Configurar proxy de CMS WebRTC pelo Expressway

Índice

Introdução

Este documento descreve as etapas para configurar e solucionar os problemas do Cisco Meeting Server (CMS) WebRTC pelo Expressway.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Expressway X8.9.2 e posterior

- Servidor CMS 2.1.4 e posterior
- Tradução de Endereço de Rede (NAT)
- Passagem usando retransmissões em torno do NAT (TURN)
- Utilitários de passagem de sessão para NAT (STUN)
- Domain Name System (DNS)

Pré-requisitos de configuração:

- Configurações relacionadas de acesso remoto e móvel (MRA) (zona de passagem UC, túneis SSH) já devem estar ativadas e definidas no Expressway, clique aqui para obter os guias de MRA
- WebBridge (WB), Protocolo extensível de mensagens e presença (XMPP) e CallBridge configurado e ativado no CMS, clique aqui para obter o guia de configuração
- Chave de opção TURN instalada no Expressway-E
- Porta TCP 443 aberta no Firewall da internet pública para o endereço IP público do Expressway-E
- Porta TCP e UDP 3478 (solicitações TURN) aberta no Firewall pela Internet pública para o endereço IP público do Expressway-E
- Porta TCP e UDP 3478 (solicitações TURN) aberta no Firewall pelo CMS para o endereço IP privado do Expressway-E (se você usar a Dual-NIC no Expressway-E)
- Registros DNS externos do FQDN do WebBridge, que podem ser resolvidos no endereço IP público do Expressway-E
- Registro DNS interno WB FQDN que pode ser resolvido no endereço IP do servidor CMS
- Reflexo NAT permitido no firewall externo do endereço IP público do Expressway-E, clique aqui para obter a configuração de exemplo

  Nota: Par Expressway que é usado para serviços de convidado do Jabber não pode ser usado em serviços proxy do WebRTC CMS.

Componentes Utilizados

Este documento não está restrito a versões específicas de software e hardware, no entanto, os requisitos mínimos de versão de software devem ser atendidos.

- Application Program Interface (API) do CMS
- Postman (cliente API)
- Expressway
- Servidor CMS

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.

Informações de Apoio

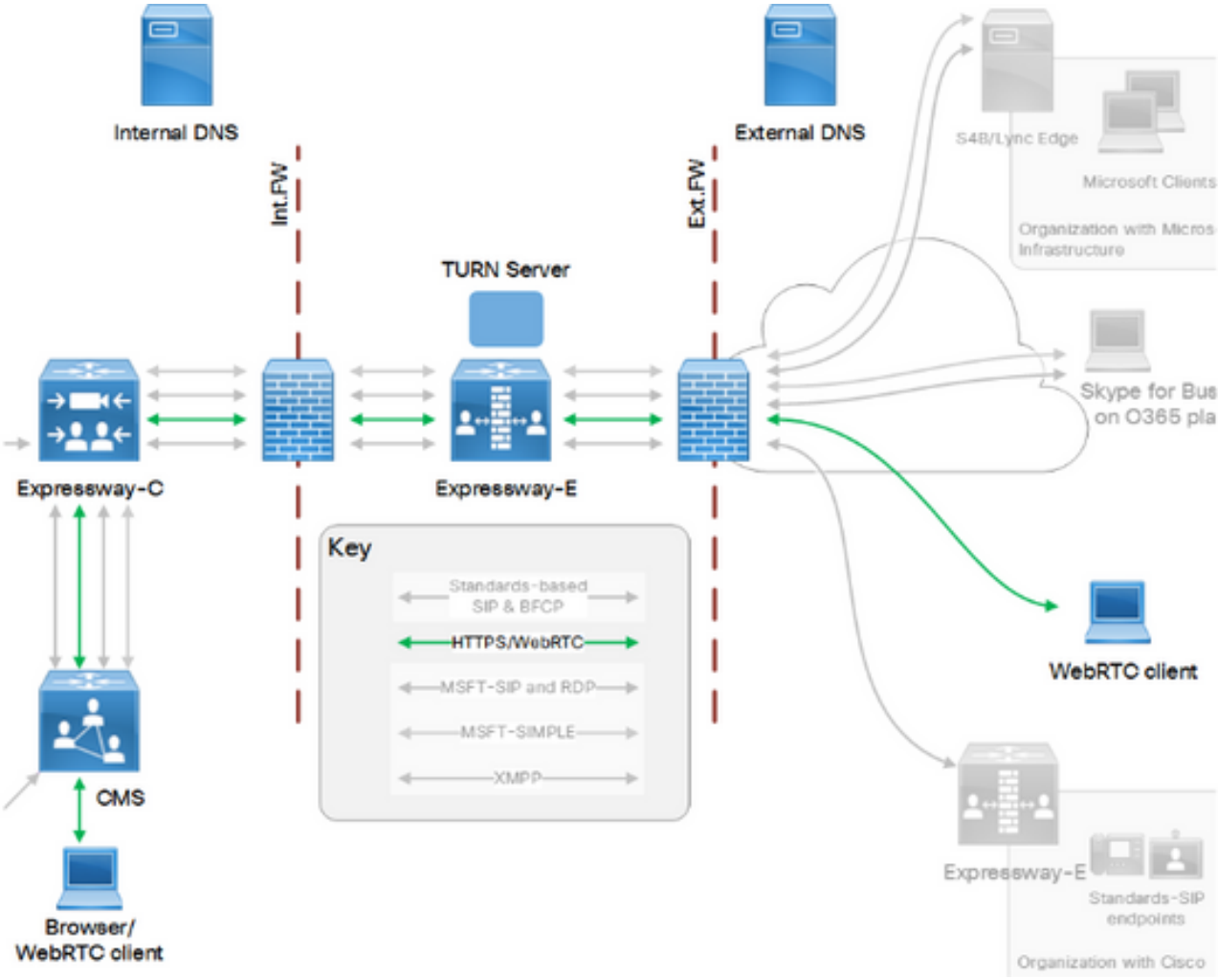
O suporte a proxy WebRTC foi adicionado ao Expressway a partir da versão X8.9.2, que permite aos usuários fora do local navegar para um Web Bridge do Cisco Meeting Server.

Clientes e convidados externos podem gerenciar ou entrar em espaços sem precisar de nenhum

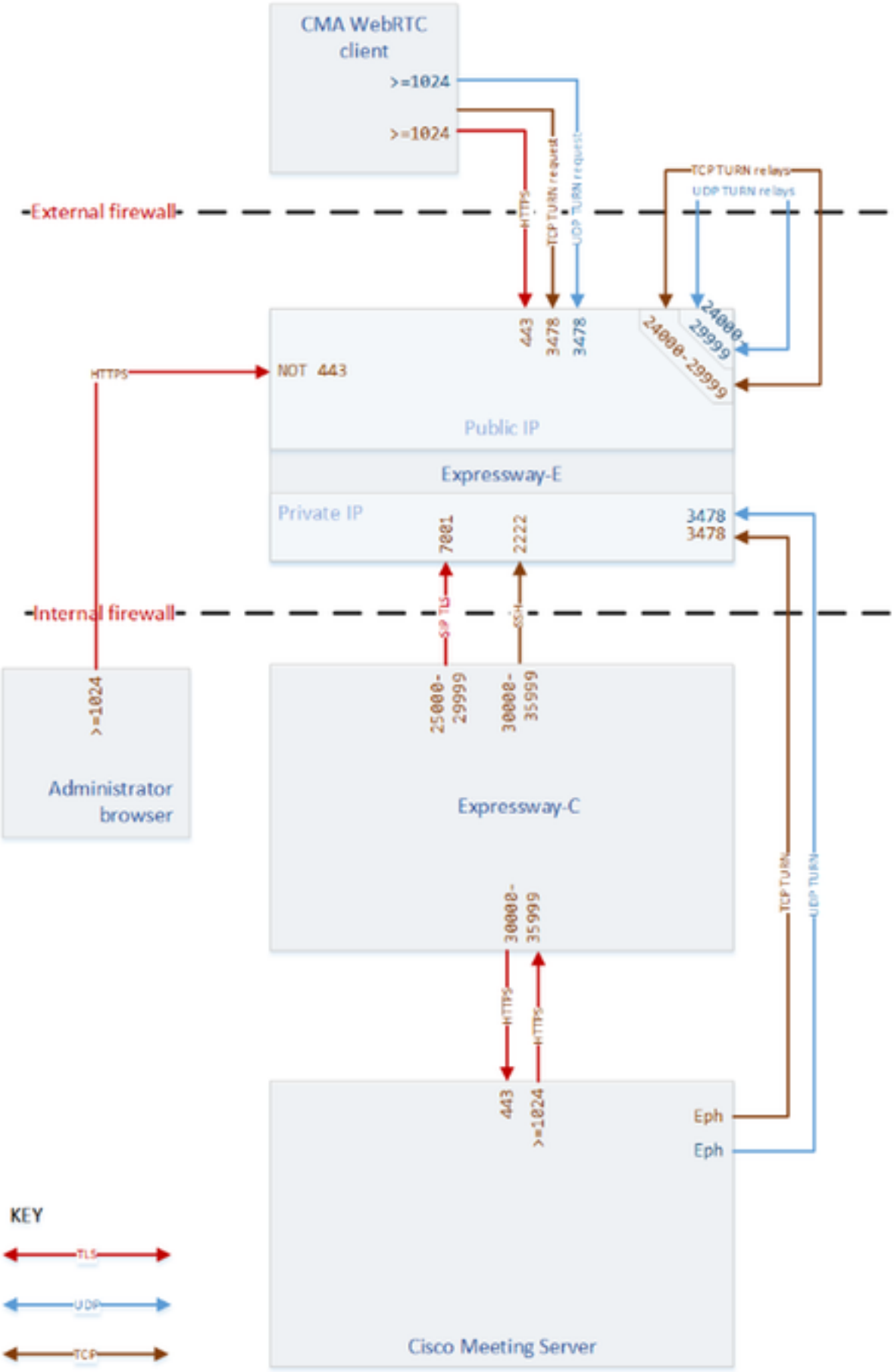
outro software além de um navegador compatível. Clique aqui para obter uma lista de navegadores compatíveis.

Configurar

Diagrama de Rede



Esta imagem oferece um exemplo do fluxo de conexões do proxy da Web para WebRTC CMS:



Nota: Você deve configurar o firewall externo para permitir o reflexo de NAT do endereço IP público do Expressway-E (firewalls normalmente não confiam em pacotes que têm o mesmo endereço IP de origem e destino).

Configuration Steps

Etapa 1. Integrar o CMS WB ao Expressway-C

a. Navegue até **Configuration > Unified Communication > Cisco Meeting Server** (Configuração > Comunicações unificadas > Cisco Meeting Server).

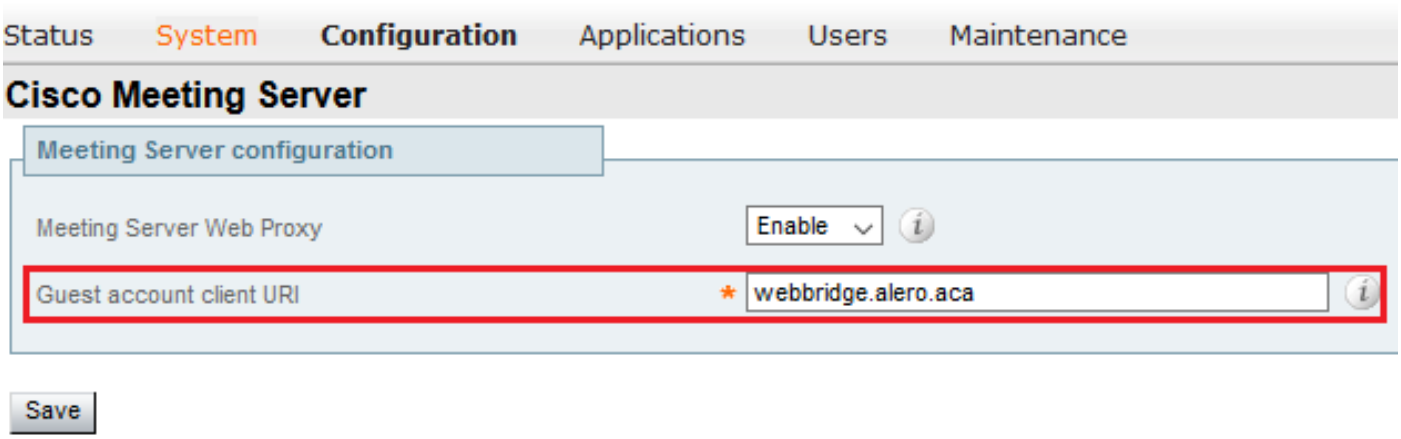
b. Ativar o **proxy da Web do servidor de reunião**

c. Insira o FQDN do WB no campo **URI de cliente de conta de convidado**

d. Clique em **Salvar**

e. Adicione o FQDN do WB no certificado de servidor do Expressway-E como um nome de assunto alternativo (SAN), clique aqui para obter o guia do certificado do Expressway.

> Nota: **A URI de cliente de conta de convidado** precisa ser configurada como no WebAdmin do servidor CMS (interface gráfica online) sem o prefixo **https://**.



Etapa 2. Habilite TURN no Expressway-E e adicione a credencial de autenticação ao banco de dados de autenticação local

a. Navegue até **Configuração > Passagem > TURN**

b. Ativar os serviços TURN, de **desligado** para **ligado**

c. Selecione **Configurar credenciais TURN do cliente no banco de dados local** e adicione as credenciais (nome de usuário e senha)

> Nota: Se tiver um cluster do Expressway-E e todos devam ser usados como servidores TURN, assegure-se de habilitá-lo em todos os nós. Você precisa configurar duas instâncias separadas de **turnServer** pela API e apontá-las para cada um dos servidores Expressway-E no cluster (conforme o processo de configuração mostrado na Etapa 4, que mostra o processo de um servidor Expressway-E; a configuração do segundo turnServer seria semelhante, usando apenas os respectivos endereços IP e credenciais TURN para o outro servidor Expressway-E).

Etapa 3. Alterar a porta de Change the administration port of the Expressway-E (optional)

a. Navegue até **Sistema > Administração**

b. Em **Configuração do servidor Web**, altere a **Porta de administrador Web** para **445** nas opções da lista suspensa e selecione **Salvar**

c. Repita as etapas **3a** a **3b** em todos os Expressway-E usados em serviços de proxy WebRTC

> Nota: A Cisco recomenda que a porta de administração seja alterada, pois os clientes WebRTC usam a 443. Se o navegador WebRTC tentar acessar a porta 80, o Expressway-E redireciona a conexão para a 443.

Etapa 4. Adicione o Expressway-E como servidores TURN de mídia NAT de passagem no servidor CMS

a. Baixe e instale o Postman aqui.

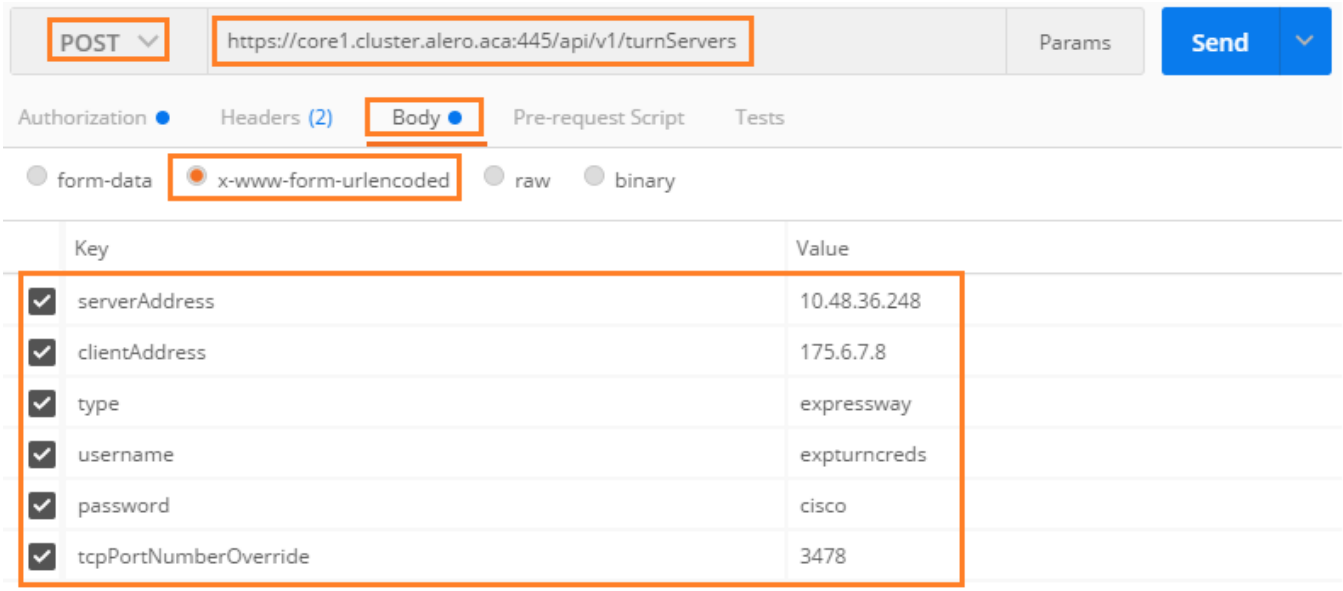
b. Insira a URL de acesso da API na barra de endereço, por exemplo; **https://<Callbridge_fqdn>:445/api/v1/<entity>**

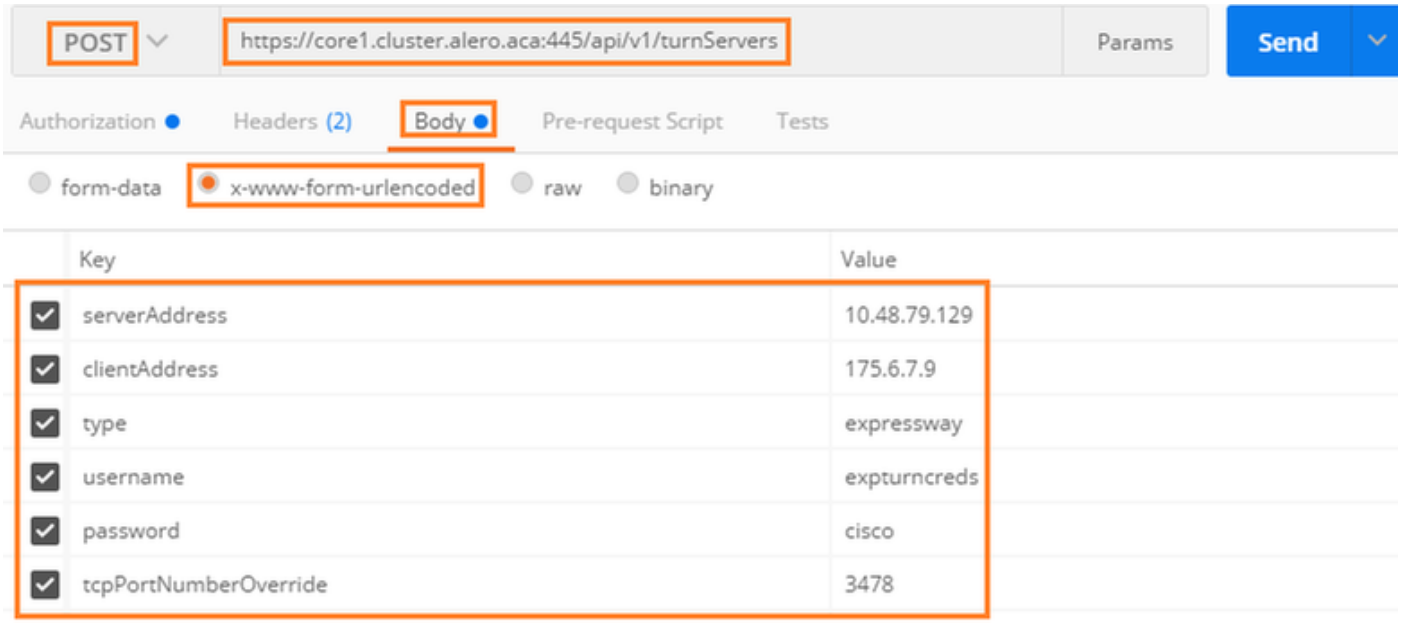
c. Enviar um POST com https://<Callbridge_fqdn>:445/api/v1/turnservers, depois de adicionar estes campos ao corpo:

- **serverAddress**: (Endreço IP privado do Expressway)
- **clientAddress**: (Endereço IP público do Expressway)
- **digite:** (expressway)
- nome de usuário: (como configurado na etapa **2c**)
- **senha**: (como configurado na etapa **2c**)
- **tcpPortNumberOverride:** 3478

d. Repita a etapa **4c** em todos os servidores Expressway-E a serem usados para TURN

Essas imagens oferecem exemplos de etapas de configuração:



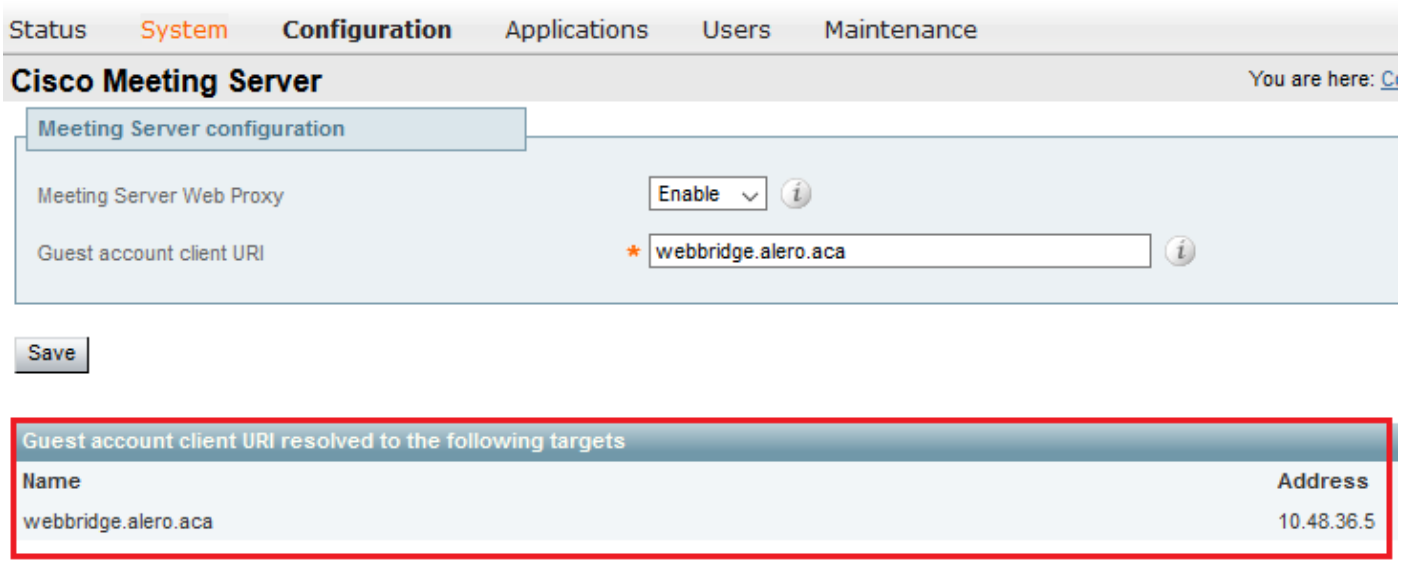


Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Etapa1. No Expressway-C, verifique se o WB está integrado corretamente

a. Navegue até **Configuration > Unified Communication > Cisco Meeting Server** (Configuração > Comunicações unificadas > Cisco Meeting Server) e você verá o endereço IP do WB:



b. Navegue até **Configuration > Unified Communication > HTTP allow list > Automatically added rules** (Configuração > Unified Communication > Lista de permissões HTTP > Regras adicionadas automaticamente), verifique se isso foi adicionado às regras:

```
Meeting Server web bridges https 443 Prefix / GET, POST, PUT, HEAD, DELETE
Meeting Server web bridges wss 443 Prefix / GET, POST, PUT, HEAD, DELETE
```

> Nota: Não é esperado encontrar o WB nos nós detectados, já que as regras são apenas para permitir o proxy de tráfego HTTPS para o WB e não necessariamente para o Unified Communication.

c. Verifique se o túnel Secure Shell (SSH) do WB FQDN WB foi criado no Expressway-C para o Expressway-E e que esteja ativo. Navegue até **Status > Unified Communications > Unified Communications SSH tunnels status** (Status > Unified Communications > Status dos túneis SSH do Unified Communications), é preciso ver o FQDN do WB e o destino deve ser o Expressway-E:

Etapa 2. Verifique se o servidor TURN foi adicionado ao servidor CMS

a. Na WebUI, se você usar um único servidor Expressway, navegue até **Logs > Event logs** (Logs > Logs de evento), o resultado mostra o endereço IP do servidor TURN, como no exemplo:

```
2017-04-1509:37:26.864Info TURN server 7: starting up "10.48.36.248" (configured object 6508065f-298f-4146-8697-4b7087279de3)
```

b. Se você usar vários servidores TURN Expressway, envie uma solicitação **GET** com um cliente de API com este comando:

https://<Callbridge_IP>:445/api/v1/turnservers

> Nota: Esse comando também pode ser usado caso você tenha um único servidor Expressway TURN.

O resultado, no caso de vários servidores Expressway TURN, é semelhante ao do exemplo:

```
<?xml version="1.0"?>
<turnServers total="2">
    <turnServer id="7eecf3eb-49f2-4963-bf67-2bac98355ca1">
        <serverAddress>10.48.79.129</serverAddress>
        <clientAddress>175.6.7.9</clientAddress>
    </turnServer>
    <turnServer id="eef94a2b-3bfa-40f7-b83c-ece8df424e15">
        <serverAddress>10.48.36.248</serverAddress>
        <clientAddress>175.6.7.8</clientAddress>
    </turnServer>
</turnServers>
```

c. Para verificar o status de cada servidor TURN, faça o seguinte:

- Copie **turnServer id** da etapa 2b
- Envie uma solicitação **GET** com o cliente da API com este comando:
  https://<Callbridge_IP>:445/api/v1/turnservers/<turnServer id>/status

O resultado exibe as informações que incluem o tempo de resposta (RTT) em milissegundos (Ms) associados ao servidor TURN. Essas informações são importantes para que o CB selecione o melhor servidor TURN a ser usado.

O resultado abaixo mostra o status do servidor TURN com a ID **7eecf3eb-49f2-4963-bf67-2bac98355ca1**:

```
<?xml version="1.0"?>
<turnServer>
   <status>success</status>
   <host>
       <address>10.48.36.248</address>
       <portNumber>3478</portNumber>
       <reachable>true</reachable>
       <roundTripTimeMs>37</roundTripTimeMs>
       <mappedAddress>10.48.36.5</mappedAddress>
       <mappedPortNumber>44920</mappedPortNumber>
   </host>
</turnServer>
```

O resultado abaixo mostra o status do servidor TURN com a ID **eef94a2b-3bfa-40f7-b83c-ece8df424e15**:

```
<?xml version="1.0"?>
<turnServer>
   <status>success</status>
   <host>
       <address>10.48.79.129</address>
       <portNumber>3478</portNumber>
       <reachable>true</reachable>
       <roundTripTimeMs>48</roundTripTimeMs>
       <mappedAddress>10.48.36.5</mappedAddress>
       <mappedPortNumber>44920</mappedPortNumber>
   </host>
```

Etapa 3. Verifique o uso de retransmissão do TURN durante uma chamada em andamento

No momento em que a chamada ao vivo é feita com o uso do cliente WebRTC, você pode ver o status de retransmissão de mídia do TURN no Expressway. Navegue até **Status > TURN relay usage,** (Status > Utilização de retransmissão do TURN) e selecione**exibir.**

Troubleshooting

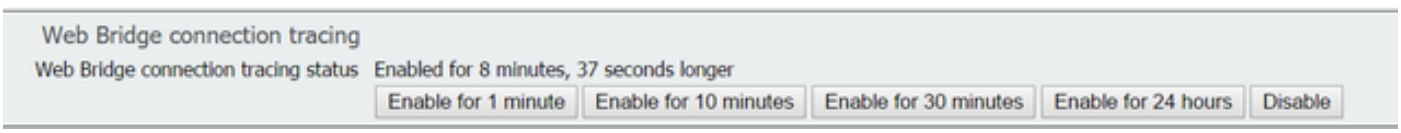
Esta seção fornece informações que você pode usar na solução de problemas da configuração de alguns problemas comuns de WebRTC e possíveis falhas.

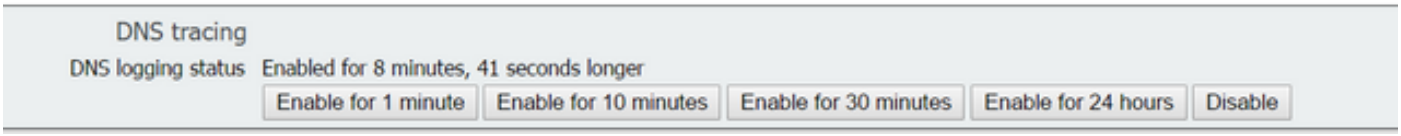
Logs das conexões WB e rastreamento de DNS podem ser habilitados no WebAdmin do servidor CMS:

a. Conecte-se ao **WebAdmin**

b. Navegue até **Logs > Detailed Tracing** (Logs > Rastreamento detalhado)

c. Ative o **Rastreamento de conexão do Web Bridge** e **rastreamento de DNS** pela duração desejada:





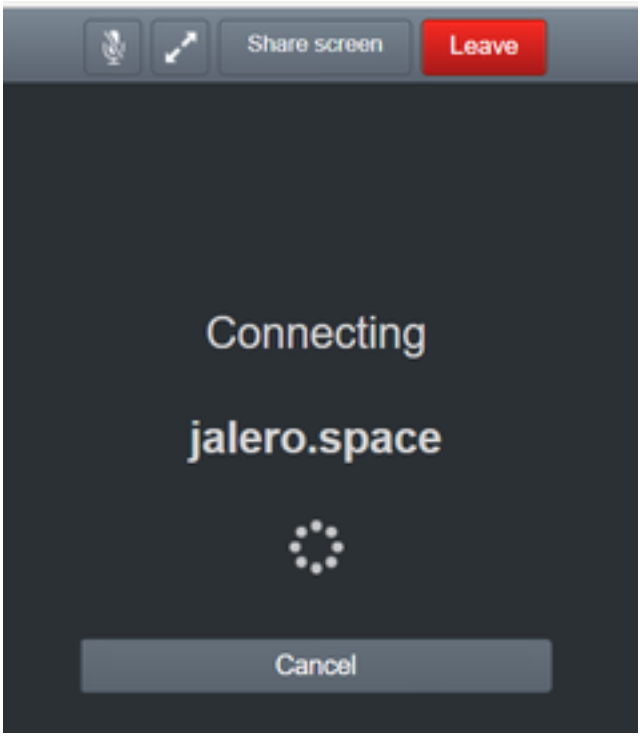
Logs de depuração do console do Chrome e do Firefox podem ser usados para solucionar problemas de falhas de conexão do cliente WebRTC, como problemas com mídia e conectividade com o WB. Isso pode ser exibido usando a combinação **Ctrl+Shift+C no teclado.**

No Chrome, use **chrome://webrtc-internals/** ou **sobre: webrtc** no Firefox, em uma guia separada no momento de uma chamada ao vivo para exibir os diagnósticos avançados, que é útil para solucionar problemas de mídia com o WebRTC.

A captura de pacotes do Whireshark no cliente WebRTC também oferece informações úteis sobre a retransmissão de mídia com o servidor TURN.

O cliente WebRTC externo se conecta, mas não há mídia (devido a falha de ICE)

Neste cenário, o cliente RTC consegue resolver a ID de chamada como **jalero.space, mas** quando você insere o nome e seleciona Joincall**, o** cliente mostra Conectando**, como mostrado** na imagem abaixo:

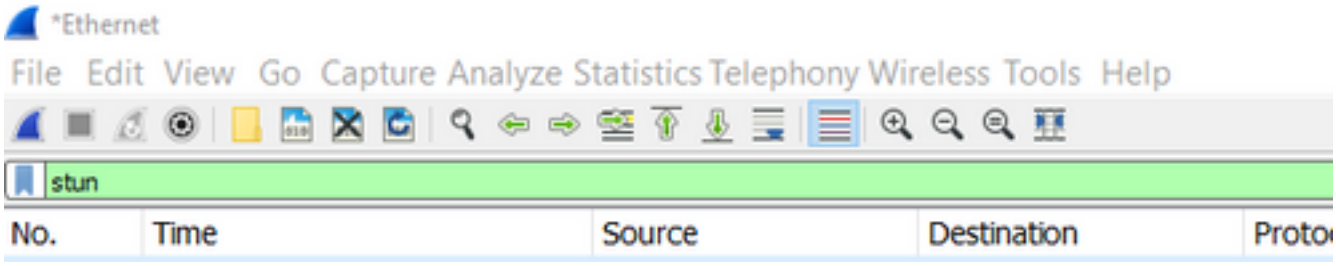


Depois de cerca de 30 segundos ele é redirecionado para a página inicial do WB.

Para solucionar problemas, faça o seguinte:

- Inicie o Wireshark no cliente RTC quando tentar ligar e, quando a falha acontece, interrompe a captura
- Depois que o programa acontecer, verifique os logs de evento do CMS
  Navegue até **Logs > Event logs (Logs > Logs de evento)** no WebAdmin do CMS

- Filtre os rastreamentos do Wireshark com **stun**, veja os exemplos abaixo:



Nos rastreamentos do Wireshark, você verá que o cliente envia **Allocate Request** (Solicitação de alocação) com as credenciais configuradas para o servidor Expressway-E TURN na porta **3478**:

```
1329    2017-04-15 10:26:42.108282    10.55.157.229    10.48.36.248    STUN    186    Allocate Request UDP user: expturncreds realm: TANDBERG with nonce
```

O servidor responde com **Allocate Error** (Erro de alocação):

```
1363    2017-04-15 10:26:42.214119    10.48.36.248    10.55.157.229    STUN    254    Allocate Error Response user: expturncreds with nonce realm: TANDBERG UDP error-code: 431 (*Unknown error code*) Integrity Check Failure
```

ou

```
3965    2017-04-15 10:34:54.277477    10.48.36.248    10.55.157.229    STUN    218    Allocate Error Response user: expturncreds with nonce realm: TANDBERG UDP error-code: 401 (Unauthorized) Unauthorized
```

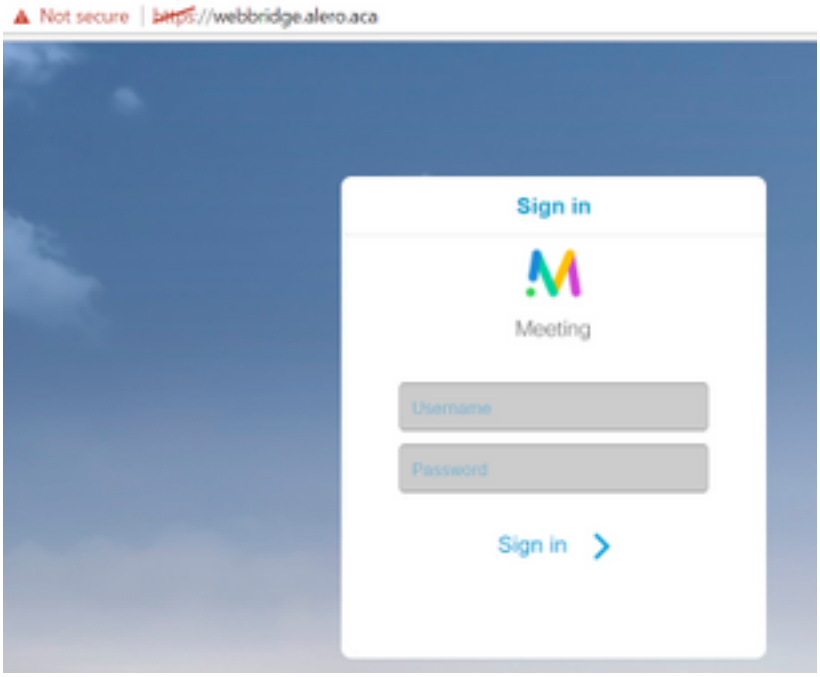
Nos logs do CMS, a mensagem de log abaixo é mostrada:

```
3965    2017-04-15 10:34:54.277477    10.48.36.248    10.55.157.229    STUN    218    Allocate Error Response user: expturncreds with nonce realm: TANDBERG UDP error-code: 401 (Unauthorized) Unauthorized
```

Solução:

Verifique as credenciais TURN configuradas no CMS e assegure-se de que correspondam ao que está configurado no banco de dados de autenticação local do Expressway-E.

O cliente WebRTC externo não tem a opção participar da chamada



Na página **Status > General** (Status > Geral) do Callbridge, isto é exibido:

```
3965    2017-04-15 10:34:54.277477    10.48.36.248    10.55.157.229    STUN    218    Allocate
Error Response user: expturncreds with nonce realm: TANDBERG UDP error-code: 401 (Unauthorized)
Unauthorized
```

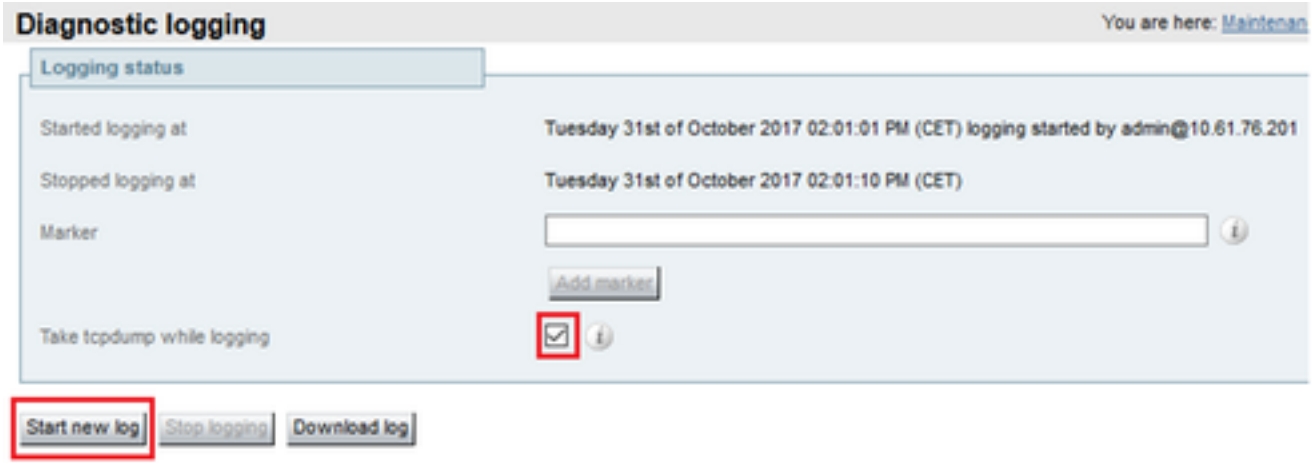
Solução:

- Certifique-se de que o Callbridge possa resolver o FQDN do WB para o endereço IP interno (o Callbridge não deve resolver isso para o endereço IP do Expressway-E)
- Limpe o cache do DNS no Callbridge, pela interface de linha de comando (CLI), com o comando **dns flush**
- Certifique-se de que o WB confie no certificado de servidor do Callbridge (não o emissor)

O cliente WebRTC externo fica preso (na mídia de carregamento) ao se conectar ao espaço conjunto e é redirecionado para a página inicial do WB

Solução:

- Assegure-se de que o CMS possa resolver o registro SRV **_xmpp-client** na rede interna para o domínio CB
- Colete a captura do Wireshark no cliente e o **Log de diagnóstico**, inclusive **tcpdump** no Expressway-E enquanto tenta conectar ao cliente externo
  Navegue até **Maintenance > Diagnostics > Diagnostic logging** (Manutenção > Diagnóstico > Log de diagnóstico) e assegure-se que **Obter o tcpdump durante o log** esteja marcado na imagem abaixo antes de selecionar **Iniciar novo log**:

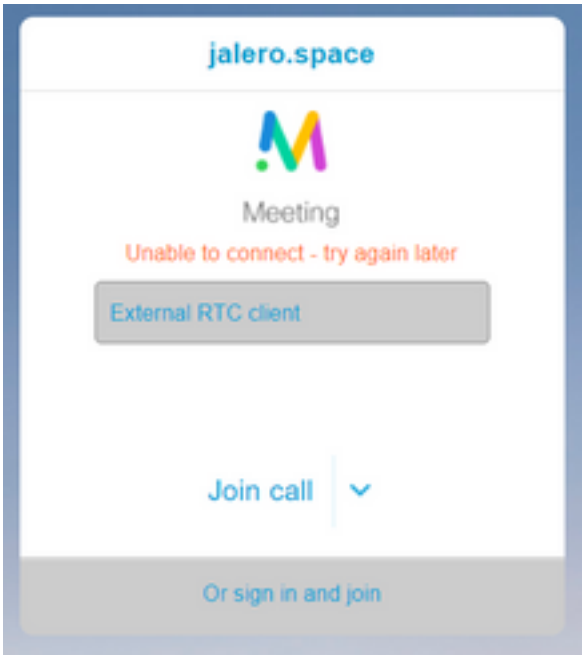


Nota: Certifique-se de que a captura do Wireshark no dispositivo cliente e o log no Expressway-E sejam iniciados antes de reproduzir a chamada com falha. Quando a chamada com falha for reproduzida, pare e baixe o log no Expressway-E e a captura no cliente.

- Extraia/descompacte o pacote de log baixado do Expressway-E e abra o arquivo **.pcap** obtido pela interface pública
- Filtre em ambas as capturas de pacote com **stun** Em seguida, procure a solicitação de vinculação do cliente Externo para o endereço IP público do Expressway-E, **clique com o botão direito do mouse** e selecione **Follow > UDP Stream** (Seguir > Fluxo UDP)Normalmente, a porta de destino da **Solicitação de vinculação** do cliente estaria no intervalo de **24000-29999**, que é o **Intervalo de porta de retransmissão TURN** no Expressway-E
- Caso não haja resposta para as **Solicitações de vinculação** pelo cliente, verifique a captura do Expressway-E para ver se as solicitações estão chegando
- Caso as solicitações estejam chegando e o Expressway-E esteja respondendo ao cliente, verifique se o FW externo está permitindo o tráfego UDP de saída
- Caso as solicitações não estejam chegando, verifique o FW para assegurar que o intervalo de portas acima não esteja bloqueado
- Caso o Expressway-E seja implantado com um Controlador de interface de rede duplo (DUAL-NIC) com o modo de NAT estático ativado, assegure que o reflexo de NAT seja compatível e esteja configurado no FW externo

O cliente WebRTC externo não é capaz de se juntar ao espaço conjunto e recebe o aviso (Não foi possível conectar - tente novamente mais tarde)

Neste cenário, o cliente RTC consegue resolver a ID de chamada como **jalero.space, but** quando você insere o nome e seleciona Joincall**, o** aviso Não foi possível **conectar - tente novamente mais tarde é** exibido imediatamente:



Solução:

Verifique se o CMS, na rede interna, consegue resolver o registro SRV **_xmpp-client** para o domínio CB.

Informações Relacionadas

- Guia de uso da porta de IP VCS/Expressway
- Suporte Técnico e Documentação - Cisco Systems