Configurar o proxy CMS WebRTC sobre a via expressa

Índice

Introdução

Este documento descreve as etapas para configurar e pesquisar defeitos Cisco que encontra o server (CMS) WebRTC sobre a via expressa.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Via expressa X8.9.2 e acima
- Server 2.1.4 CMS e acima
- Network Address Translation (NAT)
- Traversal usando relés em torno de NAT (VOLTA)
- Utilidades de Traversal da sessão para o NAT (ATURDIR)
- Domain Name System (DNS)

Pré-requisito de configuração:

- O móbil e o Acesso remoto (MRA) devem já ser permitidos e configurado na via expressa, clicam aqui para guias MRA
- WebBridge (WB) configurado e permitido no CMS, clica aqui para o manual de configuração
- GIRE a chave da opção instalada na via expressa-e
- Porta TCP 443 aberta no Firewall do Internet público ao endereço IP público do Via-e
- A porta 3478 TCP e UDP (pedidos da VOLTA) abriu no Firewall do Internet público ao endereço IP público do Via-e

- A porta 3478 TCP e UDP (pedidos da VOLTA) abriu no Firewall do CMS ao endereço IP privado do Via-e (se você usa o NIC dual na via expressa-e)
- Registros externos DNS para o FQDN do WebBridge, pode ser resolvido ao endereço IP de Um ou Mais Servidores Cisco ICM NT do público-revestimento do Via-e
- Pode ser resolvido FQDN WB do registro dos DN internos ao endereço IP de Um ou Mais Servidores Cisco ICM NT do server CMS
- A reflexão NAT permitiu no firewall externo para o endereço IP público do Via-e, clica aqui por exemplo a configuração

  Nota: Os pares da via expressa que são usados para serviços do convidado do Jabber não podem ser usados para serviços de proxy CMS WebRTC.

Componentes Utilizados

Este documento não é restringido à versão de software e hardware específica, porém as exigências da versão mínima de software devem ser cumpridas.

- Application Program Interface CMS (API)
- Carteiro (cliente API)
- Via expressa
- Server 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 sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

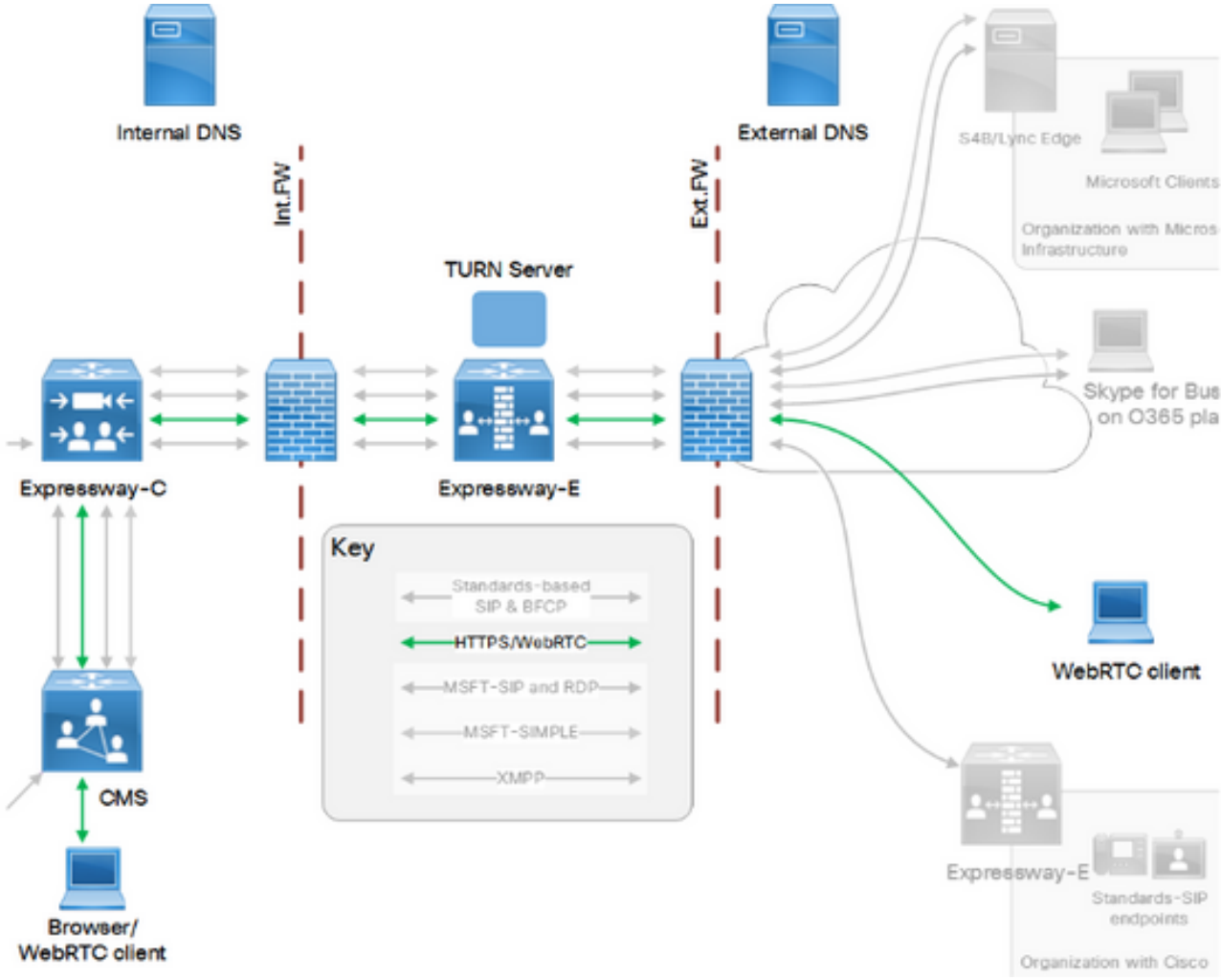
Informações de Apoio

O suporte de proxy de WebRTC foi adicionado à via expressa da versão X8.9.2, que permite usuários dos fora-locais de consultar a Cisco que encontra a ponte da Web do server.

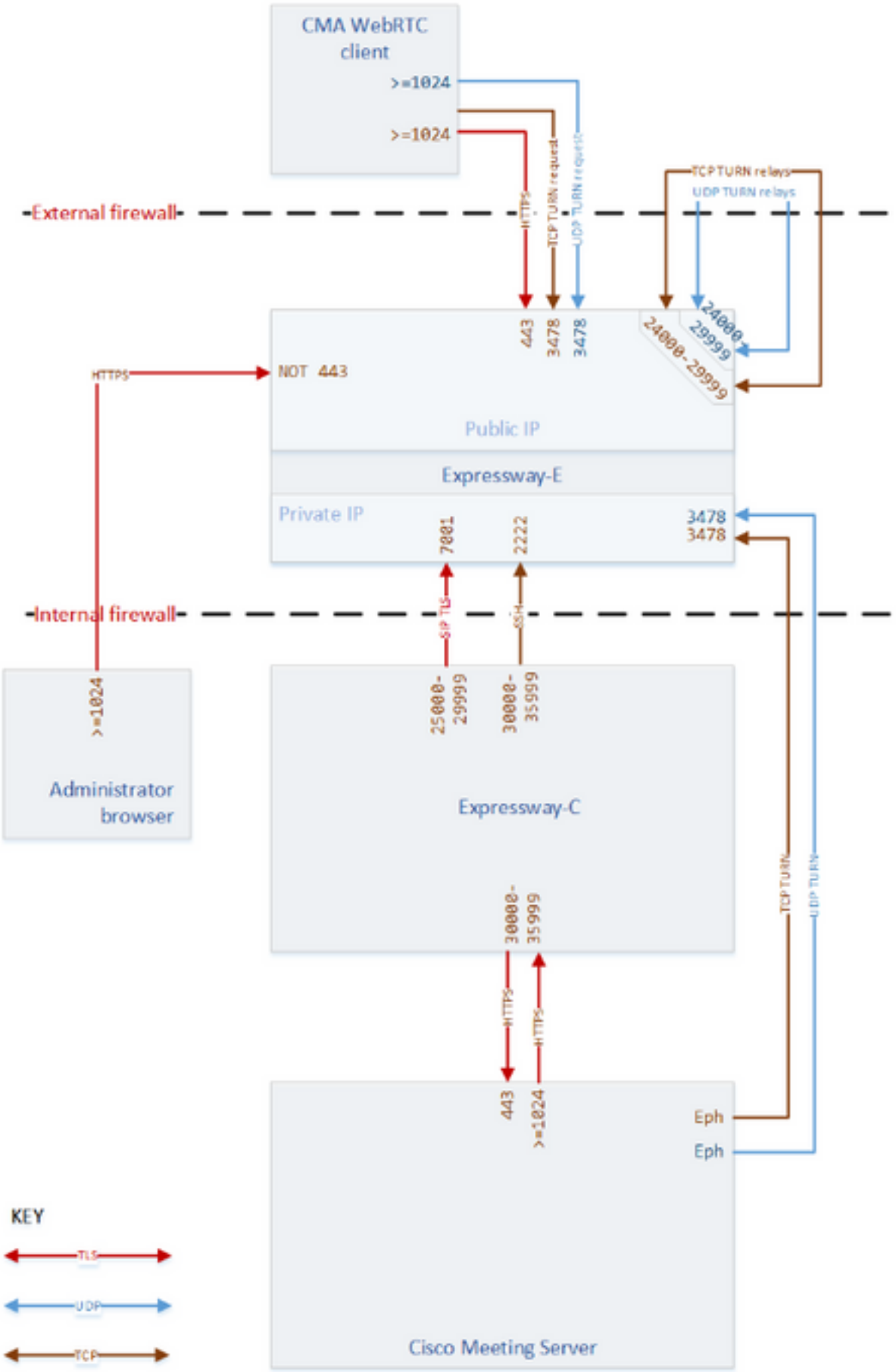
Os clientes externos e os convidados podem controlar ou juntar-se a espaços sem a necessidade de todo o software a não ser um navegador suportado. Clique aqui para uma lista de navegadores suportados.

Configurar

Diagrama de Rede



A seguinte imagem fornece um exemplo das conexões flui do proxy da Web para CMS WebRTC:



Nota: Você deve configurar seu firewall externo para permitir a reflexão NAT para o IP address público da via expressa-e (dos Firewall os pacotes da desconfiança tipicamente que têm o mesmo IP address da fonte e do destino).

Etapas de configuração

Etapa 1. Integre a WB CMS na via expressa-C.

a. Navegue à **configuração > uma comunicação unificada > Cisco que encontra o server**

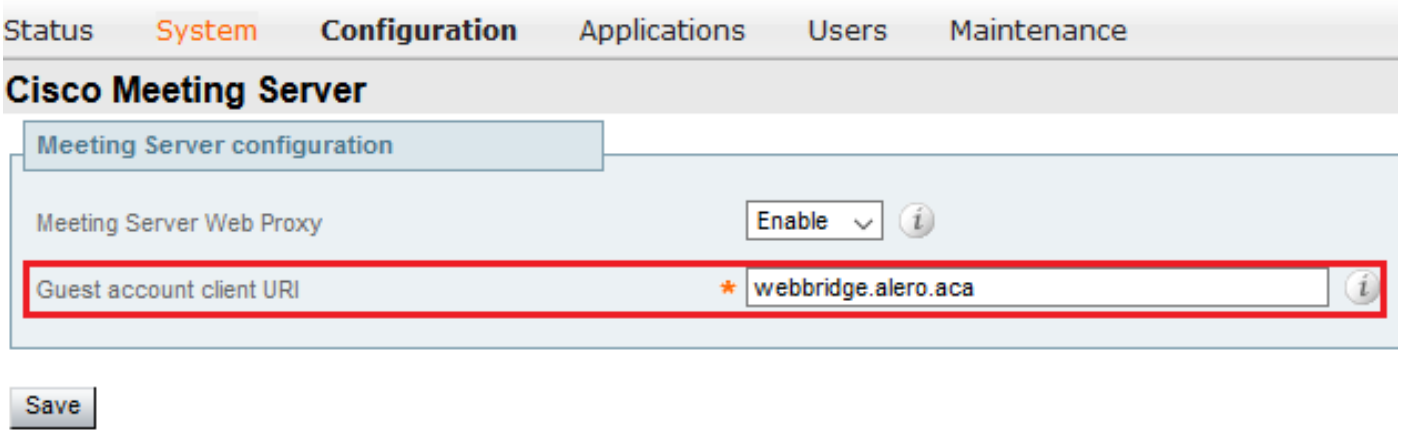
b. Permita o **proxy da Web do server da reunião**

c. Incorpore o FQDN da WB ao campo do **cliente URI da conta do convidado**

d. Clique sobre a **salvaguarda**

e. Adicionar o FQDN da WB no certificado de servidor da via expressa-e como um nome alternativo sujeito (SAN), clique-o aqui para o guia do certificado da via expressa.

> Nota: **O cliente URI da conta do convidado** deve ser como configurado no server WebAdmin CMS (interface GUI da Web) sem o prefixo de **https://**.



Etapa 2. Permita GERENCIEM sobre a via expressa-e e adicionam as credenciais de autenticação ao base de dados de autenticação local.

a. Navegue à **configuração > ao Traversal > à VOLTA**

b. Permita serviços da VOLTA, de **fora a sobre**

c. Seleto **configurar credenciais do cliente da VOLTA no base de dados local** e adicionar as credenciais (o nome de usuário e senha)

> Nota: Se você tem um conjunto de via expressa-e e são todos a ser usados como server da VOLTA, a seguir assegure para permiti-lo em todos os Nós.

Etapa 3. Mude a porta da administração da via expressa-e (opcional).

a. Navegue ao **sistema > à administração**

b. Sob a **configuração do servidor de Web**, mude a **porta do administrador da Web a 445 das** opções da gota-para baixo, a seguir selecione a **salvaguarda**

c. Repita as etapas **3a a 3b em** toda a via expressa-e usada para serviços de proxy de WebRTC

> Nota: Cisco recomenda a administração que a porta seja mudada porque o uso 443 dos clientes de WebRTC. Se o navegador de WebRTC tenta à porta de acesso 80, a via expressa-e reorienta a conexão a 443.

Etapa 4. Adicionar a via expressa-e como server da VOLTA para o traversal dos media NAT no server CMS.

a. Transfira e instale o carteiro
de; https://chrome.google.com/webstore/detail/postman/fhbjgbiflinjbdggehcddcbncdddomop?hl=en

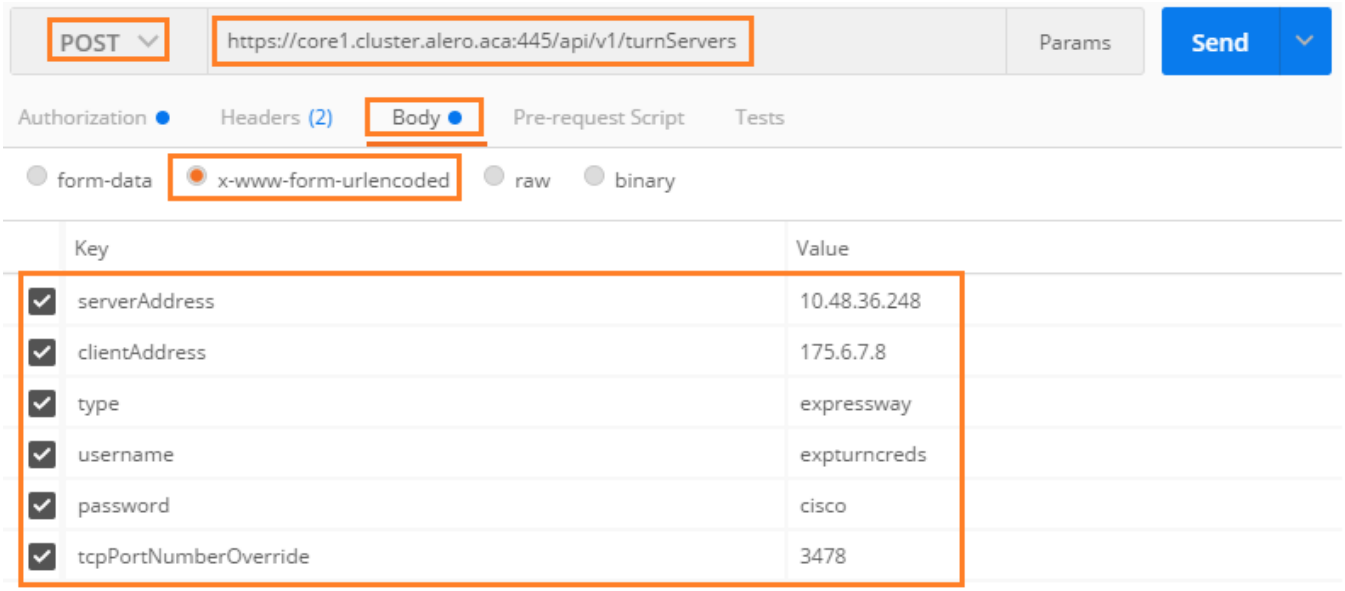
b. Incorpore o acesso URL API à barra de endereços, por
exemplo; **https://<Callbridge_fqdn>:445/api/v1/<entity>**

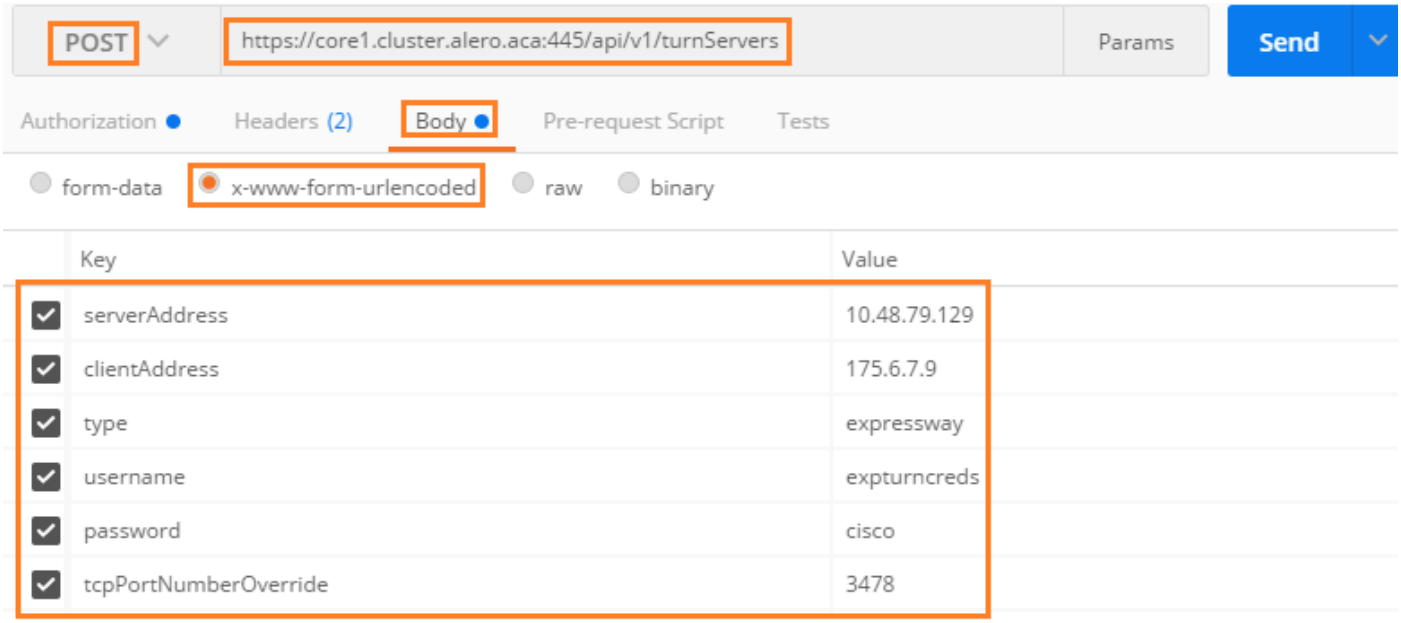
c. Envie um CARGO com https://<Callbridge_fqdn>:445/api/v1/turnservers**,** depois que você adiciona estes campos no corpo:

- **serverAddres**: (Endereço IP privado da via expressa)
- **clientAddress**: (Endereço IP público da via expressa)
- **tipo:** (via expressa)
- nome de usuário: (como configurado na etapa **2c**)
- senha: (como configurado na etapa **2c**)
- **tcpPortNumberOverride:** 3478

d. Repita a etapa **4c** para que cada server da via expressa-e seja usado para a VOLTA

As seguintes imagens fornecem exemplos das etapas configurational:



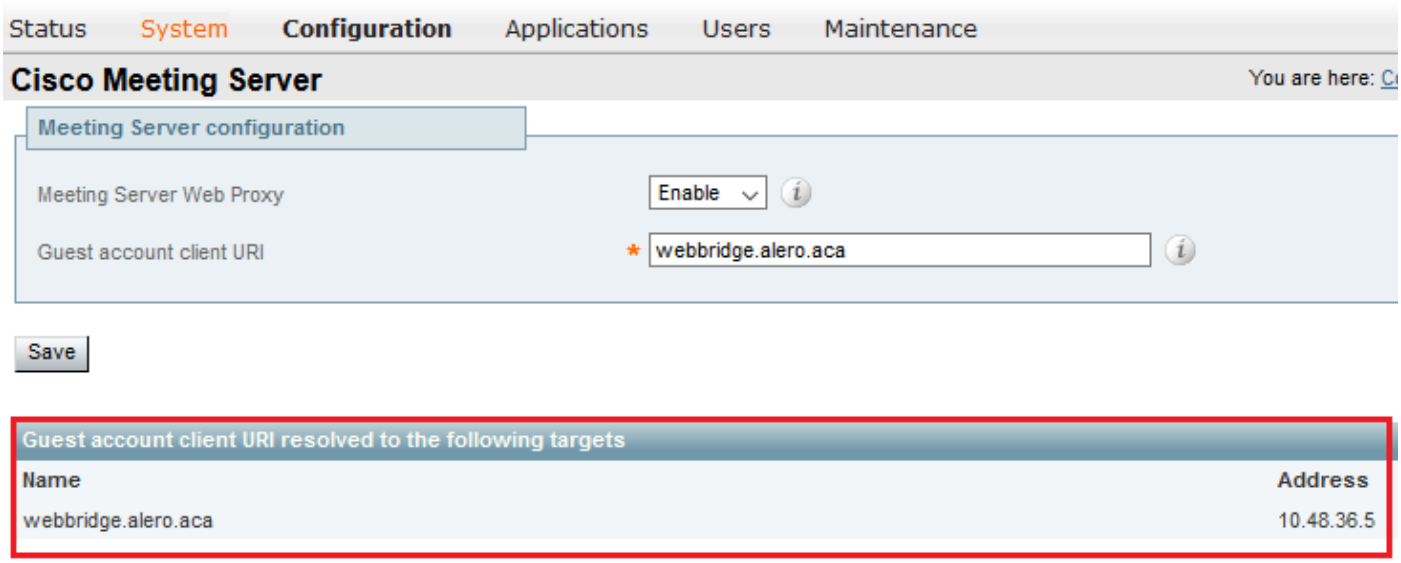


Verificar

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

Etapa 1. Na via expressa-C, certifique-se da WB esteja integrada corretamente.

a. Navegue à **configuração > uma comunicação unificada > Cisco que encontra o server,** e você deve ver o endereço IP de Um ou Mais Servidores Cisco ICM NT da WB:



b. Navegue à **configuração > uma comunicação unificada > HTTP permitem a lista > regras automaticamente adicionadas**, certificam-se de isto esteja 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 se espera encontrar não necessariamente a WB nos Nós descobertos porque as regras são simplesmente permitir o proxy do tráfego HTTPS à WB, e para uma comunicação unificada.

c. Certifique-se do túnel do Shell Seguro (ssh) para o FQDN WB esteja construído na via

expressa-C à via expressa-e e que é ativo. Navegue **estado aos túneis do estado > das comunicações unificadas > das comunicações unificadas SSH**, você deve ver que o FQDN da WB e do alvo deve ser a via expressa-e:

Etapa 2. Verifique que o server da VOLTA esteve adicionado ao server CMS.

a. No WebUI, se você usa um único server da via expressa, navegue aos **logs > aos log de eventos**, a saída mostra o endereço IP do servidor da VOLTA, 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 usa server múltiplos da VOLTA da via expressa, envie um pedido **GET** com um cliente API com este comando:

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

> Nota: Este comando pode igualmente ser usado se você tem um único server da VOLTA da via expressa.

A saída, no caso dos server múltiplos da VOLTA da via expressa, é similar àquela neste exemplo:

```
<?xml version="1.0"?>
<turnServers total="2">
    <turnServer id="20efbd08-c08d-4893-8f7e-698d1c8ca7f9">
        <serverAddress>10.48.79.129</serverAddress>
        <clientAddress>175.6.7.9</clientAddress>
    </turnServer>
    <turnServer id="61ae465d-fe30-440e-b20a-8f75e8fb9b85">
        <serverAddress>10.48.36.248</serverAddress>
        <clientAddress>175.6.7.8</clientAddress>
    </turnServer>
</turnServers>
```

c. No WebAdmin, navegue a **https://<Callbridge_FQDN>:445/turn_debug.html**

A saída indica o Round-Trip Time (RTT) associado com cada server da VOLTA. Esta informação é importante para a seleção CB do melhor server da VOLTA de usar-se.

Server da VOLTA da via expressa do exemplo único:

```
Configured TURN / Edge servers: 1
  eef94a2b-3bfa-40f7-b83c-ece8df424e15: 10.48.36.248:3478 (turn=1,edge=0,acano=0)

10.48.36.5 TURN chooser, local port number 56425
  eef94a2b-3bfa-40f7-b83c-ece8df424e15 (10.48.36.248:3478), results: 1
    0: server address 10.48.36.248:3478, reachable for 156s, mapped address 10.48.36.5:56425,
RTT 44ms
```

```
  best : eef94a2b-3bfa-40f7-b83c-ece8df424e15, server address 10.48.36.248:3478, reachable for
156s, mapped address 10.48.36.5:56425, RTT 44ms
  best (not msEdge): eef94a2b-3bfa-40f7-b83c-ece8df424e15, server address 10.48.36.248:3478,
reachable for 156s, mapped address 10.48.36.5:56425, RTT 44ms
  no best result (msEdge) returned
```

Exemplo dos server múltiplos da VOLTA da via expressa:

```
  Configured TURN / Edge servers: 2
  eef94a2b-3bfa-40f7-b83c-ece8df424e15: 10.48.36.248:3478 (turn=1,edge=0,acano=0)
  7eecf3eb-49f2-4963-bf67-2bac98355ca1: 10.48.79.129:3478 (turn=1,edge=0,acano=0)

10.48.36.5 TURN chooser, local port number 56425
  eef94a2b-3bfa-40f7-b83c-ece8df424e15 (10.48.36.248:3478), results: 1
    0: server address 10.48.36.248:3478, reachable for 283s, mapped address 10.48.36.5:56425,
RTT 52ms
  7eecf3eb-49f2-4963-bf67-2bac98355ca1 (10.48.79.129:3478), results: 1
    0: server address 10.48.79.129:3478, reachable for 64s, mapped address 10.48.36.5:56425, RTT
64ms
  best : eef94a2b-3bfa-40f7-b83c-ece8df424e15, server address 10.48.36.248:3478, reachable for
283s, mapped address 10.48.36.5:56425, RTT 52ms
  best (not msEdge): eef94a2b-3bfa-40f7-b83c-ece8df424e15, server address 10.48.36.248:3478,
reachable for 283s, mapped address 10.48.36.5:56425, RTT 52ms
  no best result (msEdge) returned
```

Etapa 3. Na altura de um atendimento vivo que seja feito com o uso do cliente de WebRTC, você pode ver o estado do relé dos media da VOLTA na via expressa. Navegue ao **uso do relé do estado > da VOLTA,** a seguir selecione a **vista.**

Troubleshooting

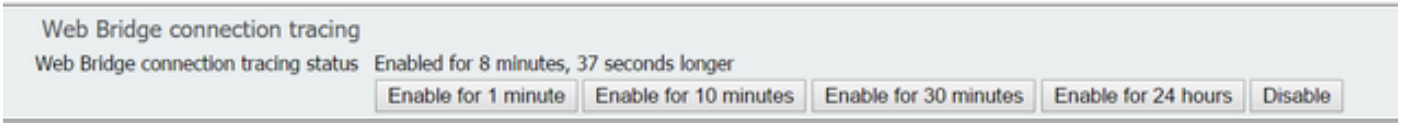
Esta seção fornece a informação que você pode se usar para pesquisar defeitos sua configuração, algumas edições de WebRTC e falhas possíveis típicas.

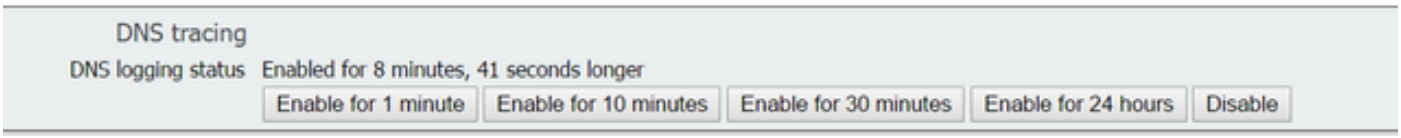
Os logs para as conexões WB e o traçado DNS podem ser permitidos no WebAdmin do server CMS:

a. Conecte ao **WebAdmin**

b. Navegue aos **logs > detalhou o seguimento**

c. Permita o **traçado da conexão de Bridge da Web** e o **DNS que seguem** para a duração desejada:





O debug logging do console de Chrome e de Firefox pode ser usado para pesquisar defeitos falhas da conexão de cliente de WebRTC, tais como edições com media e Conectividade à WB. Isto pode ser feito visível com o uso da combinação **Ctrl+Shift+C. do** teclado.

Em Chrome, use **chrome://webrtc-internals/** ou **aproximadamente: webrtc em** Firefox, em uma aba

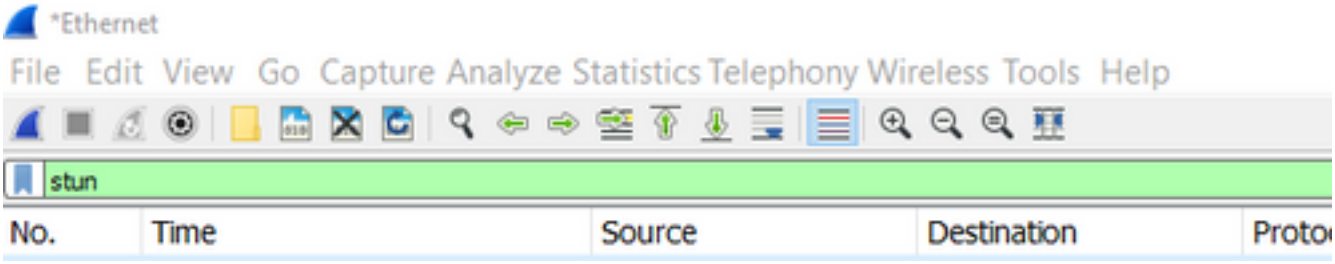
separada na altura de um atendimento vivo para indicar os diagnósticos avançados, que seja útil pesquisar defeitos edições dos media com WebRTC.

A captura de pacote de informação de Whireshark no cliente de WebRTC igualmente fornece alguma informação util sobre o relé dos media o server da VOLTA.

O cliente de WebRTC conecta mas nenhum media (devendo CONGELAR a falha)

Comece o wireshark quando você tenta a um atendimento e quando a falha ocorre, param a captação.

Filtre os traços com **aturdem**, veem o exemplo:



Nos traços de Wireshark, você vê que o cliente envia **atribui o pedido** com as credenciais configuradas, ao server da VOLTA 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 server responde com **atribui o erro**:

```
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
```

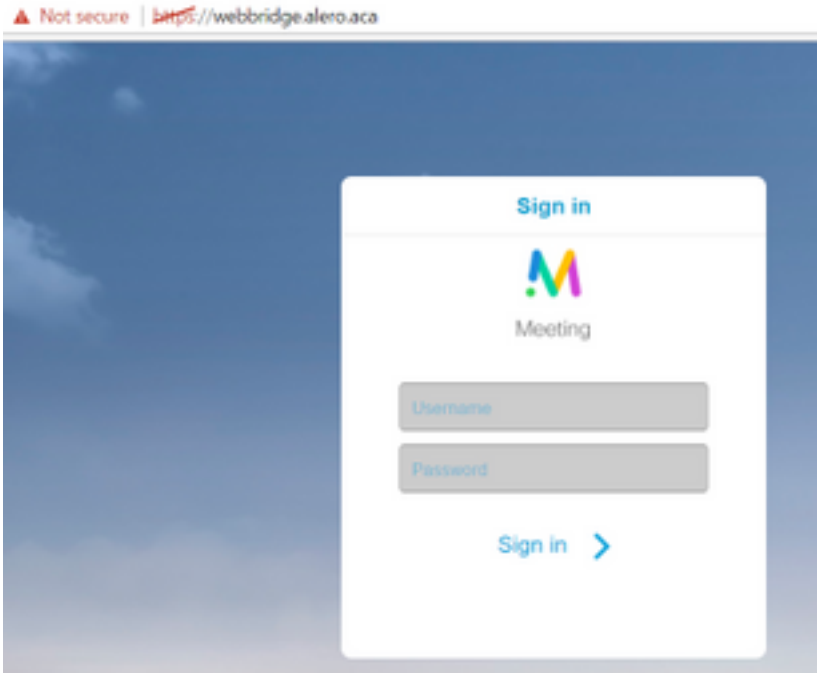
Nos logs CMS, o mensagem de registro abaixo é mostrado:

```
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 da VOLTA configuradas no server CMS e assegure-se de que combine aquele configurado no base de dados de autenticação local da via expressa-e.

O cliente de WebRTC não obtém junta-se à opção de atendimento



No estado de Callbridge **> a** página **geral**, isto é indicada:

```
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:

- Assegure-se de que o Callbridge possa resolver o FQDN WB ao endereço IP interno (o Callbridge não deve resolver este ao endereço IP de Um ou Mais Servidores Cisco ICM NT do Via-e)
- Nivele o esconderijo DNS no Callbridge, através do comando line interface(cli), com o **resplendor dns do** comando
- Assegure-se de que a WB confie o certificado de servidor de Callbridge (não o expedidor)