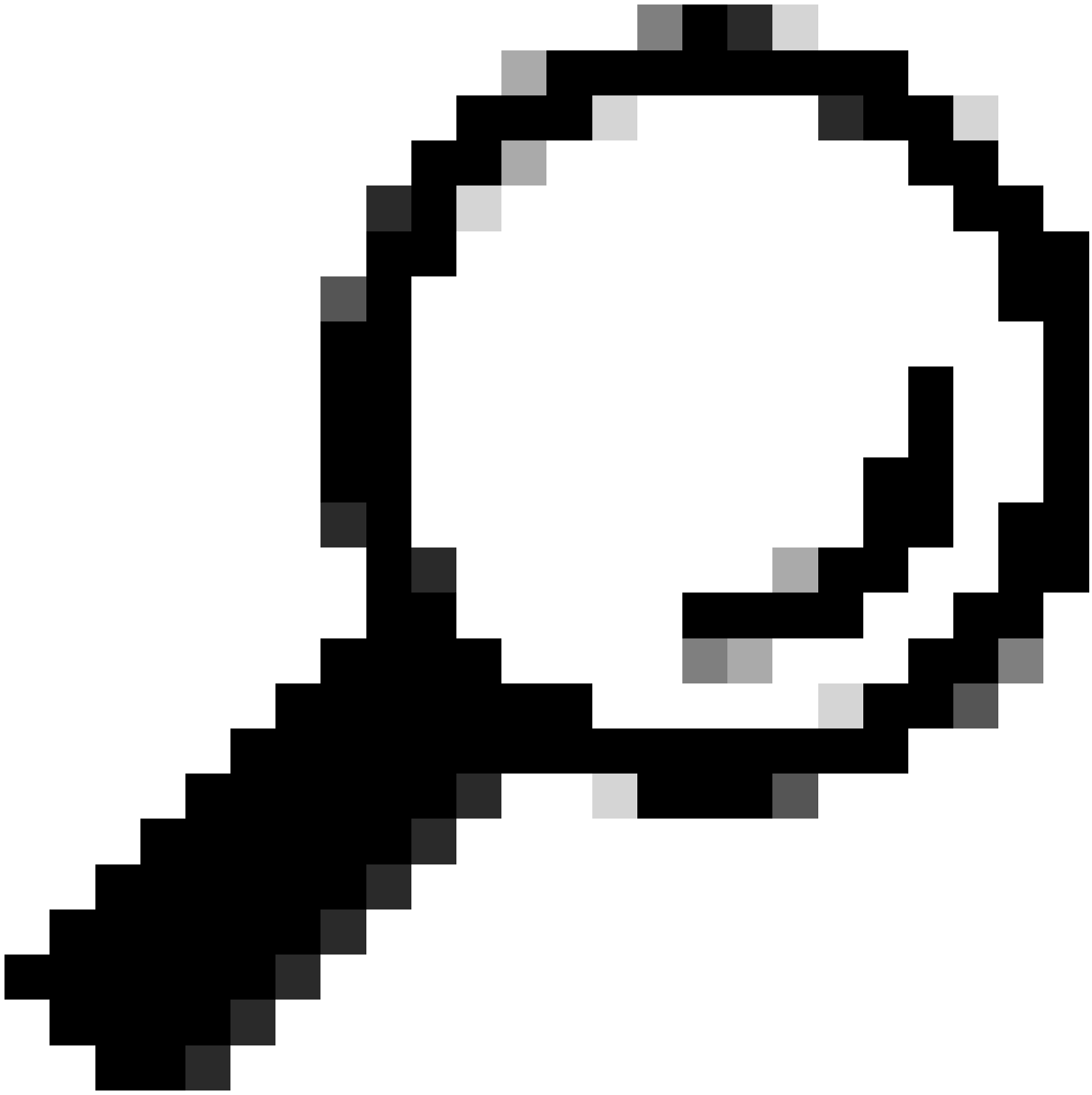
O H.323 é um conjunto de protocolos definidos pela ITU (International Telecommunication Union) para comunicações de voz, vídeo e dados em redes comutadas por pacotes, como a Internet.

O protocolo H.323 é composto de dois componentes principais:

1. H.225 Trata da sinalização de chamadas, incluindo a configuração e o encerramento de chamadas.
2. H.245: Isso é responsável pela troca de recursos e abertura e fechamento de canais para áudio e vídeo.



As portas usadas pelo protocolo de sinalização H.323 são 1718, 1719 e 1720.

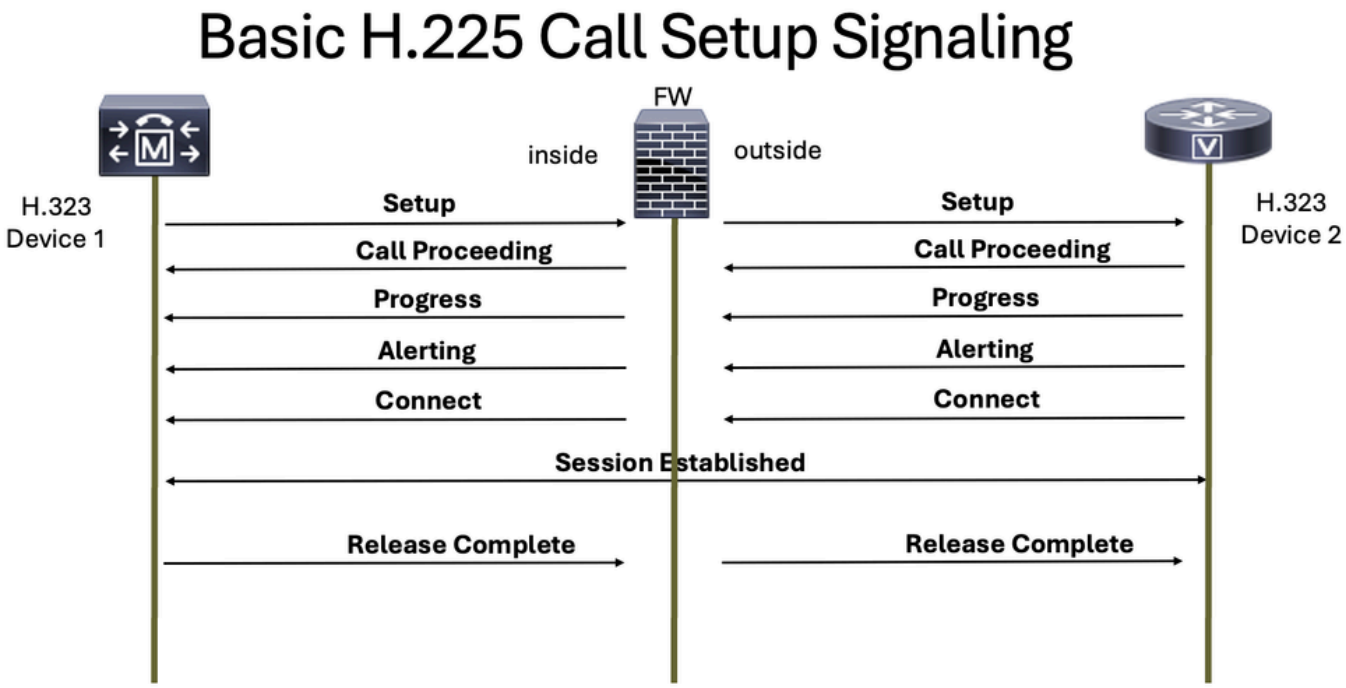


Tip: Comunicações seguras do protocolo H.323 podem encontrar problemas ao alternar de UDP para TCP devido ao uso de TLS para criptografia, o que pode fazer com que um firewall bloqueie a conexão por engano como atividade suspeita; portanto, é crucial configurar o firewall para permitir tráfego UDP e TCP para terminais ou servidores H.323.

O H.323 é um protocolo que tem dois modos de operação: início lento e início rápido.

H.225

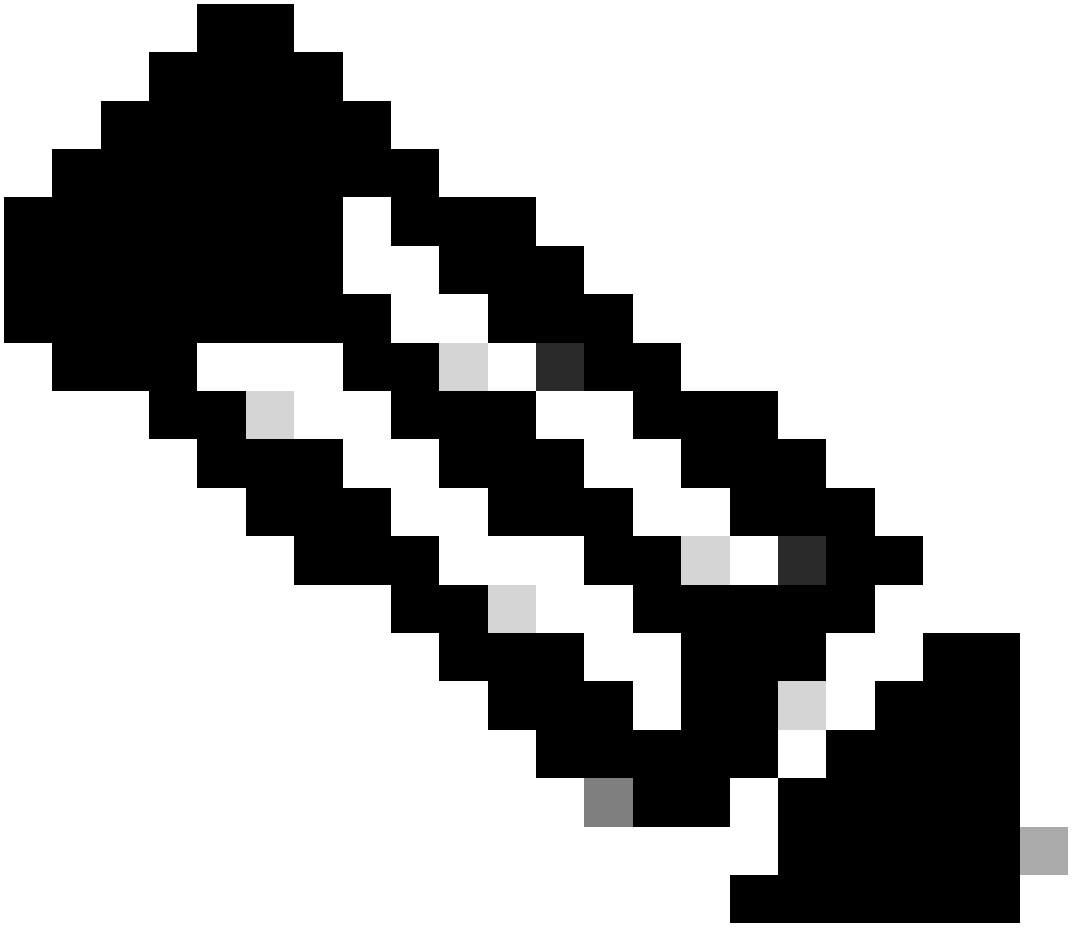
Esse protocolo é responsável por configurar a chamada e encerrar uma chamada de voz quando uma das partes desliga.



H.245

O H.245 oferece as seguintes funcionalidades:

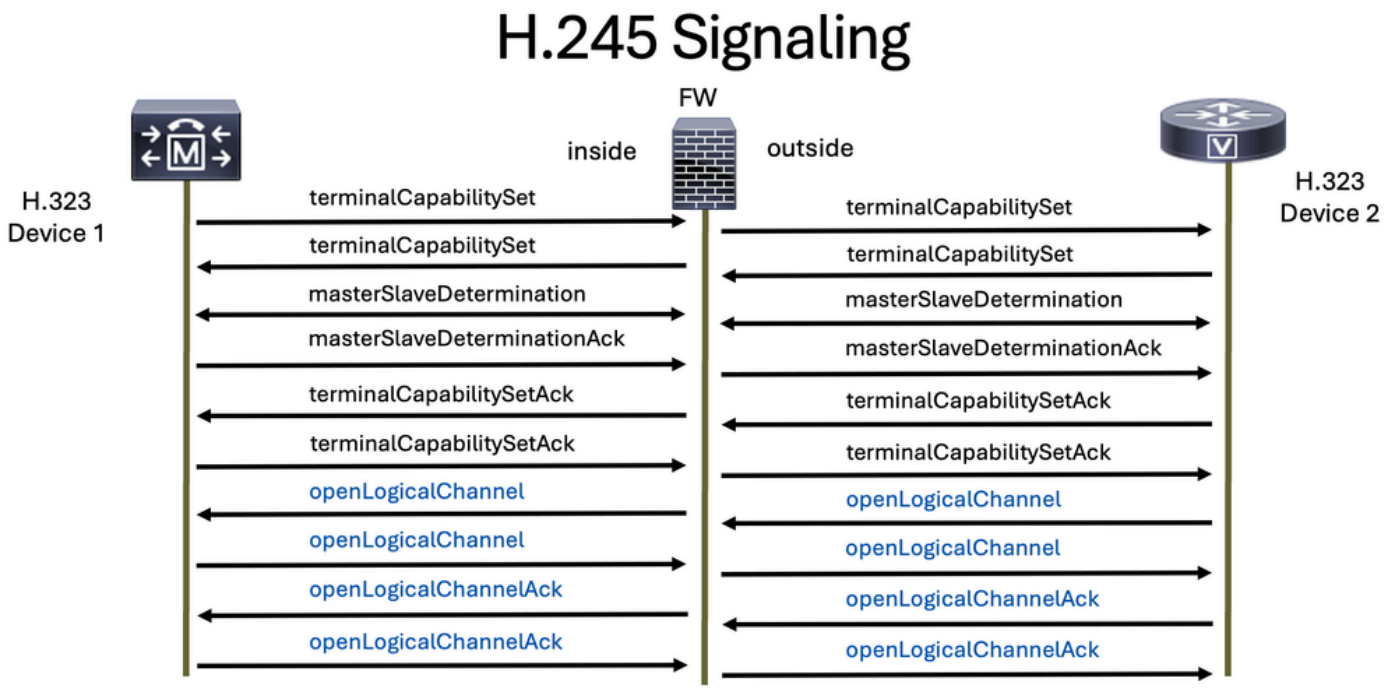
- Terminal Capability Exchange
- Determinações Master/Slave
- Sinalização de canal lógico



Note: Os termos Mestre e Escravo usados neste documento são codificados no protocolo H.323 original e não refletem as políticas ou valores de nossa empresa. Estamos comprometidos em promover uma linguagem inclusiva e respeitosa.

O protocolo H.245 é enviado após o recebimento da mensagem de conexão H.225.

Esse protocolo ajuda a determinar qual protocolo de voz é usado para o RTP e é especificado no canal lógico de abertura e no fechamento das mensagens do canal lógico para ele.

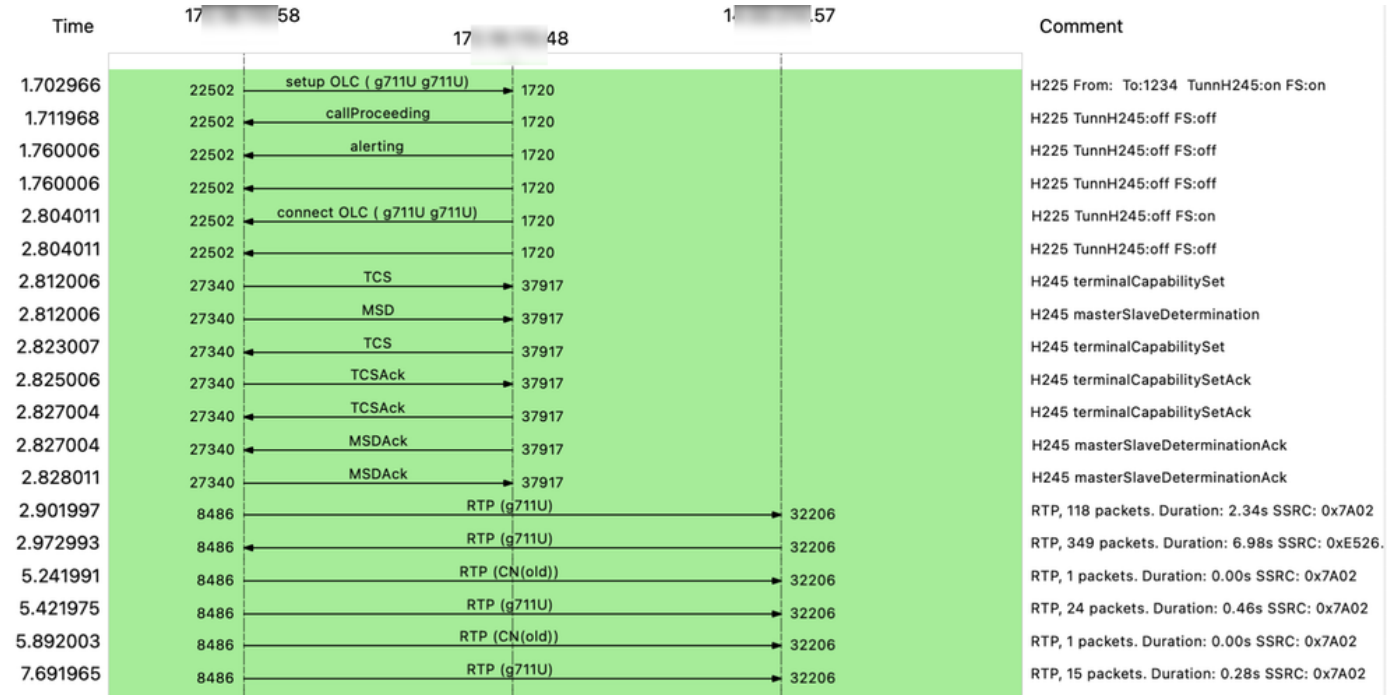


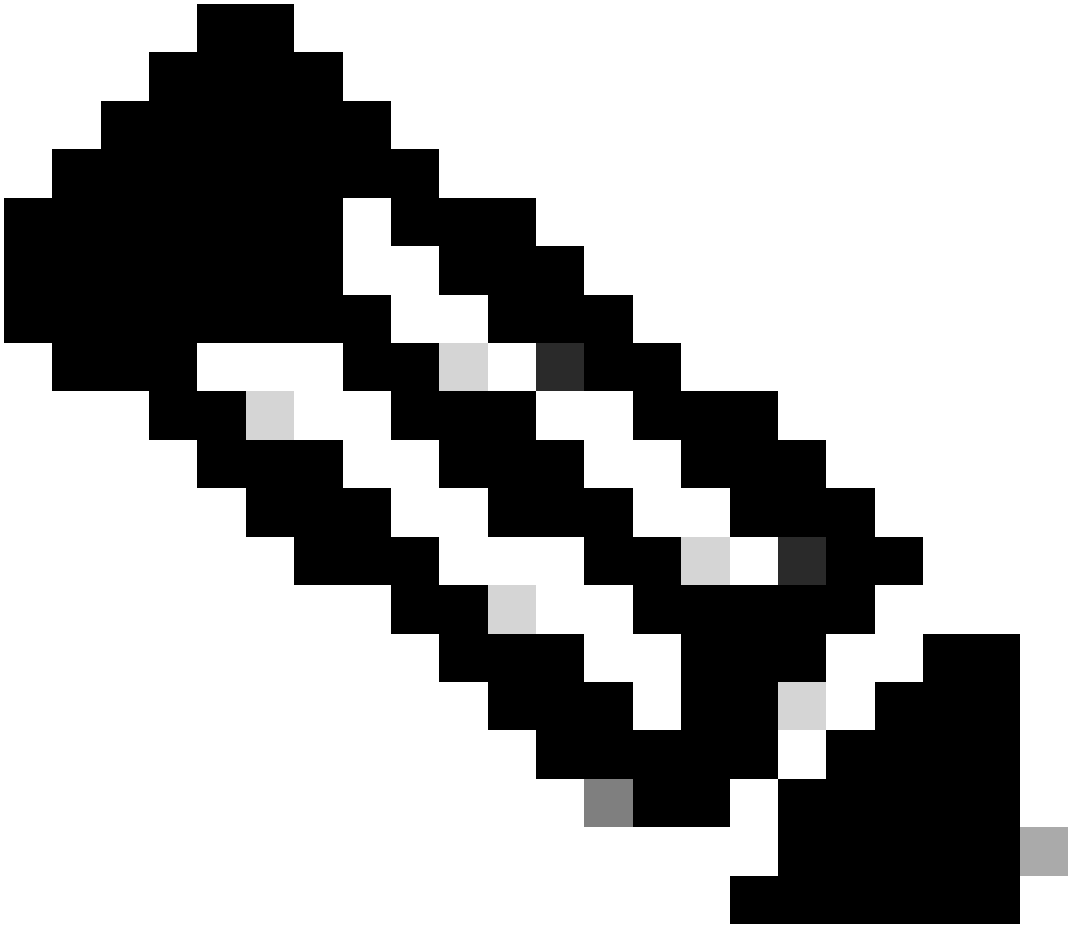
Essa captura de pacote mostra solicitações e respostas de dois dispositivos H.323 com H.225 e H.245 e também o tráfego de mídia (voz):

No.	Time	Source	Destination	Protocol	Length	Info
6	1.702966	17[redacted]58	17[redacted]48	H.225.0	683	CS: setup OpenLogicalChannel
8	1.711968	17[redacted]48	17[redacted]58	H.225.0	151	CS: callProceeding
9	1.760006	17[redacted]48	17[redacted]58	H.225.0	152	CS: alerting
10	1.760006	17[redacted]48	17[redacted]58	H.225.0	114	CS: notify
15	2.804011	17[redacted]48	17[redacted]58	H.225.0	248	CS: connect OpenLogicalChannel
16	2.804011	17[redacted]48	17[redacted]58	H.225.0	114	CS: notify
21	2.812006	17[redacted]58	17[redacted]48	H.245	135	terminalCapabilitySet
23	2.812006	17[redacted]58	17[redacted]48	H.245	68	masterSlaveDetermination
25	2.823007	17[redacted]48	17[redacted]58	H.245	176	terminalCapabilitySet
26	2.825006	17[redacted]58	17[redacted]48	H.245	65	terminalCapabilitySetAck
27	2.827004	17[redacted]48	17[redacted]58	H.245	65	terminalCapabilitySetAck
28	2.827004	17[redacted]48	17[redacted]58	H.245	64	masterSlaveDeterminationAck
30	2.828011	17[redacted]58	17[redacted]48	H.245	64	masterSlaveDeterminationAck
32	2.901997	17[redacted]58	14[redacted]7	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7A02, Seq=5180, Time=1424280842, Ma
33	2.922001	17[redacted]58	14[redacted]7	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7A02, Seq=5181, Time=1424281002
34	2.942004	17[redacted]58	14[redacted]7	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7A02, Seq=5182, Time=1424281162
35	2.961992	17[redacted]58	14[redacted]7	RTP	218	PT=ITU-T G.711 PCMU, SSRC=0x7A02, Seq=5183, Time=1424281322
36	2.972993	1[redacted]57	17[redacted]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 ([redacted]:9a:00), Dst: V[redacted]:84:d2:80)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 249
> Internet Protocol Version 4, Src: 17[redacted]58, Dst: 17[redacted]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
```

Este é um exemplo de um fluxo de sinalização H.323 com H.225 e H.245 e mídia RTP (voz):

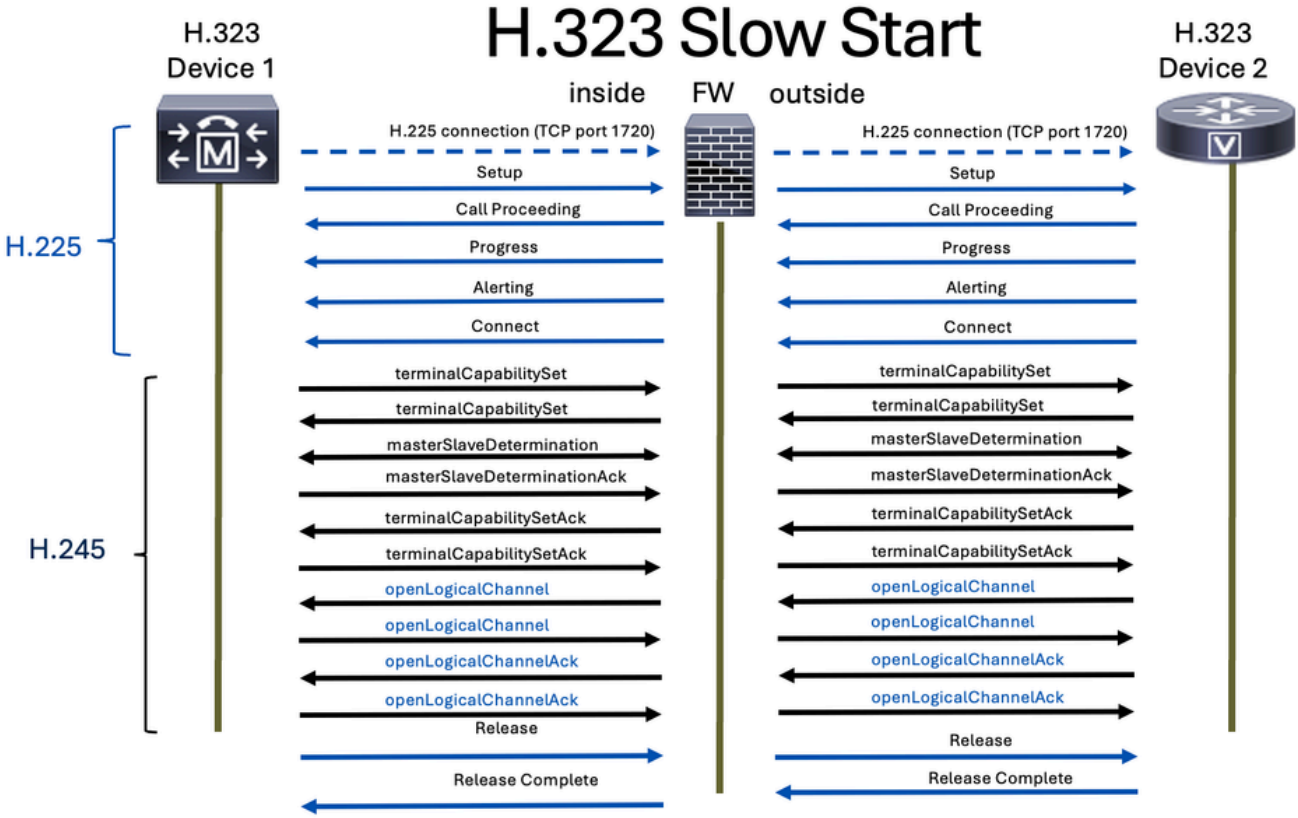

Time
Comment
1.702966 22502 setup OLC (g711U g711U) 1720 H225 From: To:1234 TunnH245:on FS:on
1.711968 22502 callProceeding 1720 H225 TunnH245:off FS:off
1.760006 22502 alerting 1720 H225 TunnH245:off FS:off
1.760006 22502 1720 H225 TunnH245:off FS:off
2.804011 22502 connect OLC (g711U g711U) 1720 H225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



Note: A inspeção H.323 é ativada por padrão no Cisco Secure Firewall Threat Defense (FTD) e no Secure Firewall Adaptive Security Appliance (ASA).

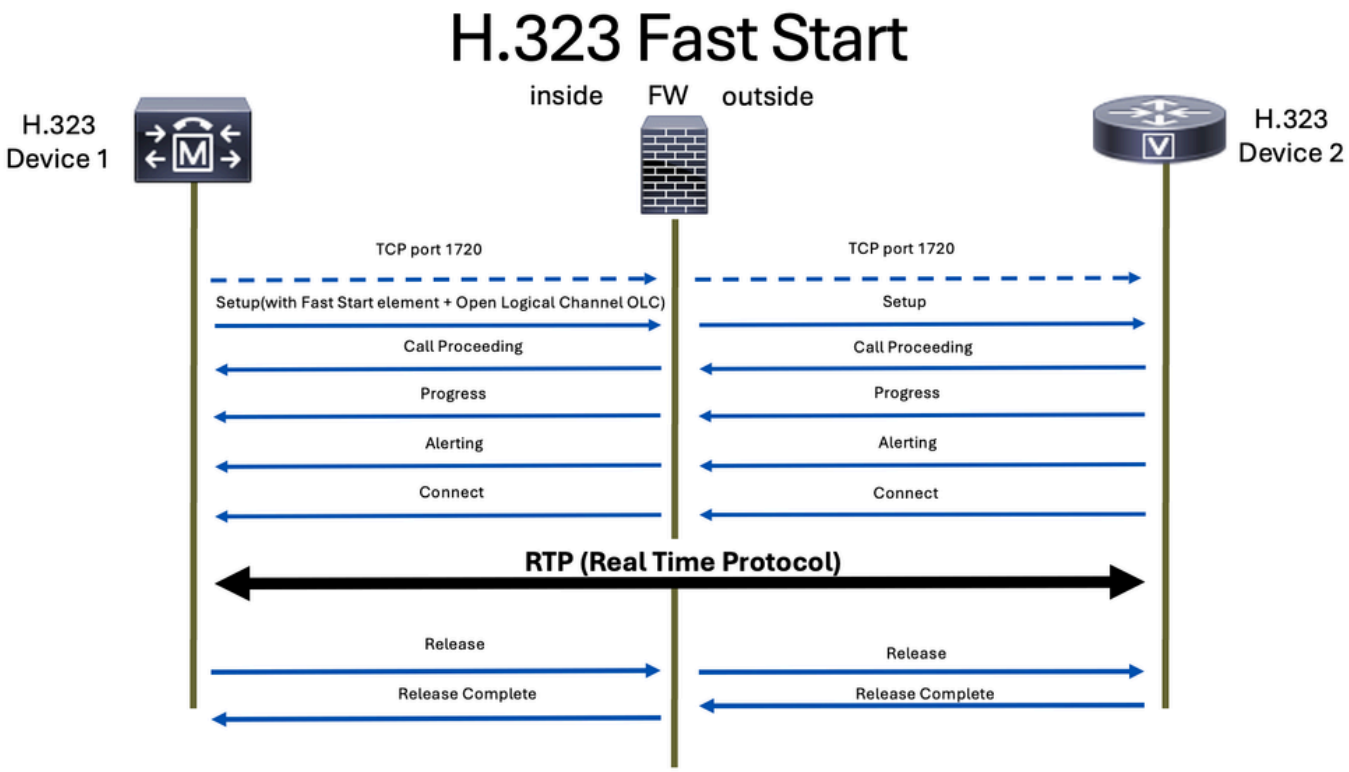
Início lento

No modo de início lento, o processo de configuração de chamada envolve várias etapas de sinalização antes que os canais de mídia sejam estabelecidos. As etapas incluem Configuração, Continuação de chamada, Alerta e Conectar. Após essas etapas, a negociação de mídia H.245 é executada separadamente. Isso significa que os canais de mídia não são estabelecidos até que a sinalização de chamada inicial seja concluída, o que pode resultar em um tempo de configuração mais longo.



Início rápido

Por outro lado, o modo de início rápido permite que a negociação de mídia ocorra na mensagem de Configuração inicial. Isso significa que os canais de mídia podem ser estabelecidos mais rapidamente, já que a negociação é feita como parte da configuração inicial da chamada. O início rápido simplifica o processo, reduzindo o número de mensagens trocadas e a quantidade de processamento necessária antes que os canais de mídia sejam estabelecidos.

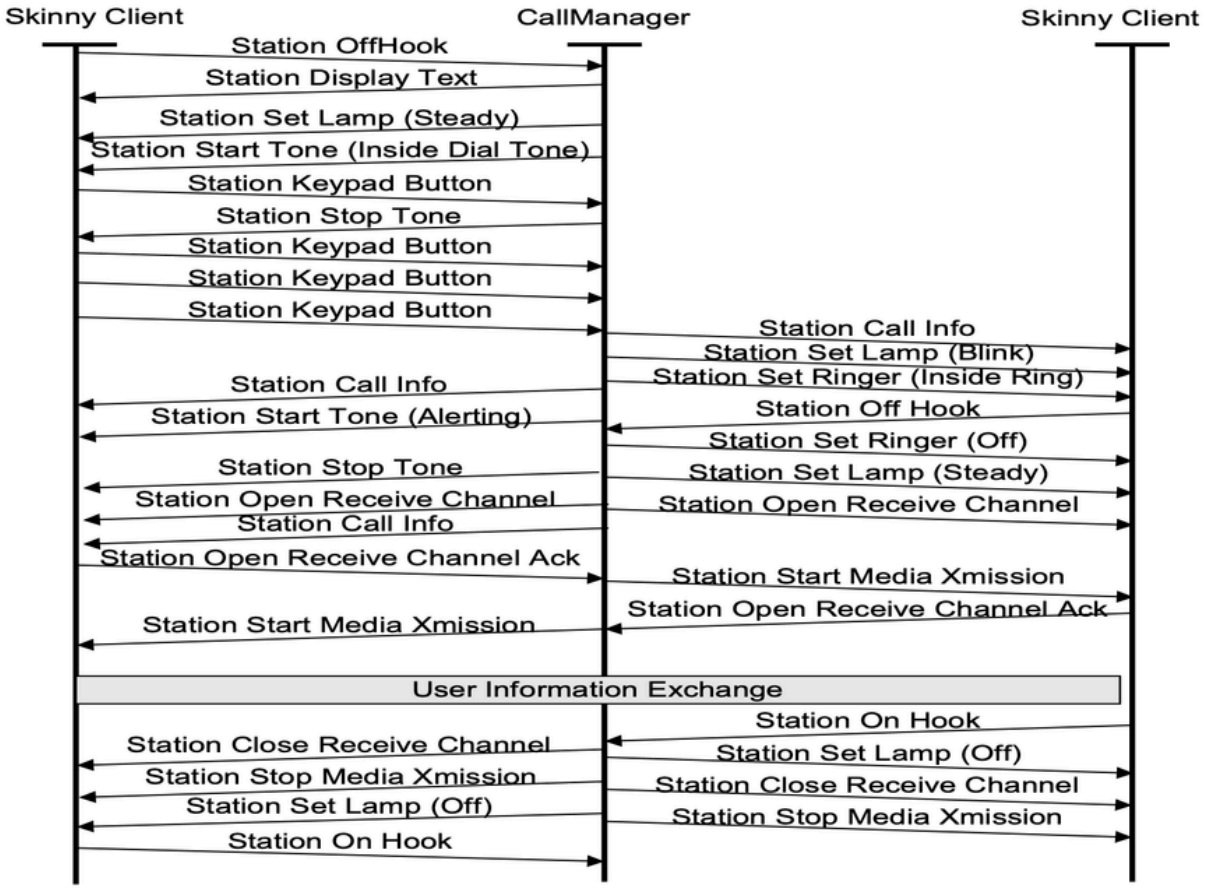


SCCP

O Skinny Client Control Protocol (SCCP), geralmente conhecido simplesmente como Skinny, é um protocolo de sinalização proprietário da Cisco. Ele é usado principalmente pelos roteadores Cisco Unified Communications Manager (CUCM), Cisco Unified Communications Manager Express (CME) e Cisco IP Phones para facilitar a configuração e o controle de chamadas.

O protocolo SCCP usa TCP na porta 2000 para SCCP não seguro e usa a porta 2443 para SCCP seguro.

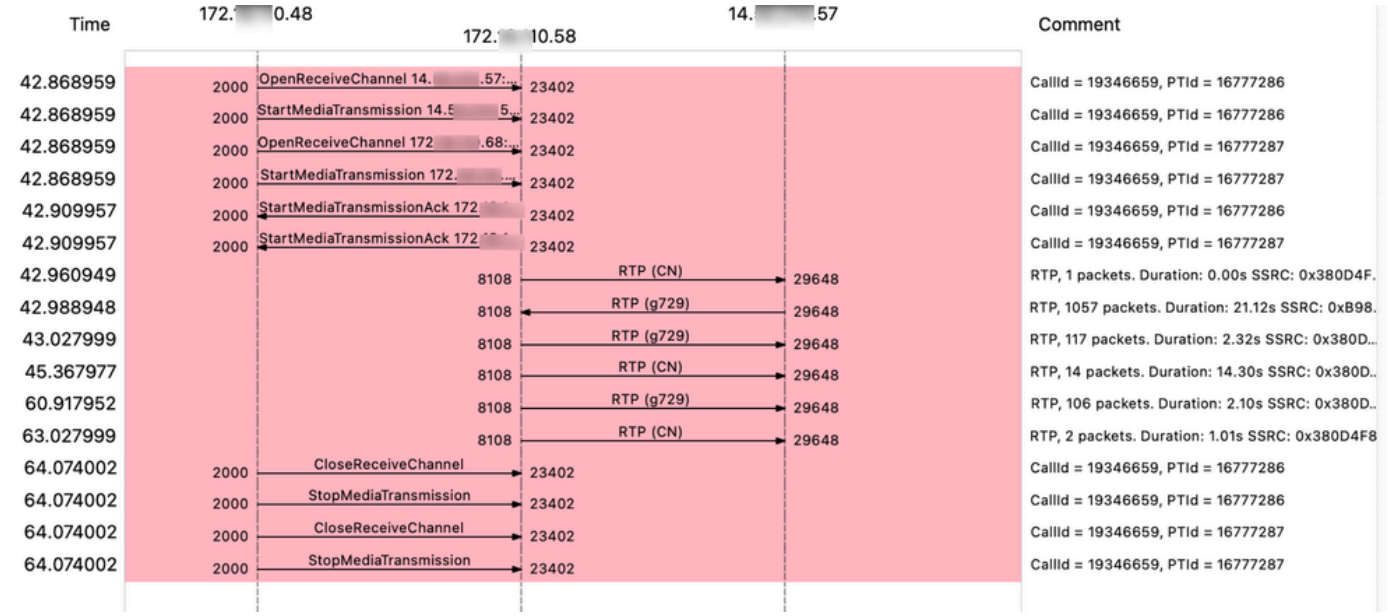
Estas são as mensagens SCCP comuns que você pode encontrar em uma chamada SCCP:

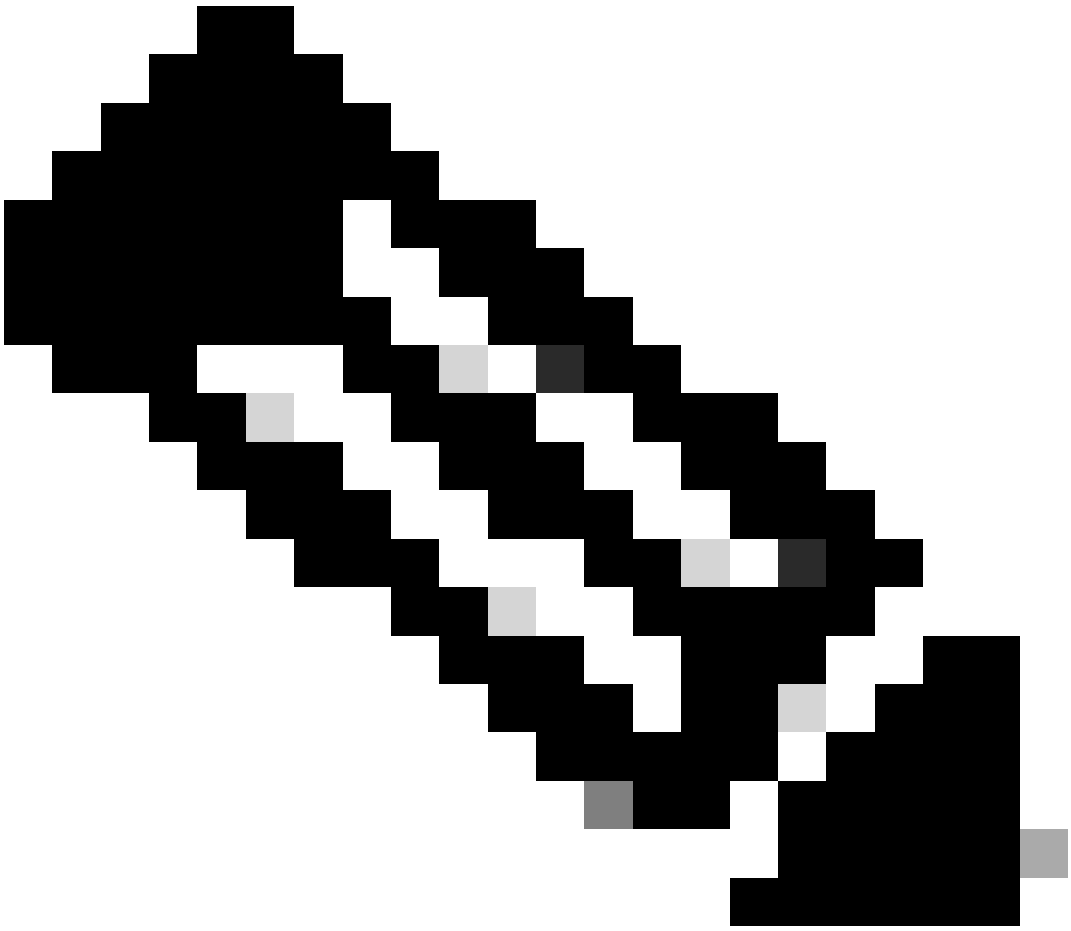


Essa captura de pacote mostra solicitações e respostas de dois dispositivos SCCP e também o tráfego de mídia (voz):

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

Este é um exemplo de um fluxo de sinalização SCCP e mídia RTP (voz):





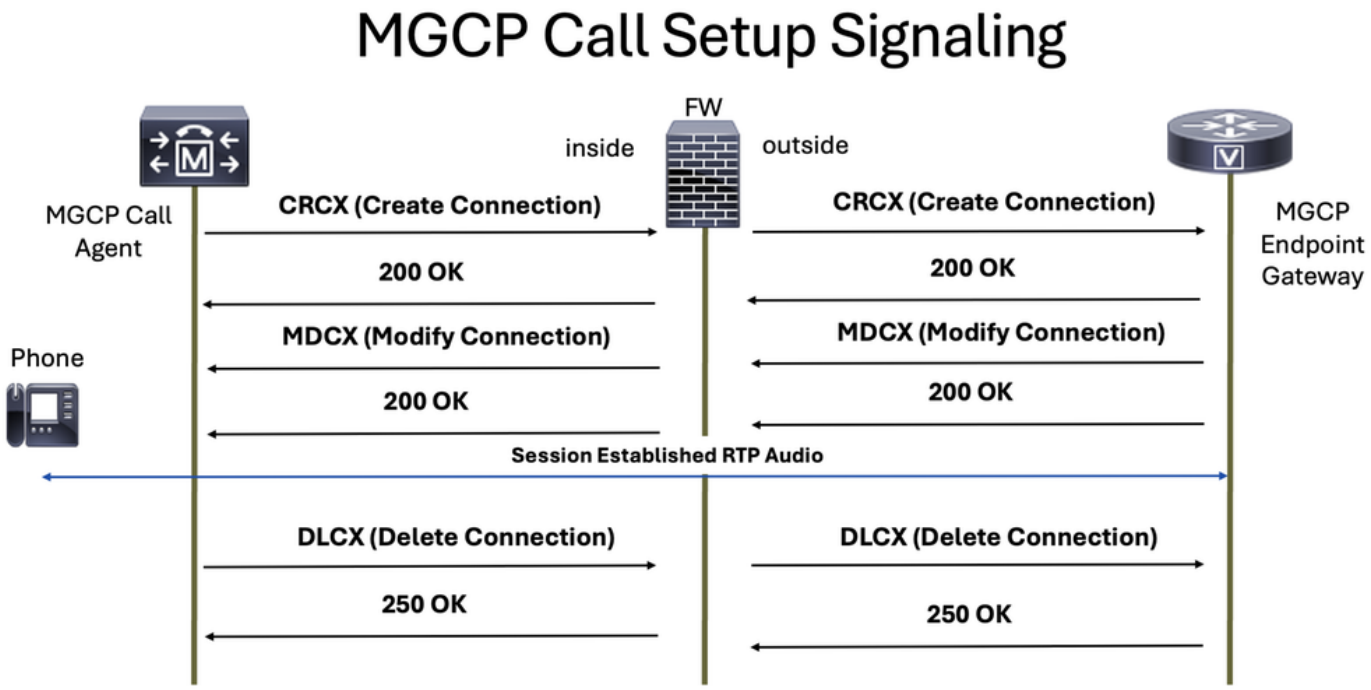
Note: A inspeção de SCCP é ativada por padrão no Cisco Secure Firewall Threat Defense (FTD) e no Secure Firewall Adaptive Security Appliance (ASA).

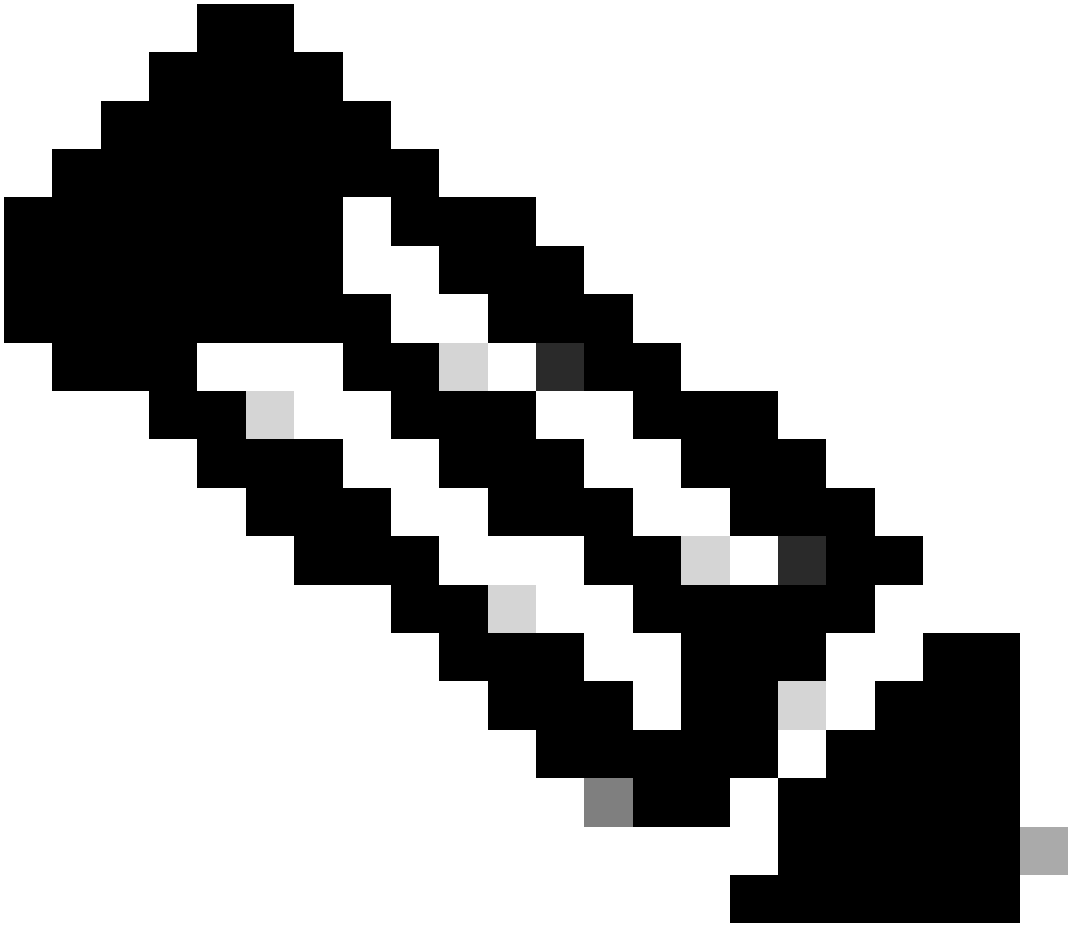
MGCP

O Media Gateway Control Protocol (MGCP) é um protocolo usado para o controle de chamadas VoIP por um dispositivo de controle de chamadas, por exemplo, CUCM.

O protocolo de sinalização MGCP é definido no RFC 2705 e usa a porta TCP 2428 e a porta UDP 2427 para comunicação.

Os pacotes normais de MGCP que você espera para uma comunicação de chamada são:



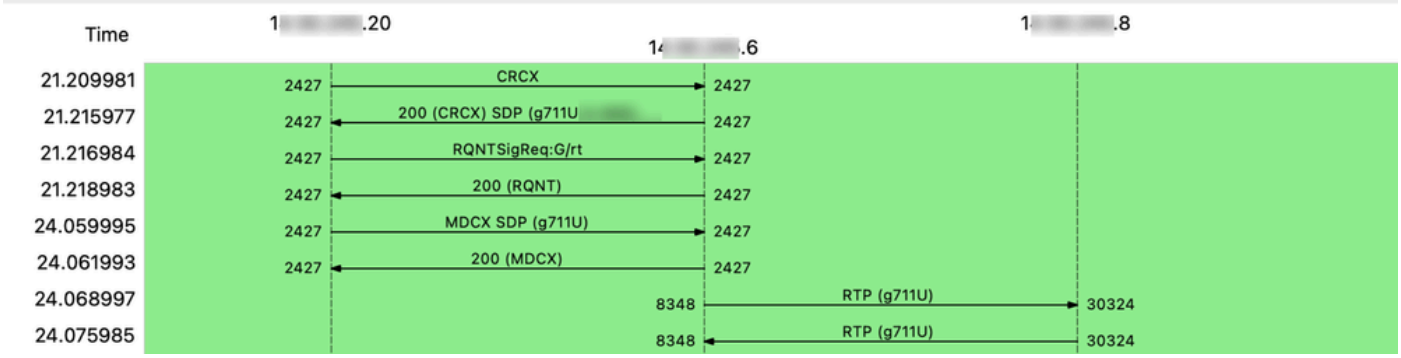


Note: A inspeção de MGCP não está habilitada na política de inspeção padrão no Cisco Secure Firewall Threat Defense (FTD) e no Secure Firewall Adaptive Security Appliance (ASA), portanto, você deve habilitá-la se precisar dessa inspeção.

Essa captura de pacote mostra solicitações e respostas de dois dispositivos MGCP e também o tráfego de mídia (voz):

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

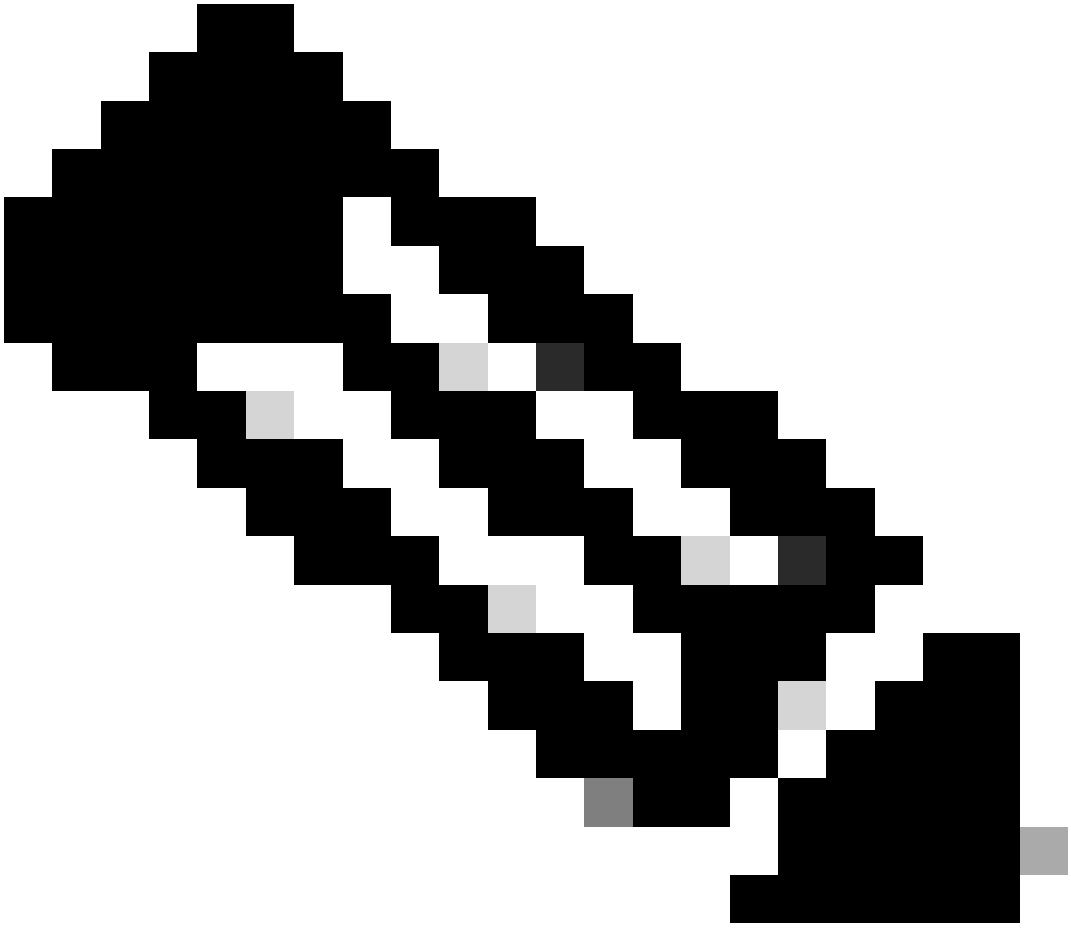
Este é um exemplo de um fluxo de sinalização MGCP e mídia RTP (voz):



Melhores práticas

Para o ASA:

- Use uma regra de permissão que permita o tráfego de e para os dois componentes de sinalização (dispositivos ou servidores). Isso pode ser limitado pelas portas usadas no protocolo VoIP de sinalização especificado.
- Permita o intervalo de portas RTP entre os dispositivos de mídia que podem enviar e/ou receber fluxos de áudio e/ou vídeo.



Note: Lembre-se de que esses dispositivos de áudio ou mídia podem ser diferentes dos componentes de sinalização (dispositivos ou servidores).

Para FTD:

- Defina regras de pré-filtro para componentes de sinalização (dispositivos ou servidores) e defina a porta específica para limitar somente o tráfego para um protocolo de sinalização específico.
- Configure o pré-filtro para o protocolo RTP de áudio e/ou vídeo.

Troubleshooting

Ao solucionar problemas de voz, você precisa saber se o problema é de sinalização ou de mídia (voz ou vídeo) ou ambos. Aqui estão alguns exemplos que podem orientá-lo a diferenciar isso:

Exemplo de problemas de sinalização:

++O usuário relata que a chamada não foi estabelecida.

++O usuário não pode chamar outros usuários ou números.

++O Tronco SIP não está sendo ativado porque a mensagem SIP OPTIONS não está obtendo resposta.

++Meu dispositivo não pode se registrar.

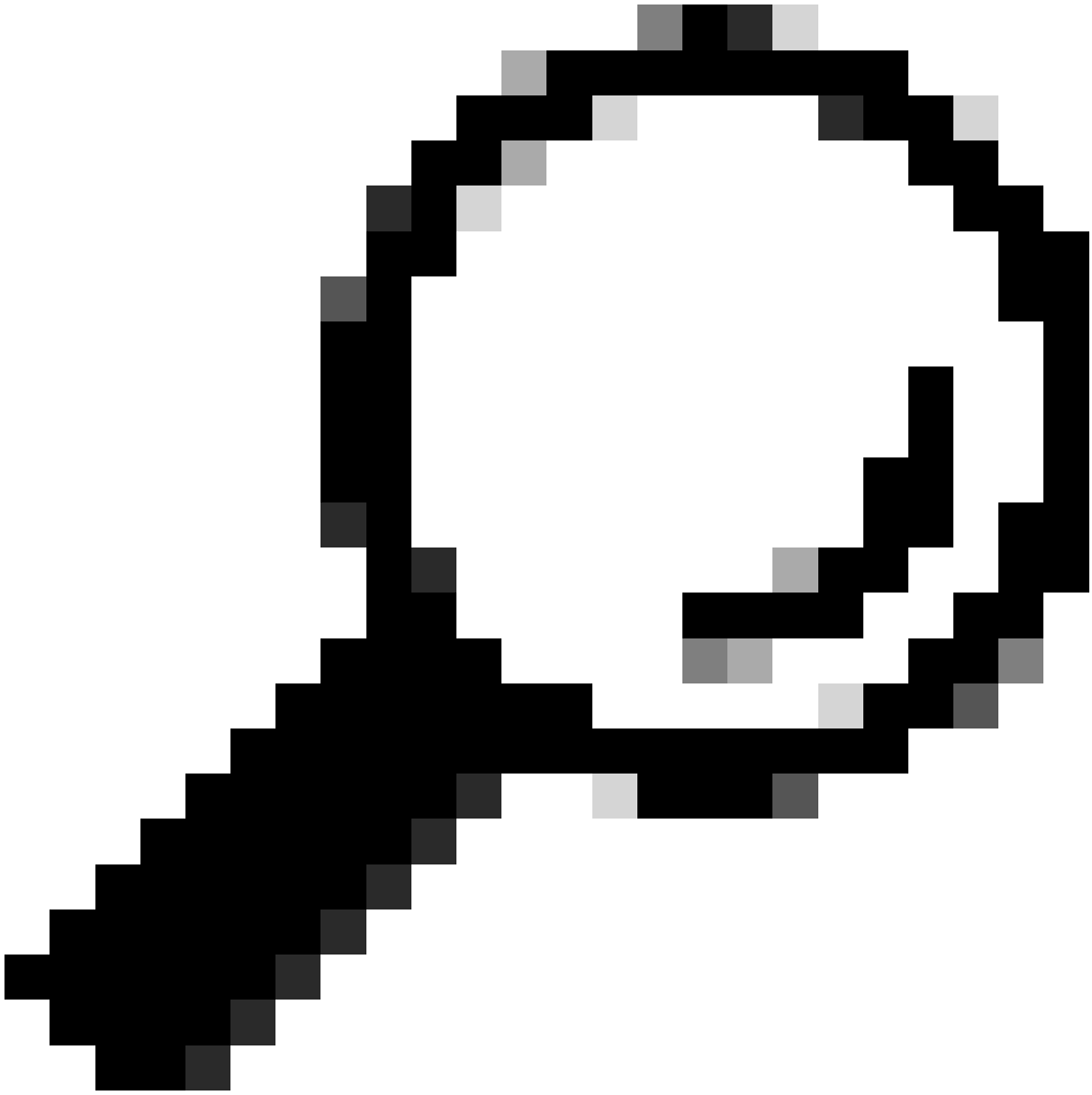
Exemplo de problemas de mídia (voz ou vídeo):

++Há um problema de áudio unidirecional.

++Não há áudio em chamada.

++Não há nenhum vídeo.

++A chamada fica em silêncio.



Tip: Durante uma chamada de vídeo, o SDP pode negociar até três linhas de mídia (linhas m): áudio, vídeo e imagem. Cada linha m corresponde a um fluxo RTP (Real-Time Transport Protocol) separado por trecho de chamada, o que significa que pode haver até três fluxos RTP distintos—um para cada tipo de mídia—em cada trecho da chamada.

Troubleshooting de Sinalização no Firewall

Para solucionar problemas da parte de sinalização, você precisa garantir que:

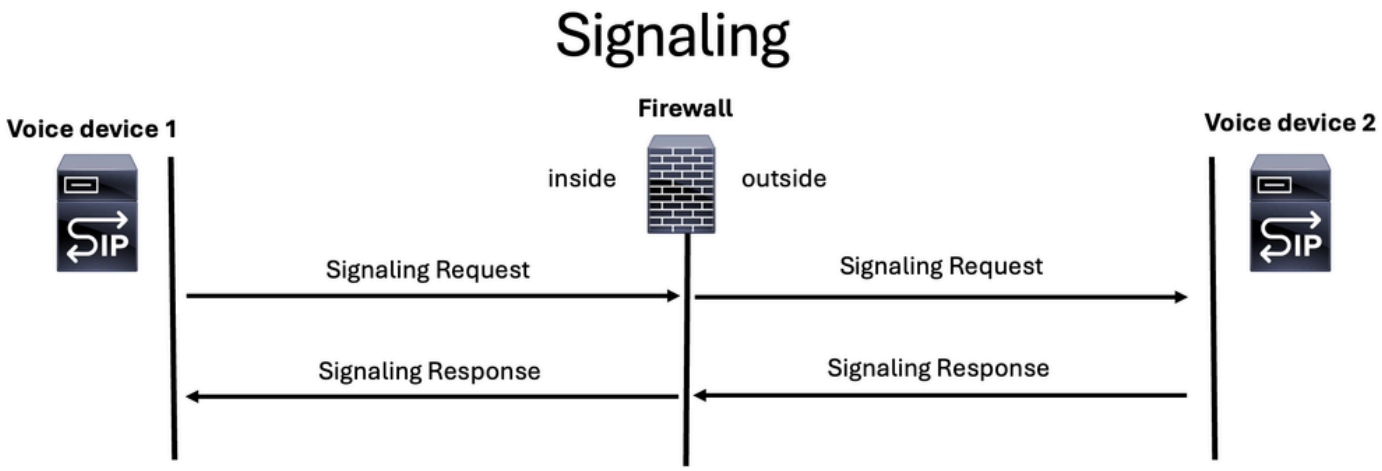
++Identifique todos os componentes de sinalização (dispositivos ou servidores) envolvidos na chamada das interfaces de entrada e saída e configure os critérios de correspondência apropriados nas capturas de pacotes no CLI de qualquer um dos FWs seguros.

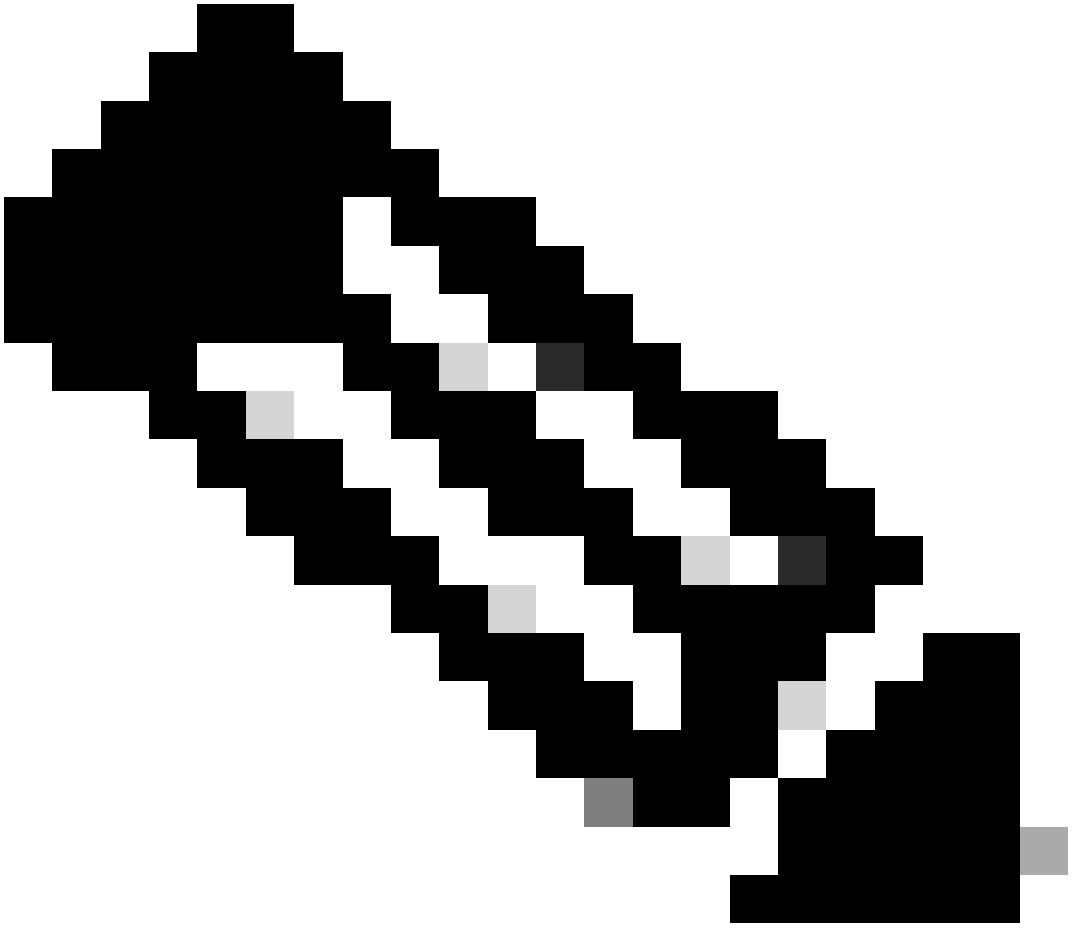
++Lembre-se de que o número de mensagens de sinalização na interface de entrada deve

corresponder à interface de saída.

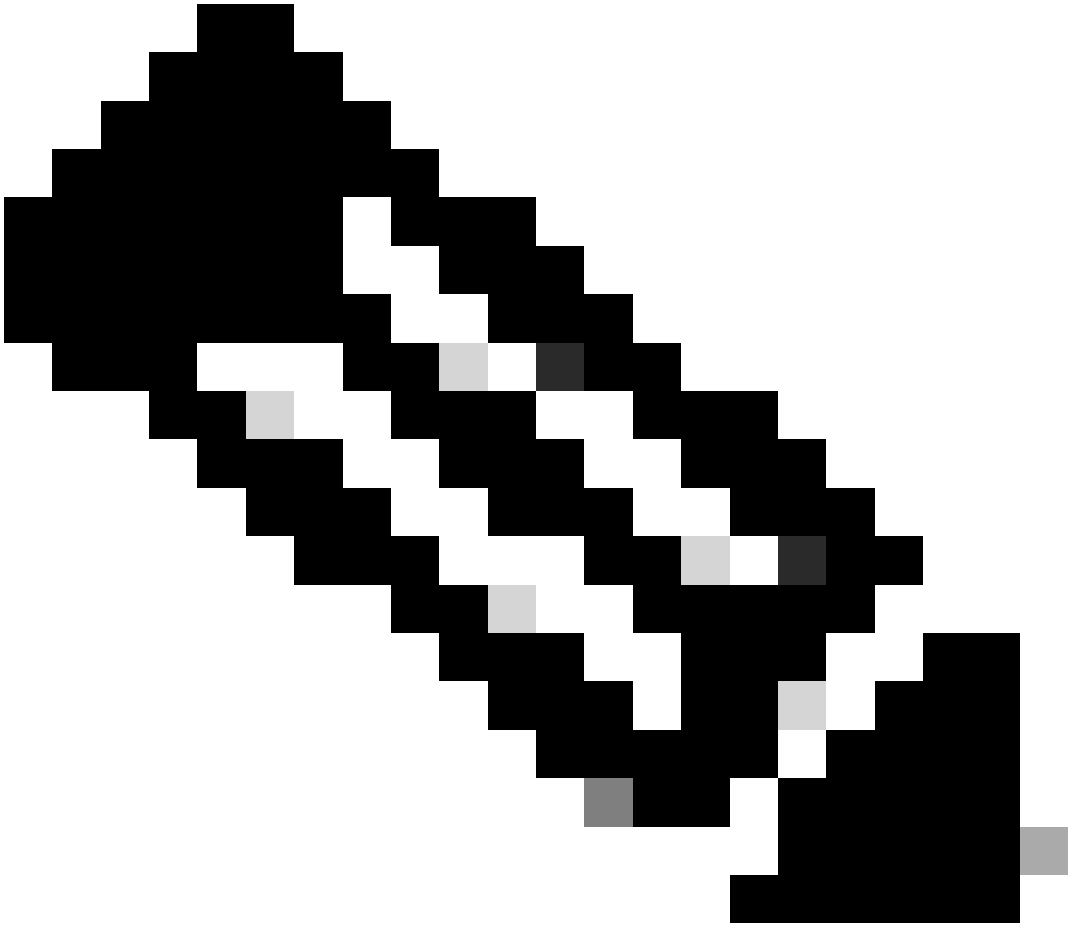
++A captura de pacotes pode se tornar mais eficiente especificando se o protocolo de sinalização usa TCP ou UDP e filtrando o número de porta esperado. Como todos os protocolos de sinalização operam sobre IP, a aplicação desses filtros na CLI ajuda a restringir a quantidade de tráfego que você vê nas capturas.

++Somente para interfaces de saída, certifique-se de que o endereço IP do NAT atribuído ao tráfego de saída esteja especificado no filtro de captura de pacotes. Isso garante que você esteja capturando o tráfego correto conforme ele aparece na interface de saída.





Observação: lembre-se de que, independentemente do protocolo de sinalização usado para voz, sempre deve haver uma solicitação e uma resposta e deve ser consistente nas interfaces de entrada e saída.

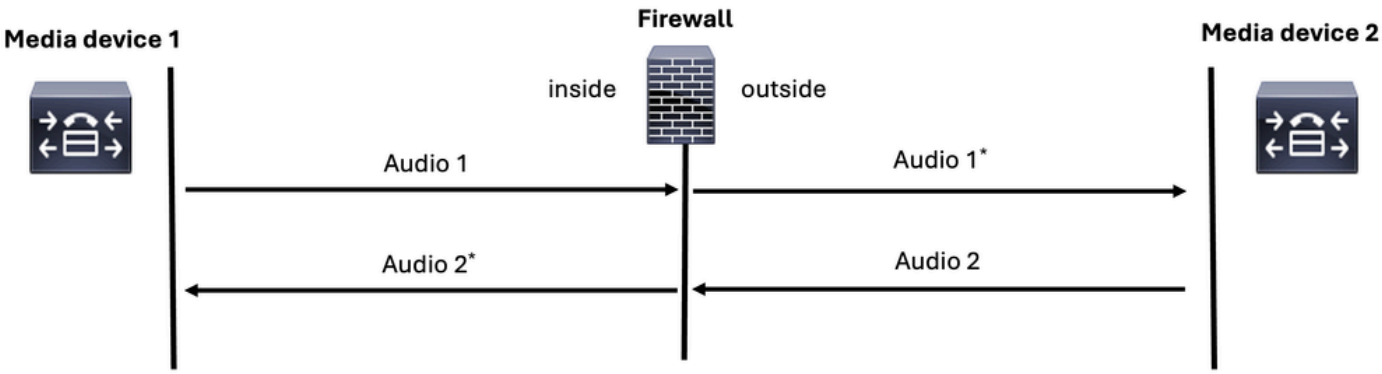


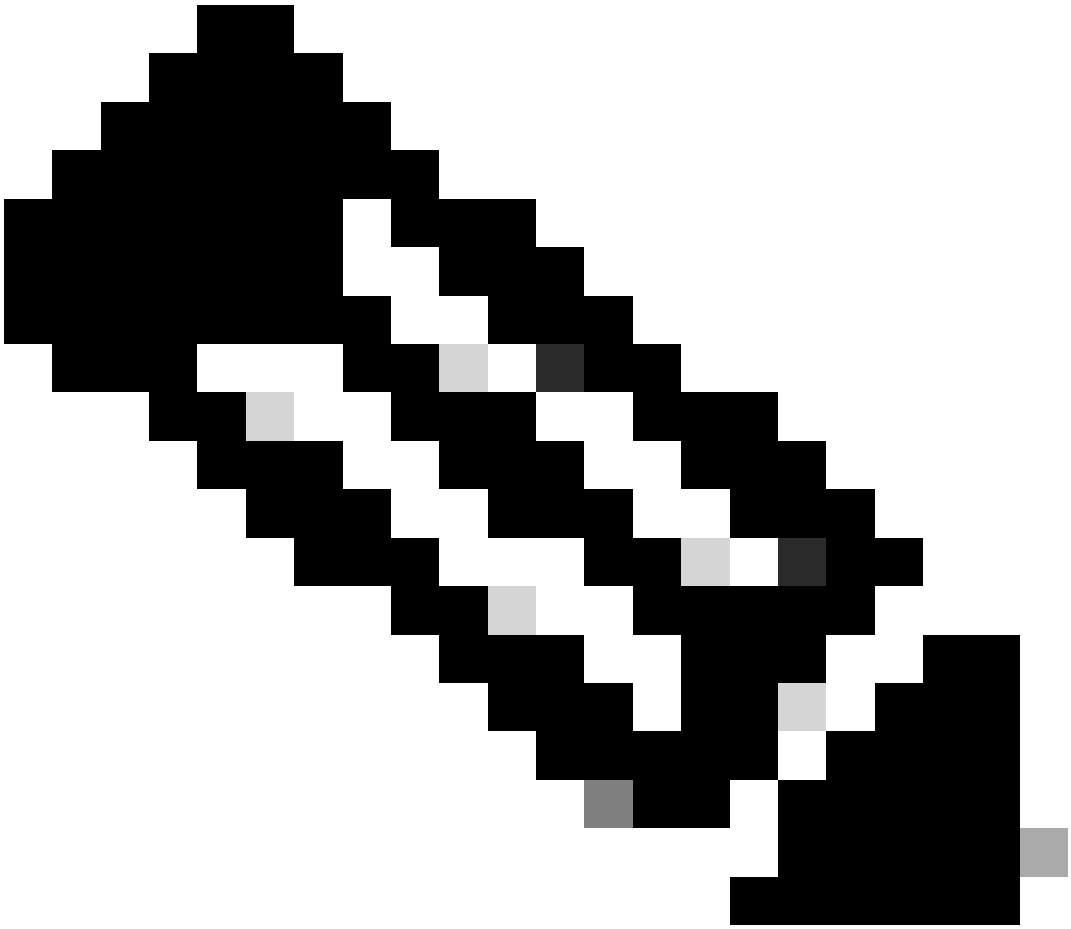
> Observação: sempre que possível, certifique-se de que apenas um firewall esteja envolvido no caminho de comunicação. Em algumas implantações, a sinalização de voz e os fluxos de mídia podem atravessar firewalls separados. Nesses casos, certifique-se de incluir todos os firewalls relevantes em seu processo de solução de problemas

Solução de problemas de mídia no firewall

Da perspectiva do FW, haverá 4 fluxos que devem ser analisados durante a solução de problemas de áudio unidirecional, áudio bidirecional ou sem áudio:

1. Fluxo de RTP do chamador para o receptor da chamada (interface de entrada).
2. Fluxo de RTP do chamador para o receptor da chamada (interface de saída).
3. Fluxo de RTP do receptor da chamada para o chamador (interface de saída).
4. Fluxo de RTP do receptor da chamada para o chamador (interface de entrada).



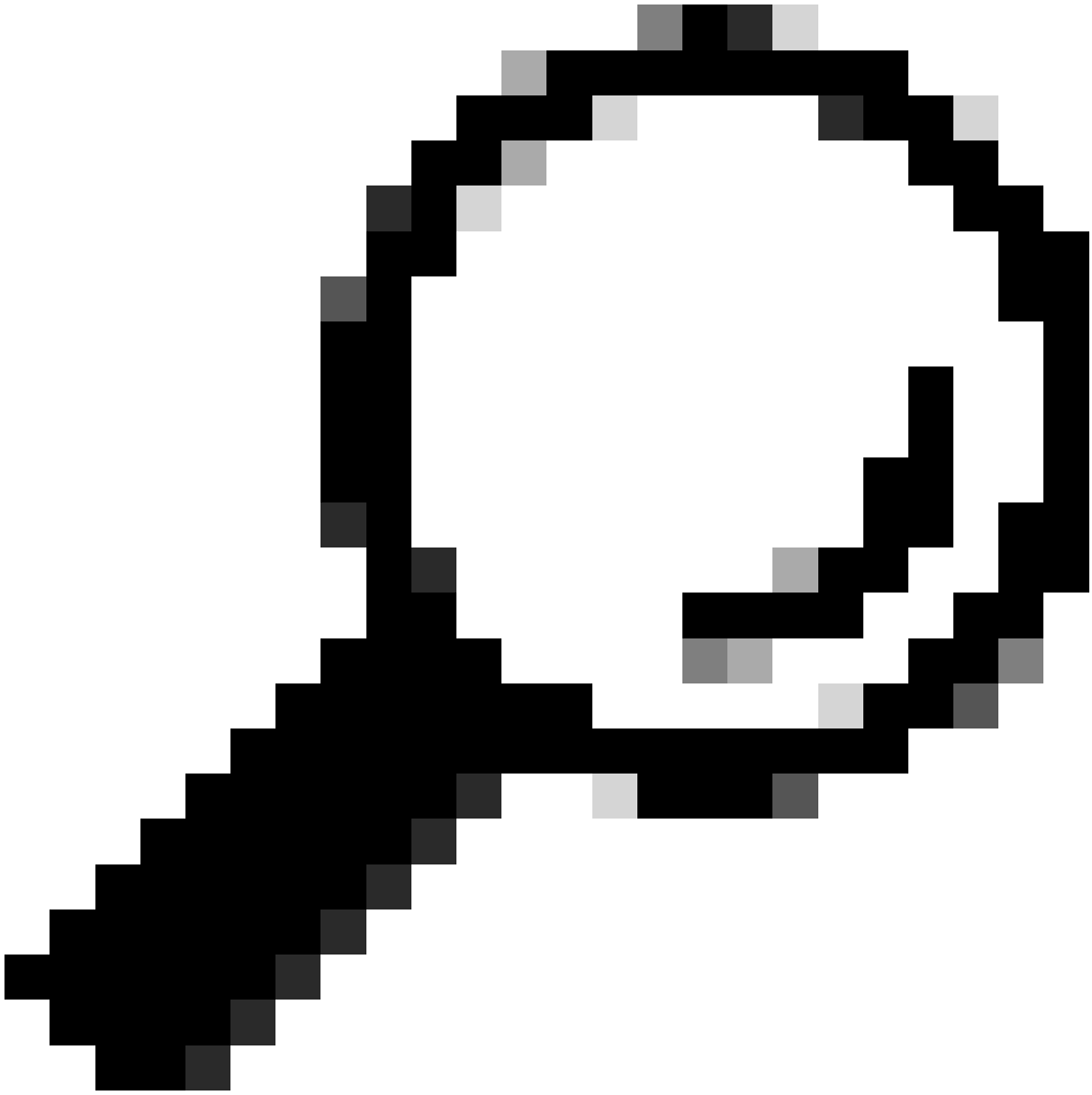


Note: Certifique-se de executar a solução de problemas usando capturas de pacotes CLI no modo ASA ou LINA no FTD, pois isso fornece maior flexibilidade para aplicar várias correspondências em uma única captura de pacote.

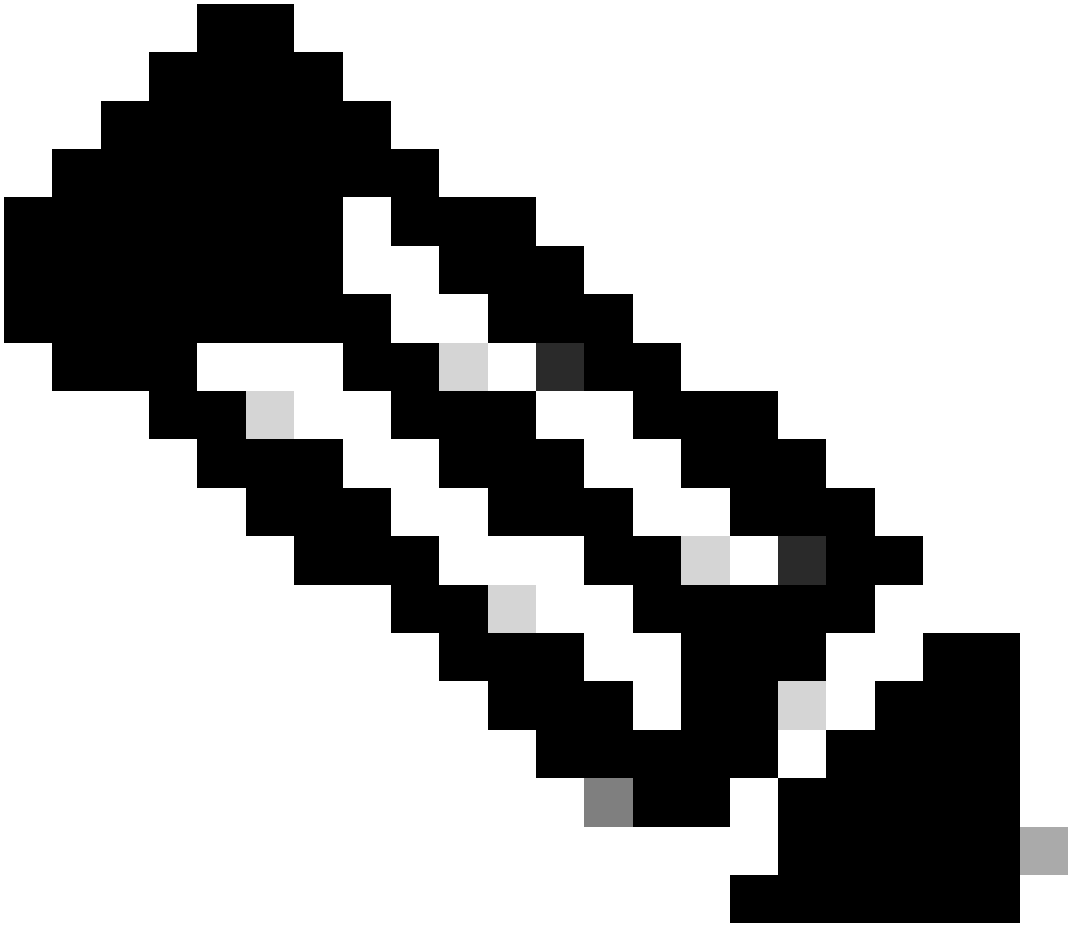
Troubleshooting de Chamadas SIP

Ao solucionar problemas de voz no FW seguro (ASA ou FTD), você precisa executar estas etapas:

1. Verifique se você tem o fluxo de chamadas e o diagrama de topologia.
2. Assegure-se de compreender o problema da perspectiva do usuário.
3. Entender o caminho para o protocolo de sinalização.
4. Entender o caminho do protocolo RTP de mídia.
5. Faça capturas de pacotes nas interfaces de entrada e saída.
6. Revise as regras de configuração da ACL e as regras de NAT.
7. Verifique se o tráfego de sinalização SIP não está sendo bloqueado pelo firewall. Além disso, compare as interfaces de entrada e saída para analisar o fluxo do tráfego de voz.
8. Verifique se o tráfego de mídia RTP não está sendo bloqueado pelo firewall comparando o fluxo de tráfego nas interfaces de entrada e saída.
9. Certifique-se de que os dispositivos de sinalização suportem a inspeção e, se não, desative-a.



Tip: As mensagens de sinalização SIP que entram no FW também devem ser as mesmas que saem do FW.



Note: As dicas de Troubleshooting para SIP também podem ser aplicadas aos protocolos H.323, MGCP e SCCP.

Informações Relacionadas

- Configurar capturas de pacotes ASA com CLI
- Usar capturas do Firepower Threat Defense

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.