Configurar o proxy WebRTC com CMS sobre Expressway com domínio duplo

Contents

Introduction

Este documento descreve um exemplo de configuração da Web Real-Time Communication (WebRTC) de proxy para o Cisco Meeting Server (CMS) através do Expressway com diferentes domínios internos e externos.

Prerequisites

Requirements

A Cisco recomenda que você conheça estes tópicos:

- Implantação única combinada CMS versão 2.1.4 e superior
- Expressway C e Expressway E versão X8.9.2 e superior
- Callbridge e webbridge configurados no CMS
- Acesso móvel e remoto (MRA) habilitado no par Expressway

- Tecla de opção Traversal Using Relay NAT (TURN) adicionada ao Expressway-E
- Registro do Servidor de Nomes de Domínio (DNS) resolvível externo para URL da webbridge, para domínio externo
- Registro DNS resolvível interno para endereço IP CMS de domínio externo para domínio interno
- Multisdomínio Extensible Messaging and Presence Protocol (XMPP) configurado no CMS, para domínio interno e externo
- Porta TCP 443 aberta no Firewall da internet pública para o endereço IP público do Expressway-E
- Porta TCP e UDP 3478 aberta no Firewall da Internet Pública para o endereço IP público do Expressway-E
- Intervalo de portas UDP 24000-29999 abertas no Firewall para e do endereço IP público do Expressway-E

Componentes Utilizados

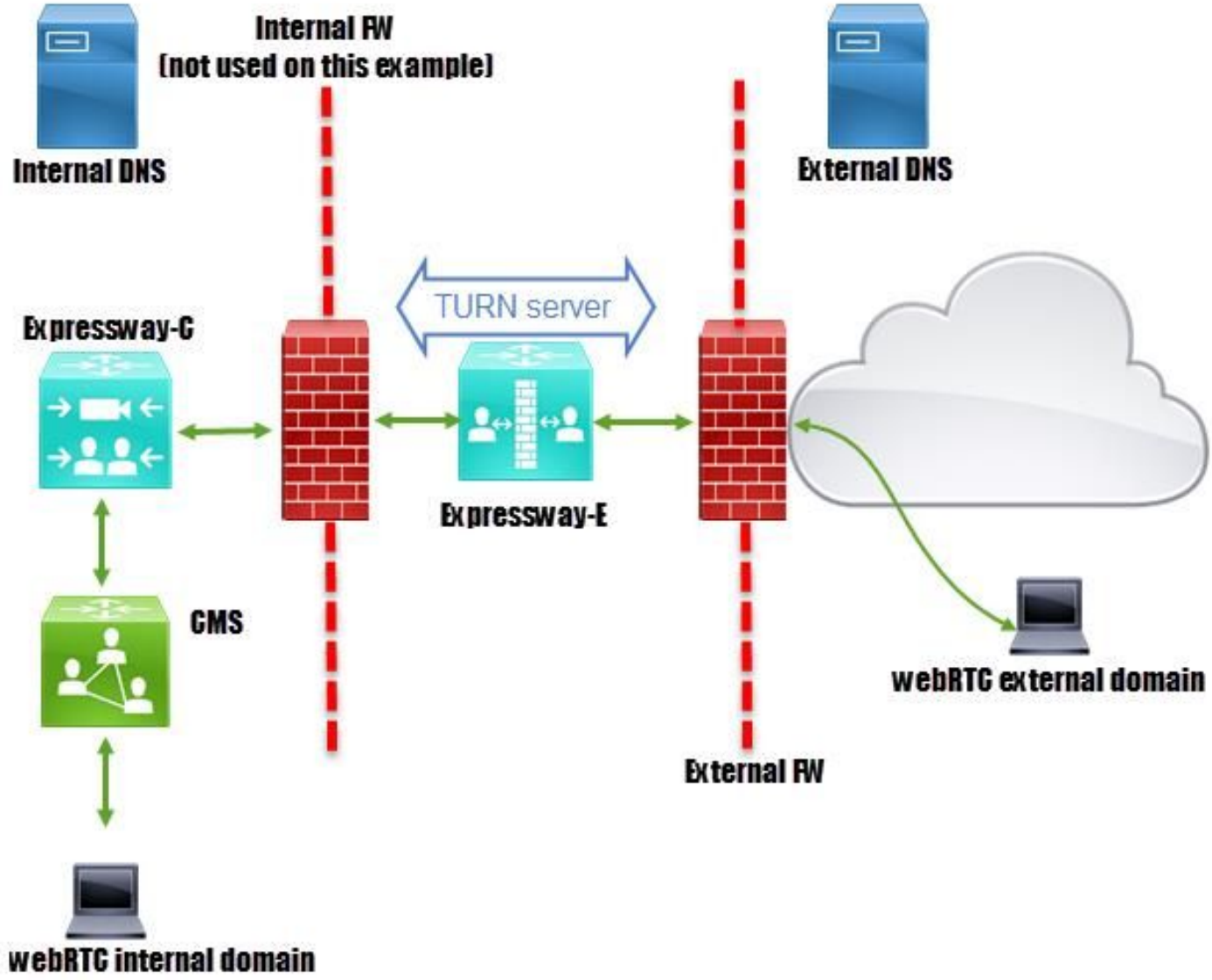
As informações neste documento são baseadas nestas versões de software e hardware:

- Implantação única combinada CMS versão 2.2.1
- Expressway-C e Expressway-E com placa de interface de rede (NIC) dupla e software de conversão de endereço de rede (NAT) estático versão X8.9.2
- POSTMAN

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Diagrama de Rede

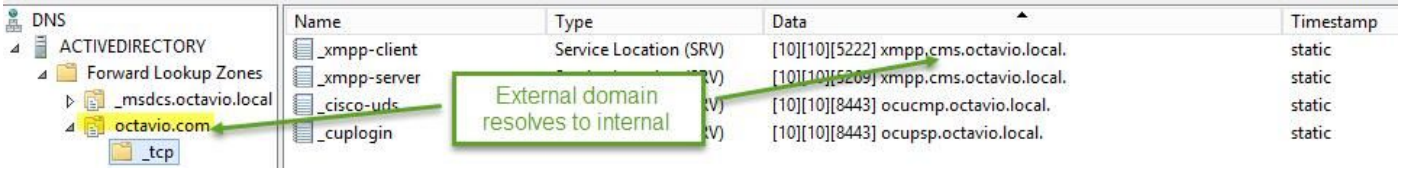


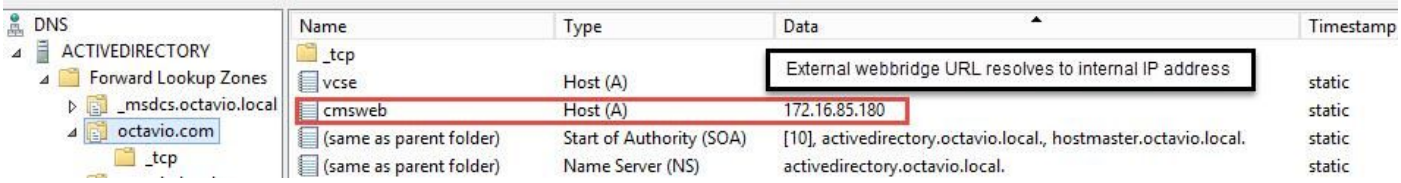
Informações técnicas

Domínio interno	cms.octavio.local
Domínio externo	octavio.com
endereço IP CMS	172.16.85.180
Endereço IP do Expressway-C	172.16.85.167
Endereço IP da LAN1 Expressway-E (interno)	172.16.85.168
Endereço IP da LAN2 Expressway-E (externo)	192.168.245.61
Endereço IP NAT estático	10.88.246.156

Configuração DNS

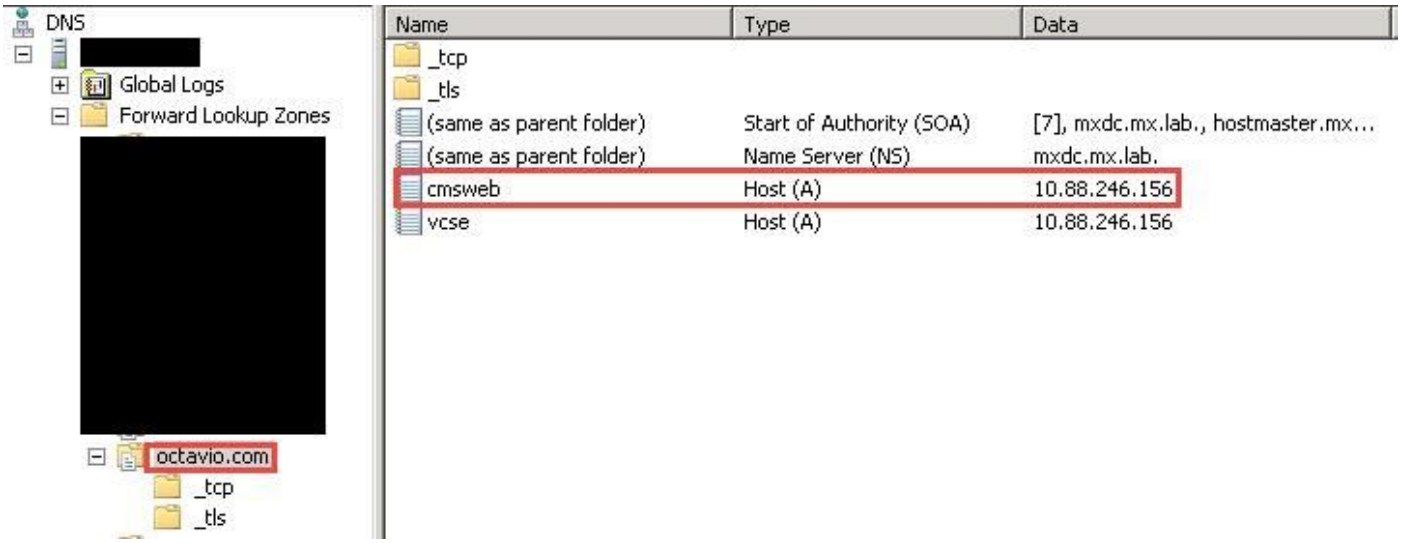
Configuração interna de DNS





Configuração de DNS externo

O DNS externo deve ter a URL da webbridge que é resolvida para o endereço IP de NAT estático do Expressway-E como mostrado na imagem.



Configuração de CMS, Callbridge, Webbridge e XMPP

Etapa 1. Você deve ter a licença callbridge ativada. A imagem mostra uma licença callbridge ativa.

```
proxyWebRTC> license
Feature: callbridge status: Activated expiry: 2017-Jul-09
```

Para obter mais informações sobre licenciamento:

http://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Deployment_Guide/Version-2-1/Cisco-Meeting-Server-2-1-Single-Combined-Server-Deployment.pdf#page=10

Etapa 2. Ative callbridge, webbridge e XMPP por meio do MMP, como mostrado na imagem.

```
proxyWebRTC> callbridge
Listening interfaces   : a
Preferred interface    : none
Key file               : callbridge.key
Certificate file       : callbridge.cer
Address                : none
CA Bundle file         : root.cer
proxyWebRTC>
proxyWebRTC> webbridge
Enabled                : true
Interface whitelist    : a:443
Key file               : webbridge.key
Certificate file       : webbridge.cer
CA Bundle file         : root.cer
Trust bundle           : callbridge.cer
HTTP redirect          : Enabled
Clickonce URL          : none
MSI download URL       : none
DMG download URL       : none
iOS download URL       : none
proxyWebRTC>
proxyWebRTC> xmpp
Enabled                : true
Clustered              : false
Domain                 : cms.octavio.local
Listening interfaces   : a
Key file               : xmpp.key
Certificate file       : xmpp.cer
CA Bundle file         : root.cer
Max sessions per user  : unlimited
STATUS                 : XMPP server running
```

```
proxyWebRTC> xmpp multi_domain list
 ***
Domain                 : octavio.com
Key file               : xmppmu.key
Certificate file       : xmppmu.cer
Bundle file            : root.cer
```

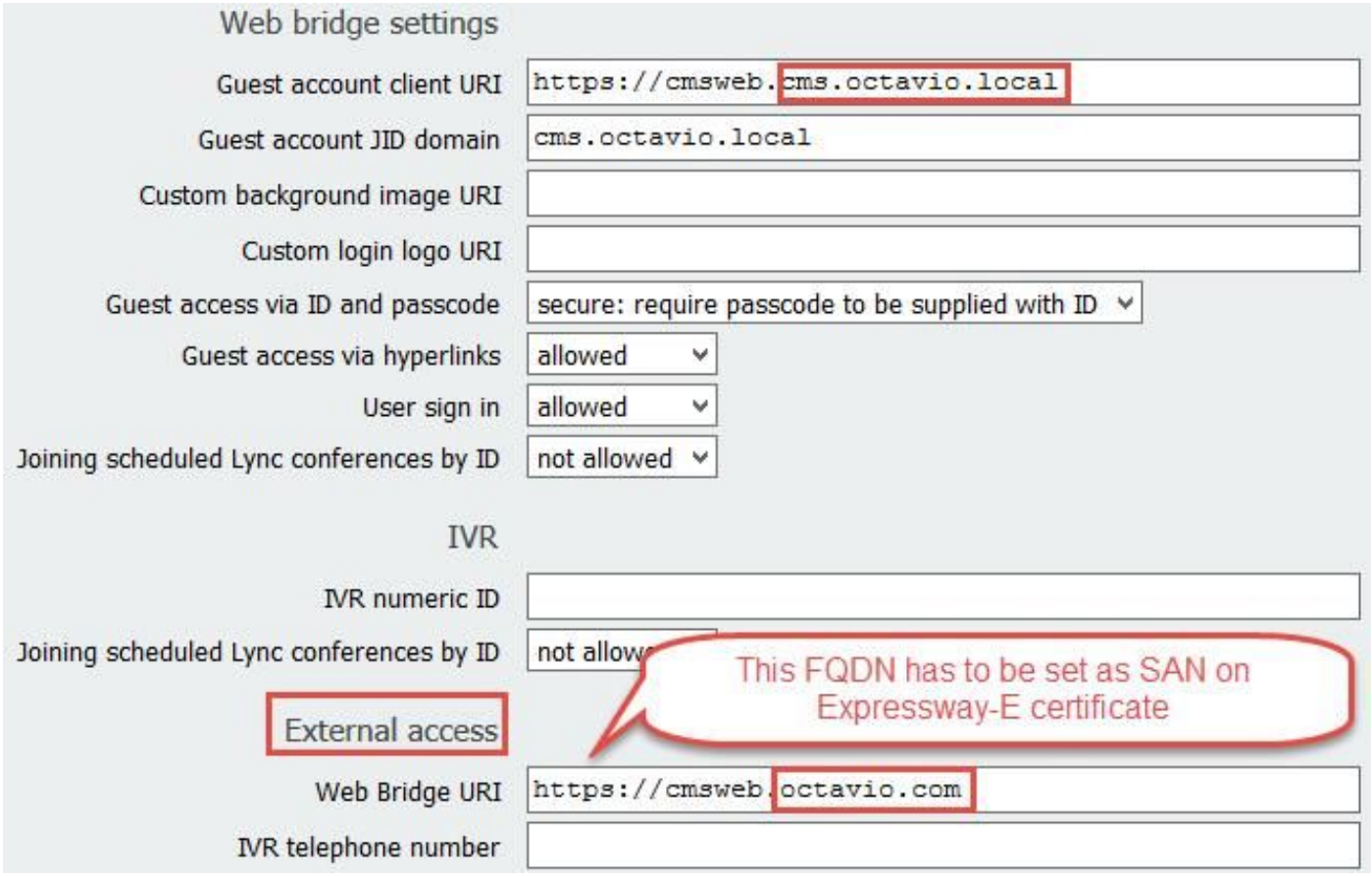
Siga este link para obter um processo detalhado sobre como habilitá-los:

http://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Deployment_Guide/Version-2-1/Cisco-Meeting-Server-2-1-Single-Combined-Server-Deployment.pdf

Siga este link para obter um processo detalhado sobre como criar um certificado:

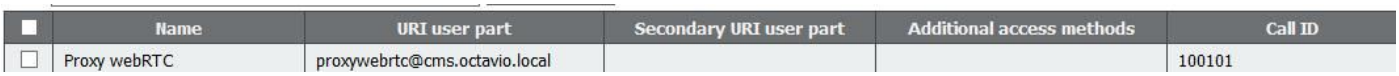
http://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Deployment_Guide/Version-2-2/Certificate-Guidelines-Single-Combined-Server-Deployment-2-2.pdf

Etapa 3. Navegue até a página da Web do CMS em **Configuration > General** e configure a URL interna e externa para a webbridge como mostrado na imagem.



Note: O CMS deve ser configurado com pelo menos um espaço.

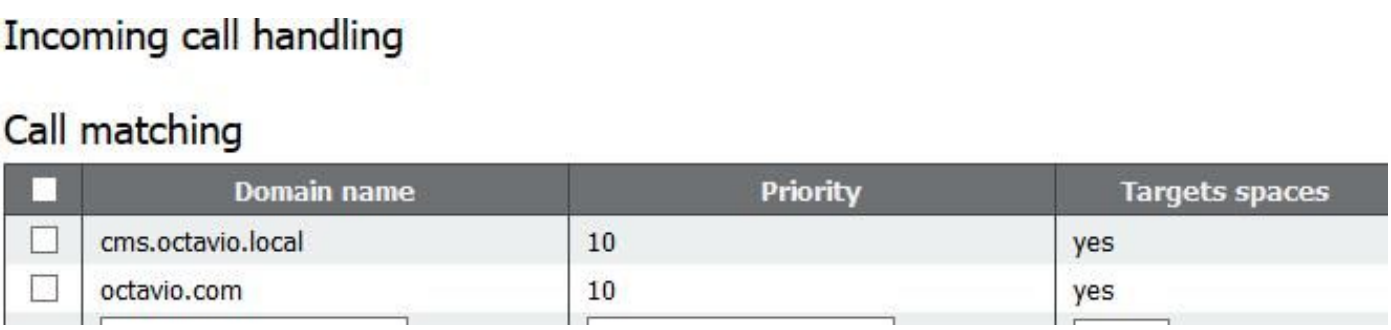
Um exemplo de um espaço configurado no CMS, como mostrado na imagem.



	Name	URI user part	Secondary URI user part	Additional access methods	Call ID
☐	Proxy webRTC	proxywebrtc@cms.octavio.local			100101

Note: As chamadas recebidas devem ser configuradas para os domínios interno e externo

Um exemplo de domínios configurados para o tratamento de chamadas recebidas é mostrado na imagem.



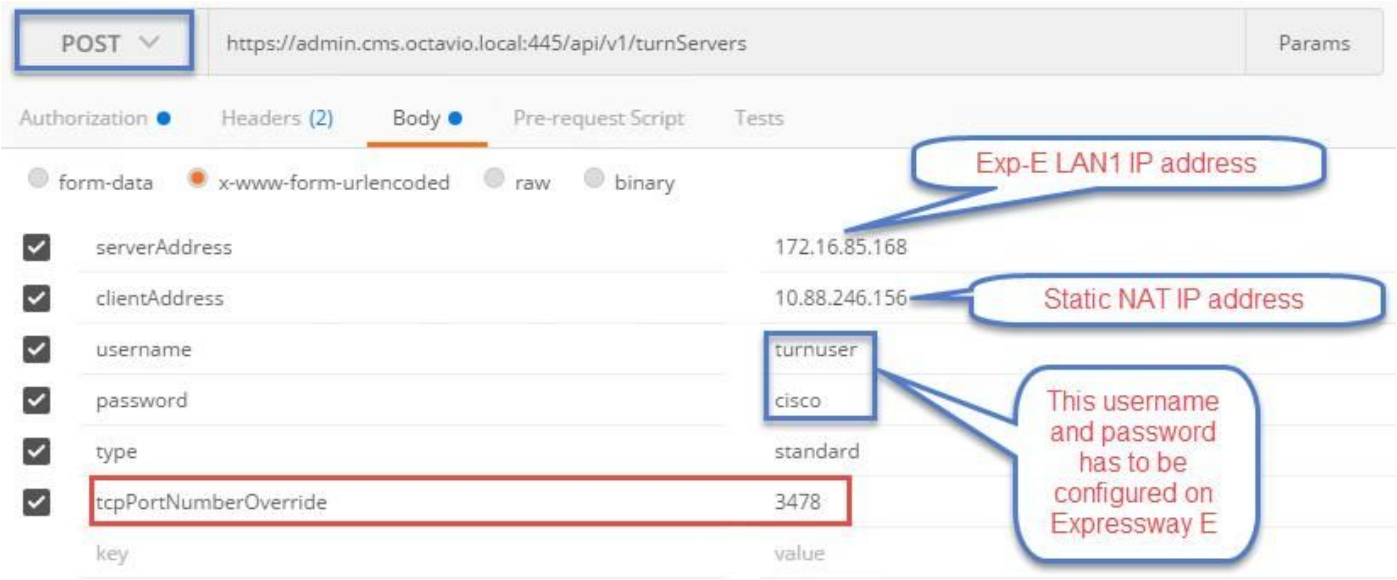
Configuração de TURN

Etapa 1. TURN deve ser configurado pela API através do Postman. Esse comando é usado em

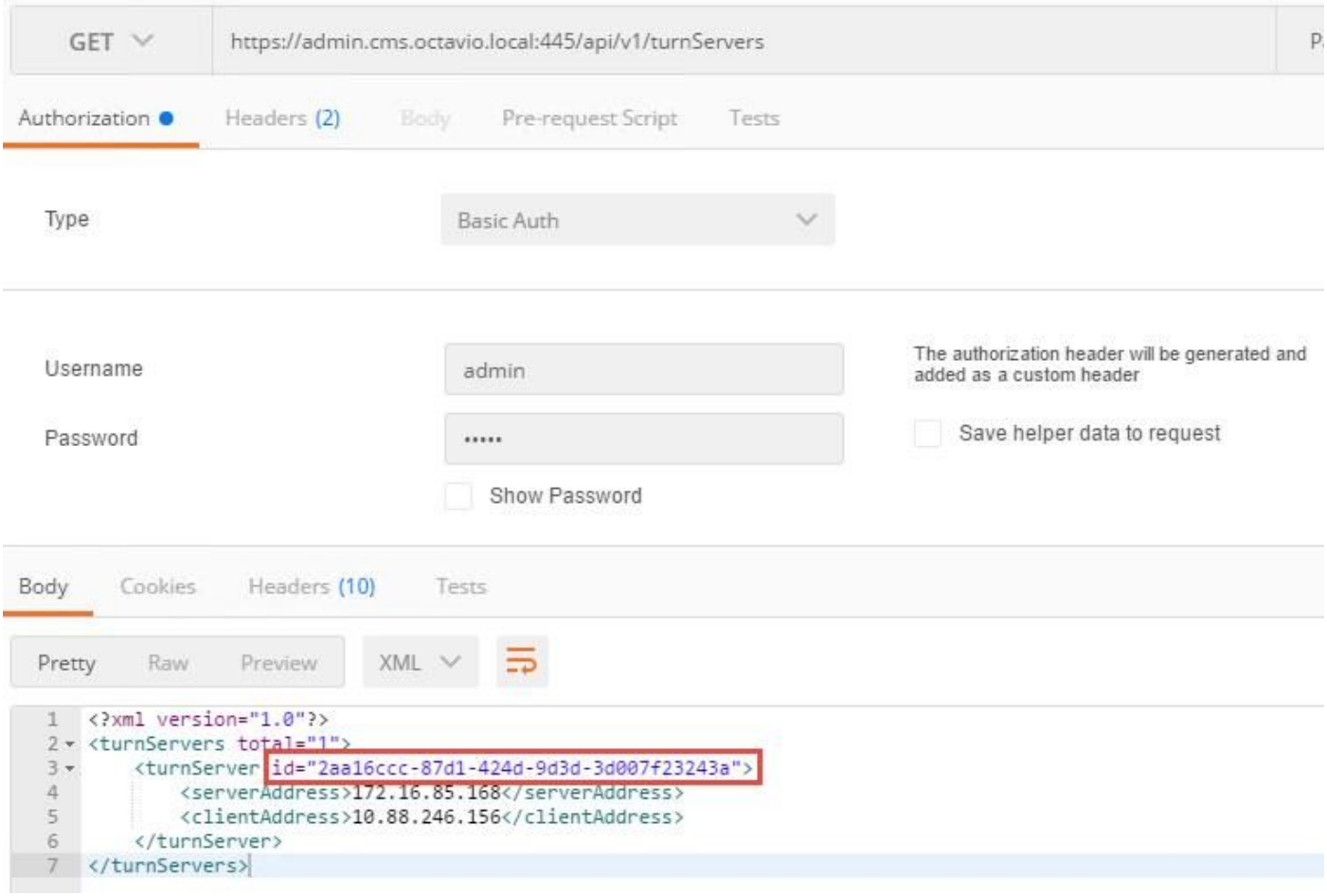
toda a configuração.

https://

Etapa 2. Use o método POST e navegue até **Body** para exibir os parâmetros do servidor TURN ou editá-los. Os parâmetros configurados para o servidor TURN são como mostrado na imagem.

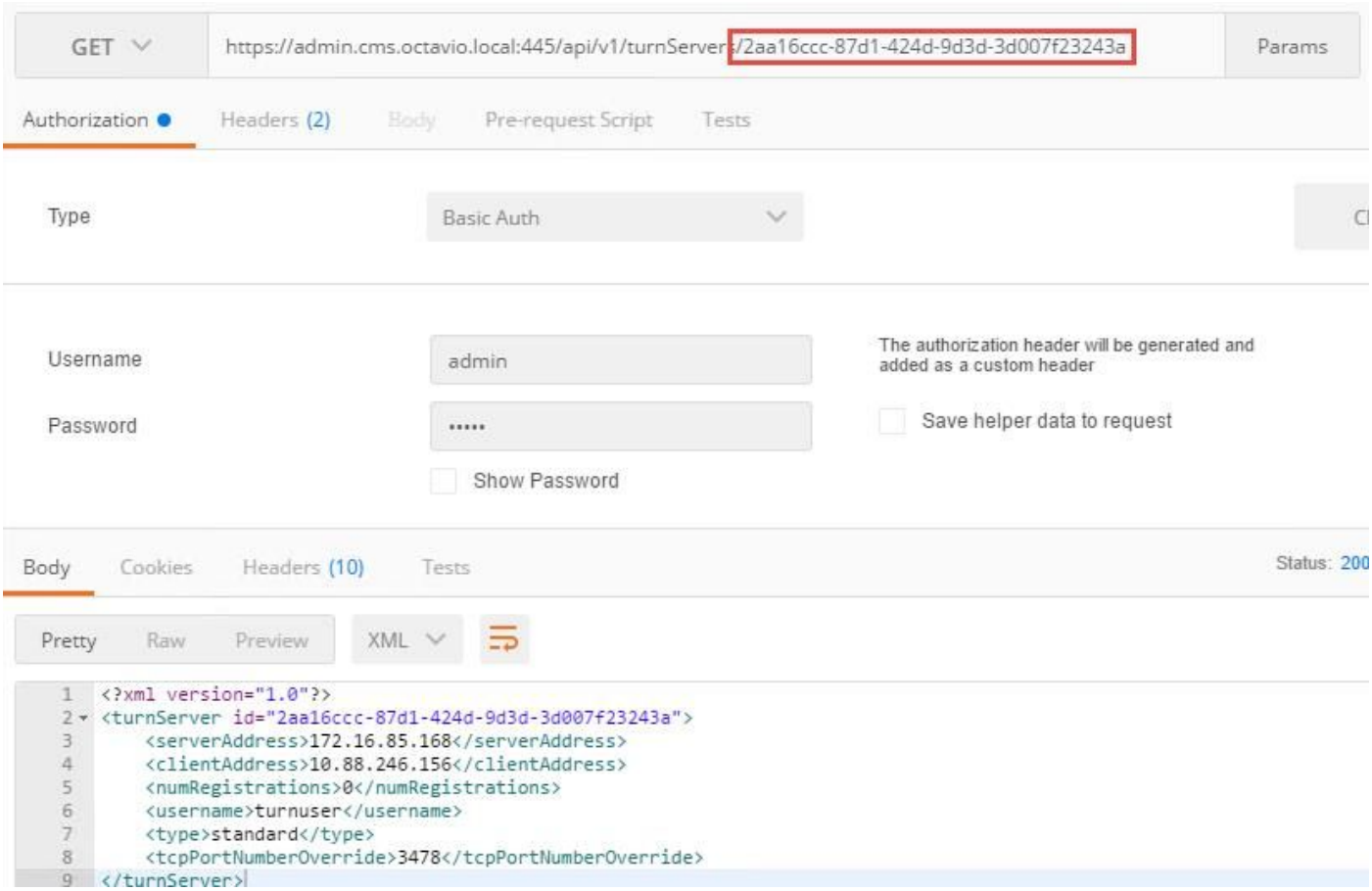


Etapa 3. Verifique o status da configuração do servidor TURN executando o método GET e copiando a ID do servidor. O ID que deve ser copiado é como mostrado na imagem.

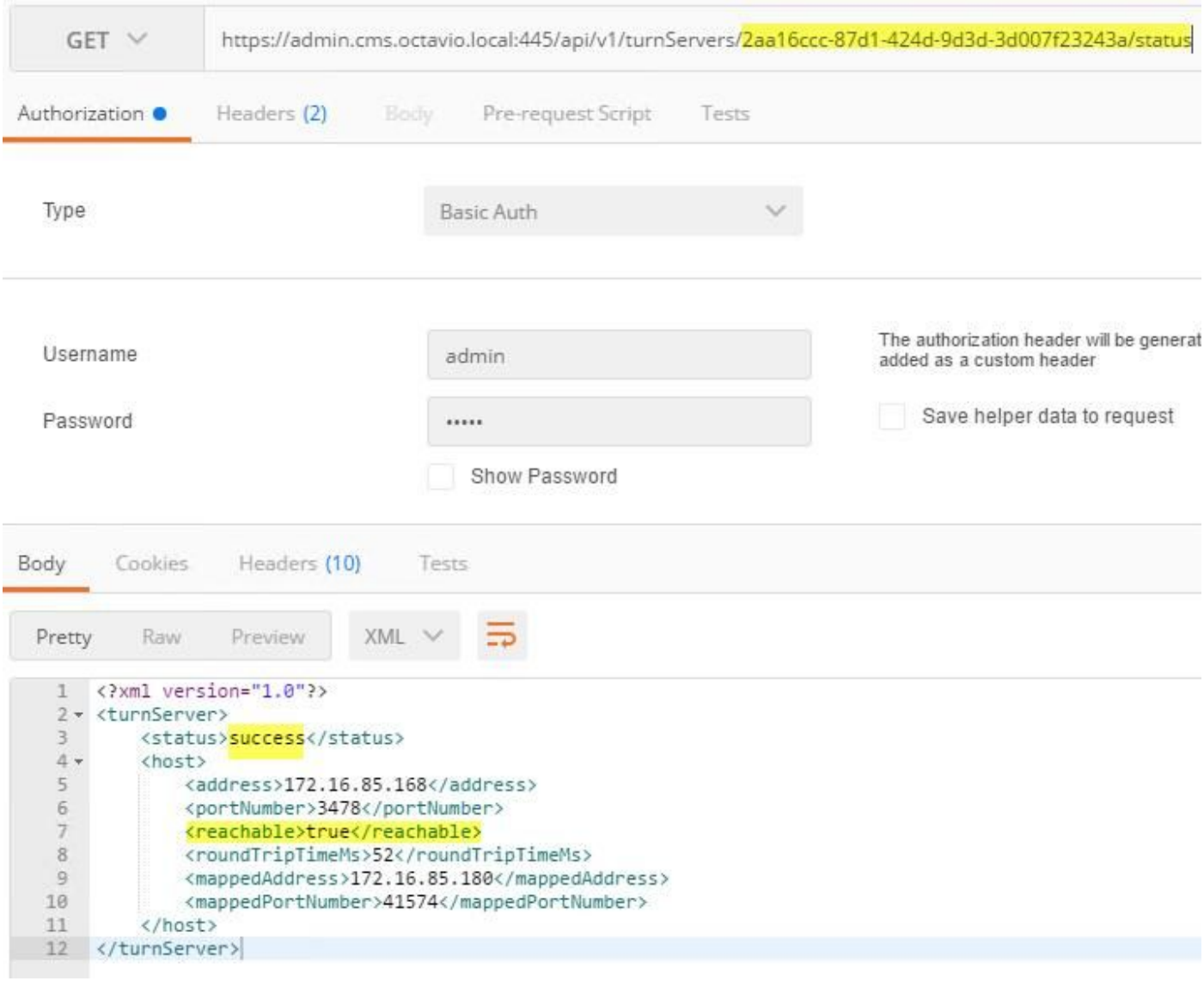


Etapa 4. Copie a ID no final do comando API e use o método GET para ver as informações do servidor TURN como mostrado na imagem.

Note: As informações não mostrarão a senha do servidor.

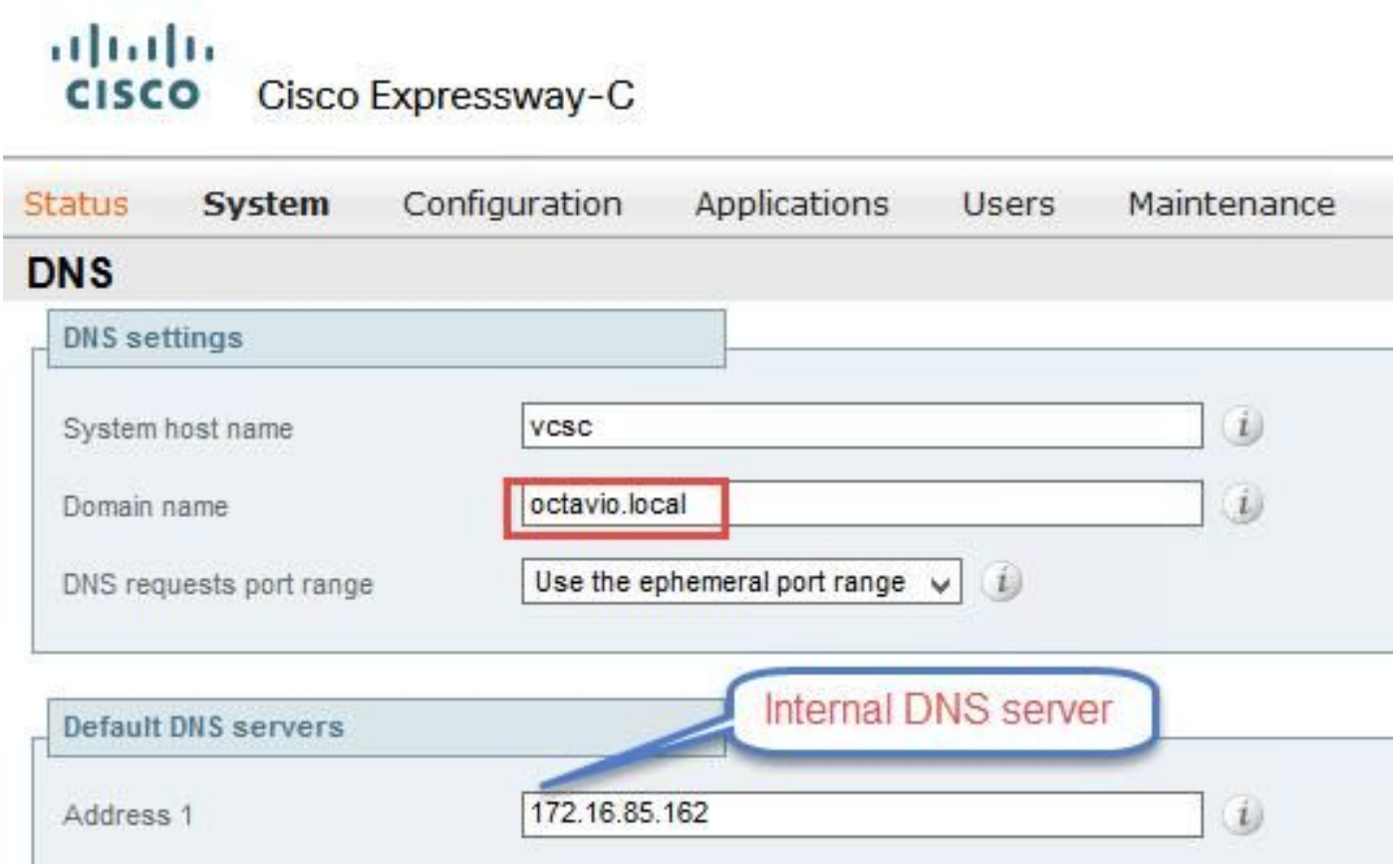


Etapa 5. Clique em **enviar** para obter o status do servidor. Um exemplo de uma configuração bem-sucedida como mostrado na imagem.



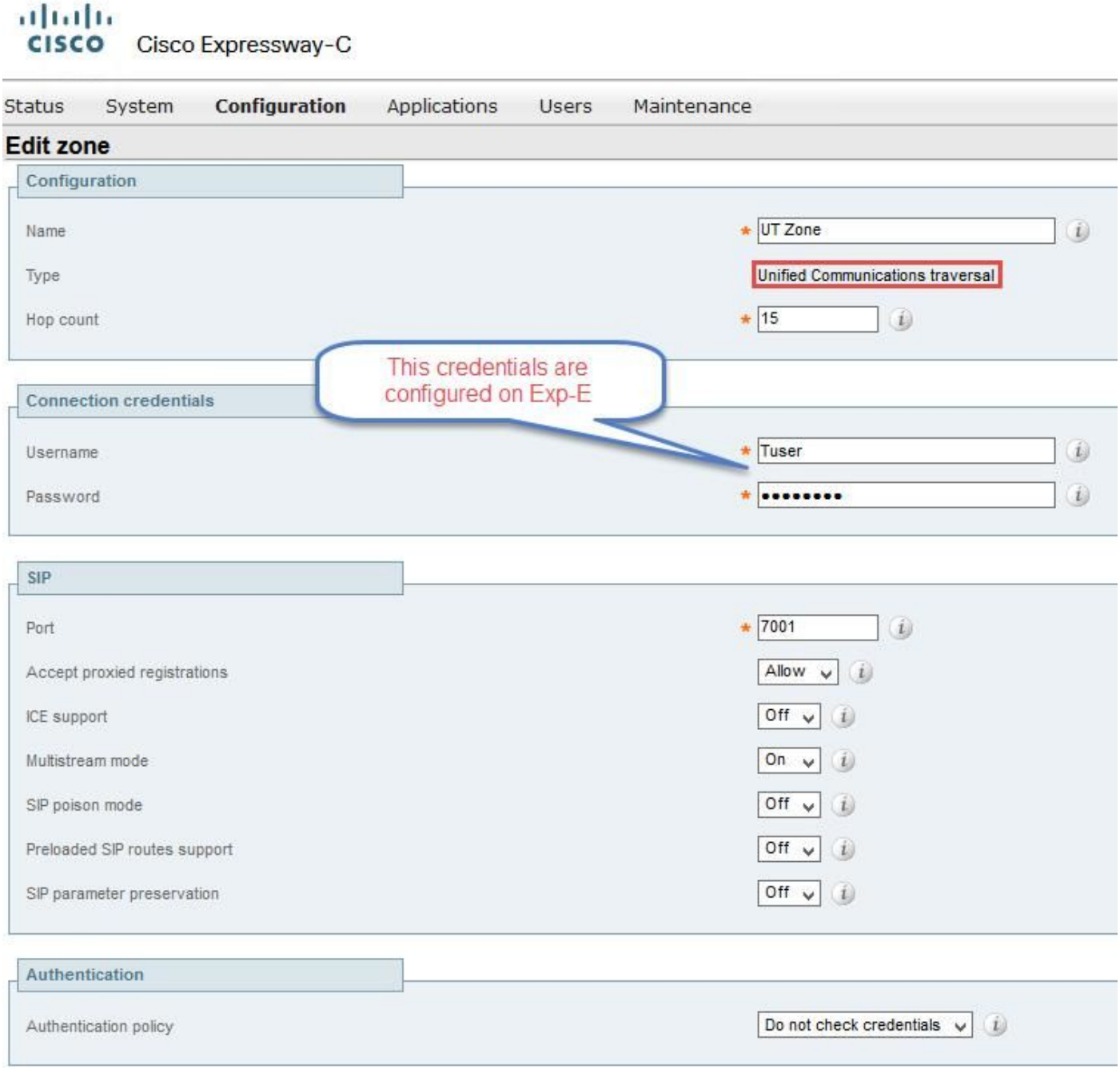
Configuração do Expressway-C e E

Etapa 1. O expressway-C deve ter o domínio interno (octavio.local) e o Expressway-E deve ter o domínio externo (octavio.com) configurado como mostrado na imagem.



Etapa 2. O MRA deve ser ativado no Expressway C e E conforme mostrado na imagem.

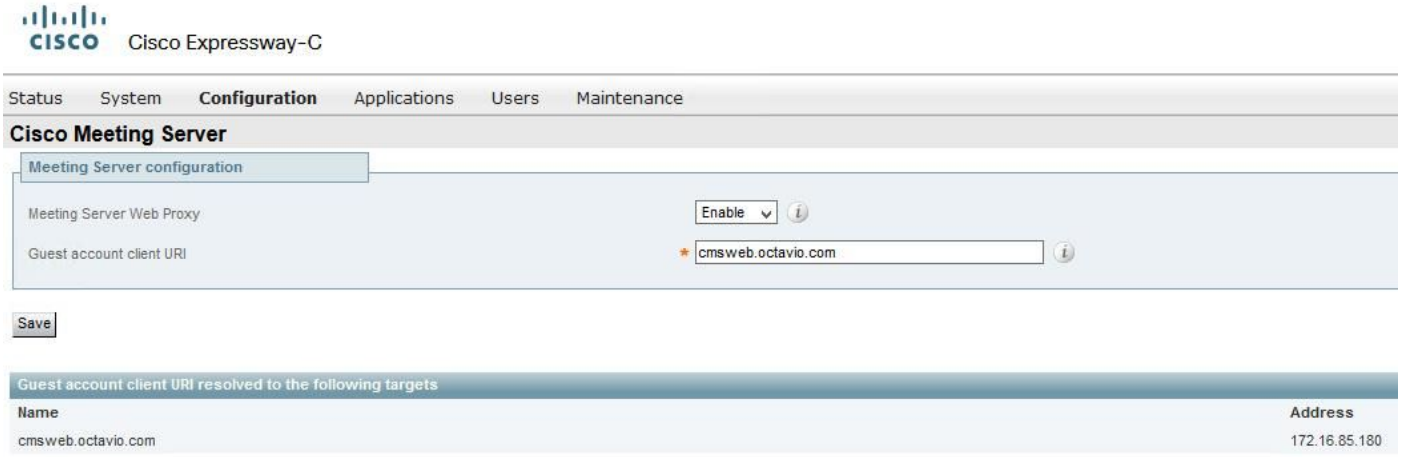
Etapa 3. Crie uma zona de passagem de comunicação unificada entre o Expressway-C e E conforme mostrado na imagem.



Configuração no Expressway-C

Etapa 1. Configure o domínio interno e externo no Expressway-C como mostrado na imagem.

Etapa 2. Ative a configuração da reunião Cisco. Navegue até **Configurarion > Unified Communications > Cisco Meeting Server** (Configuração > Comunicações unificadas > Cisco Meeting Server). Configure a URL da webbridge externa no campo URI do cliente de conta de convidado como mostrado na imagem.



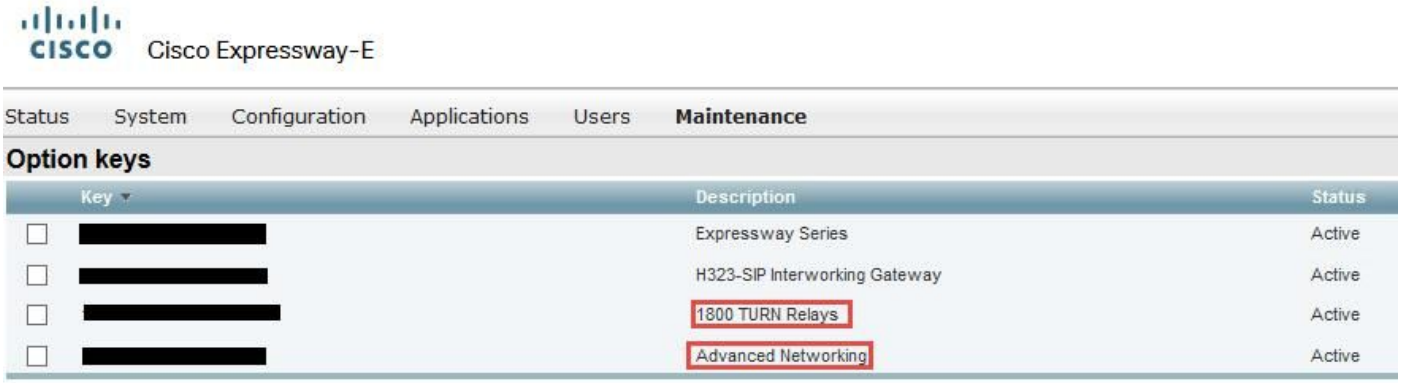
Note: O DNS interno deve resolver o URL externo da webbridge (cmsweb.octavio.com) para o endereço IP interno da webbridge do CMS. Nesse caso, o IP é 172.16.85.180.

Os túneis Secure Shell (SSH) no Expressway-C devem ficar ativos após alguns segundos como mostrado na imagem.

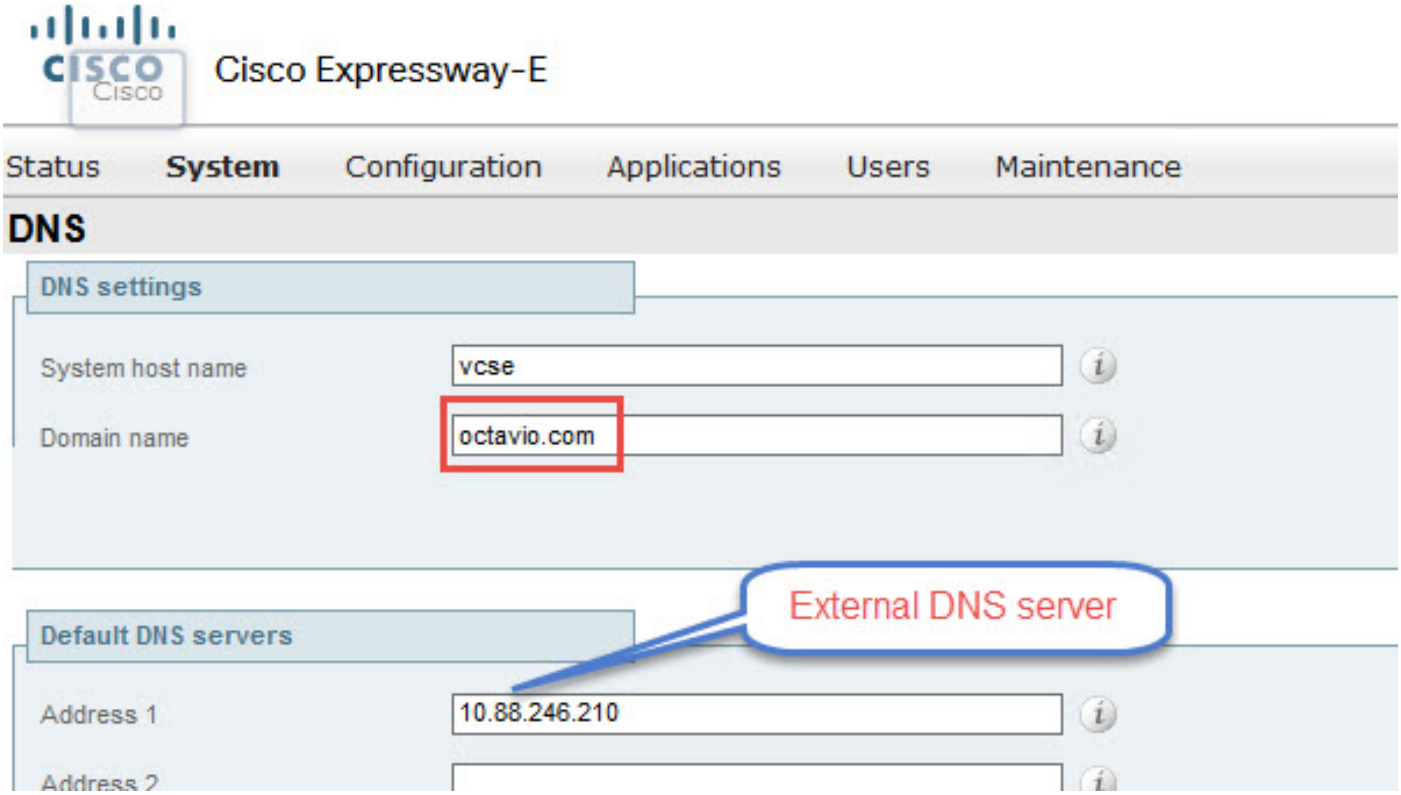
Nota:O servidor deve ter um certificado de servidor e um certificado CA.

Configuração no Expressway-E

Etapa 1. O expressway-E deve ter uma licença TURN conforme mostrado na imagem.

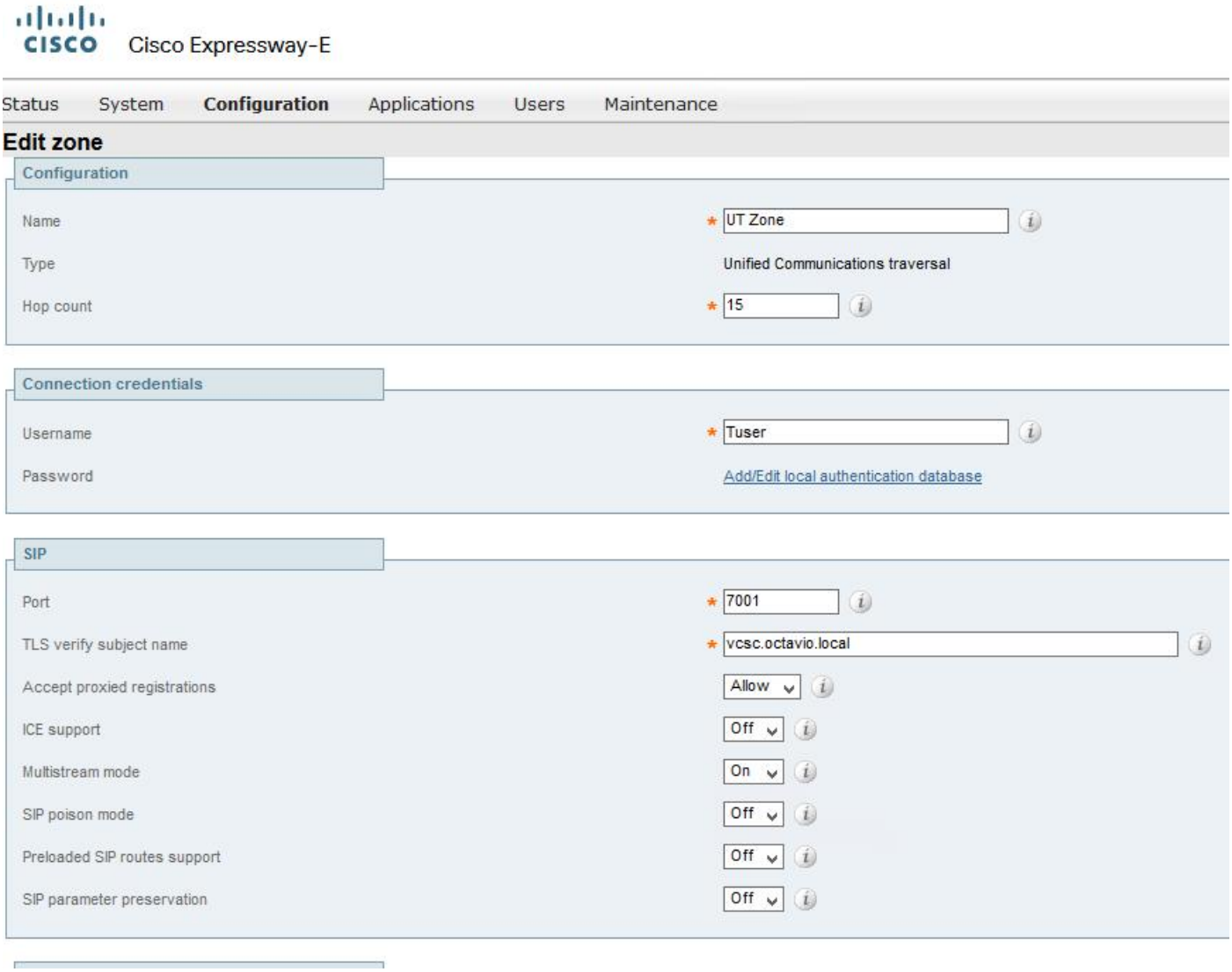


Etapa 2. O Expressway-E deve ser configurado com o domínio externo como mostrado na imagem.



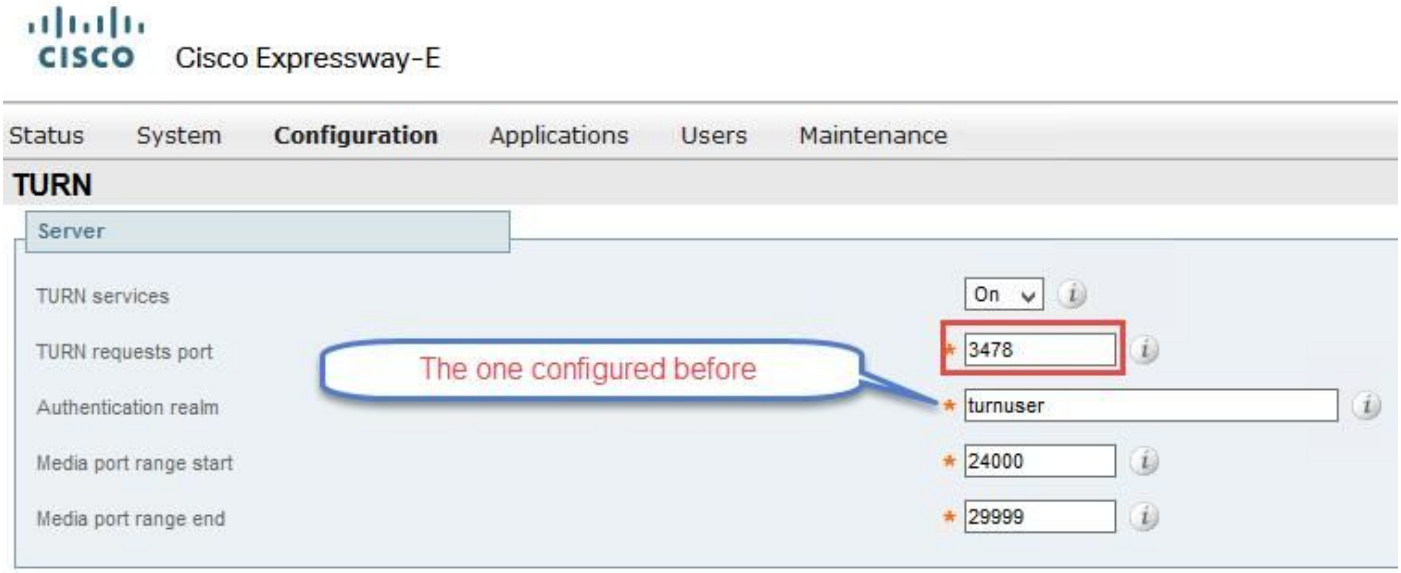
Etapa 3. Crie usuários para o servidor TURN e para a zona de passagem da Comunicação Unificada conforme mostrado na imagem.

Etapa 4. Crie uma zona de passagem de comunicação unificada conforme mostrado na imagem.



Etapa 5. Configure o servidor TURN. Navegue até **Configuration > Traversal > TURN** como mostrado na imagem.

> **Note**: A solicitação TURN deve ser para a porta 3478, pois é a porta onde o cliente Web solicita a conexão TURN.



Quando a opção Turn up (Ativar) for exibida, o status mostrará Ative (Ativo) como mostrado na imagem.

Etapa 6. Navegue até **Sistema > Administração.** O cliente webRTC solicita acesso na porta 443, por esse motivo, a porta de administração do Expressway-E deve ser alterada para outra, neste caso de exemplo, ela é alterada para 445 como mostrado na imagem.

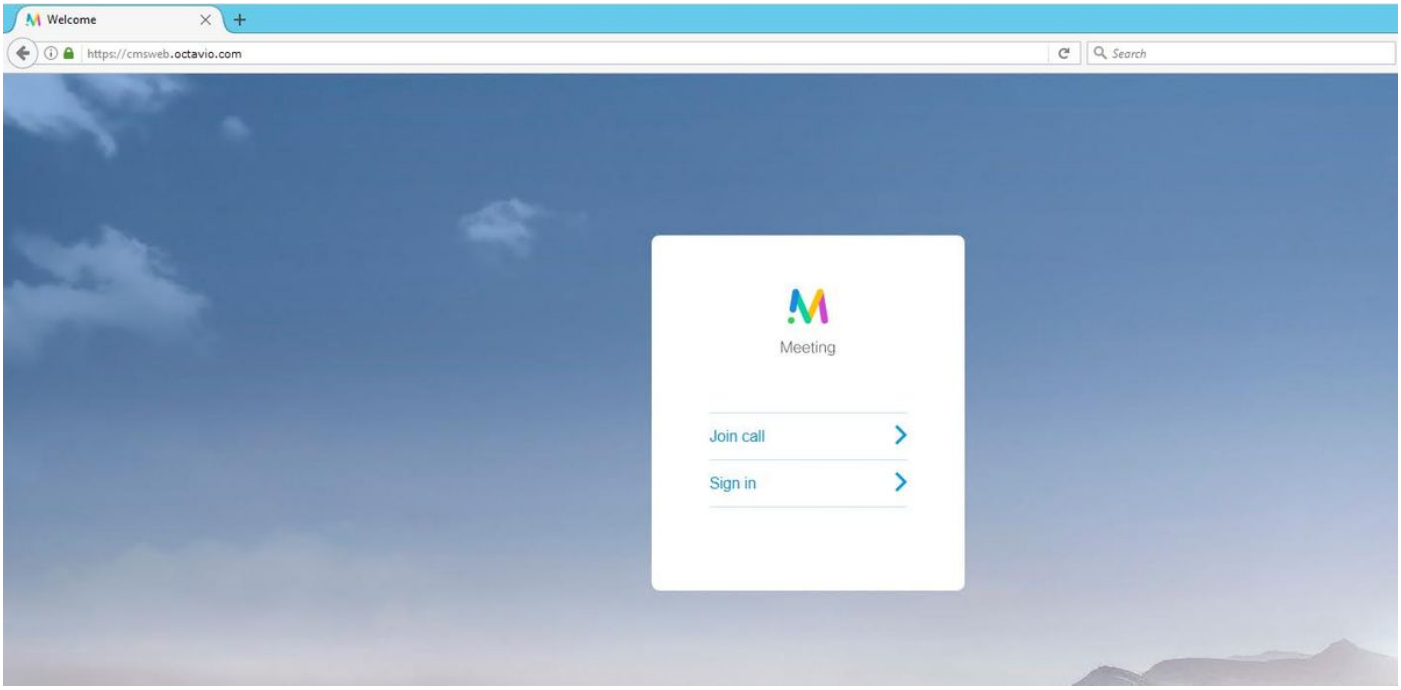
Passo 7. Criação de certificado para o Expressway-E: o URL da webbridge deve ser adicionado como uma SAN no certificado do servidor conforme mostrado na imagem.

Verificar

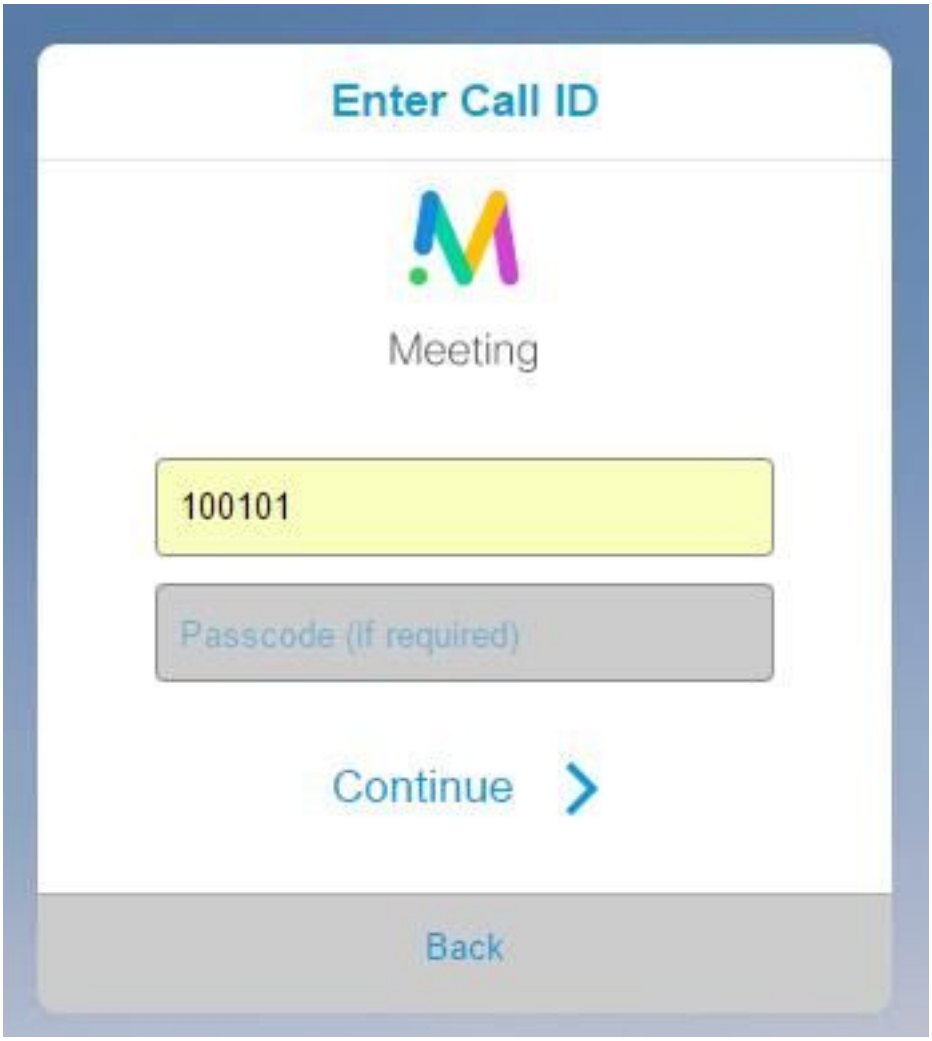
Use esta seção para confirmar se a sua configuração funciona corretamente.

Etapa 1. Selecione um navegador da Web suportado e insira o URL externo da webbridge. Você deve ver a próxima tela como mostrado na imagem.

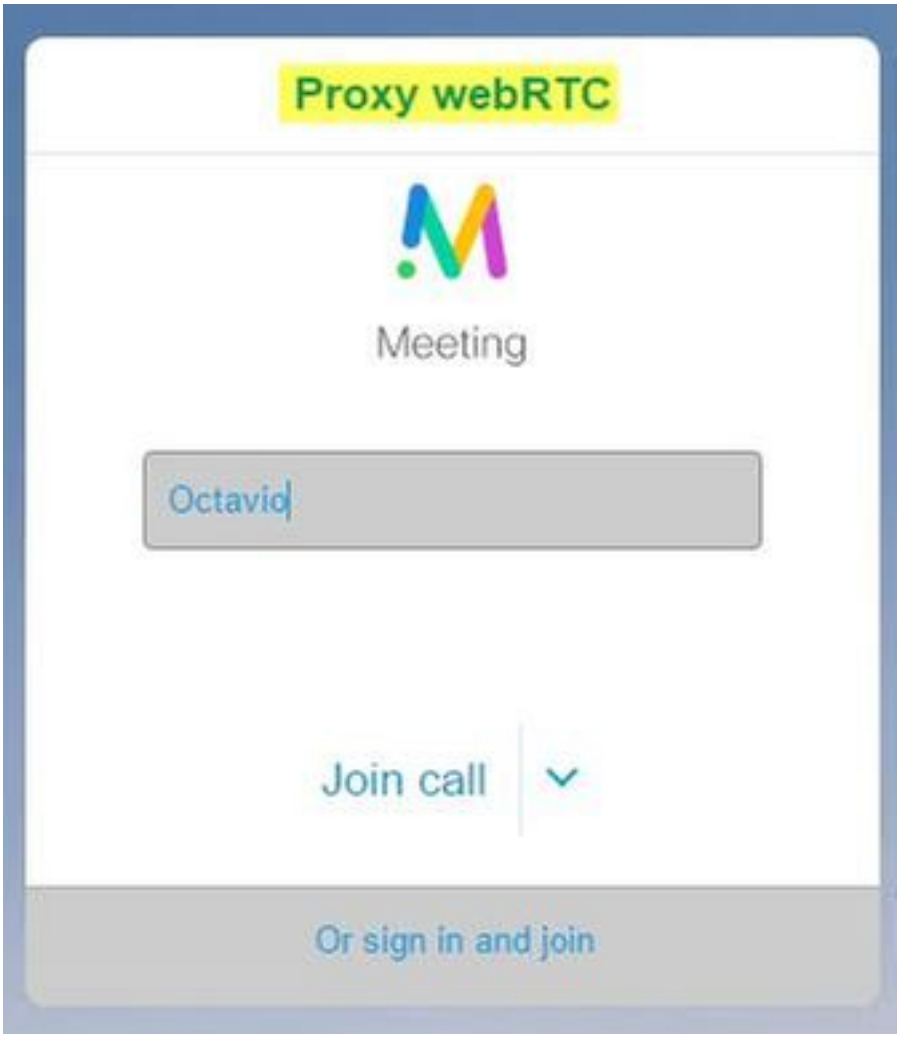
> **Note**: Você pode encontrar uma lista de navegadores e versões compatíveis no link: https://kb.acano.com/content/2/4/en/what-versions-of-browsers-do-we-support-for-webrtc.html?highlight=html%5C-5%20compliant%20browsers#content



Etapa 2. Selecione **Unir chamada** e introduza a ID de espaço previamente configurada como mostrado na imagem.



Etapa 3. Clique em **continuar** e digite seu nome. Nesse ponto, você deve ver o nome do espaço no qual você vai se unir. Nesse caso, o nome do espaço é Proxy webRTC**.** Clique em **Unir chamada** conforme mostrado na imagem.



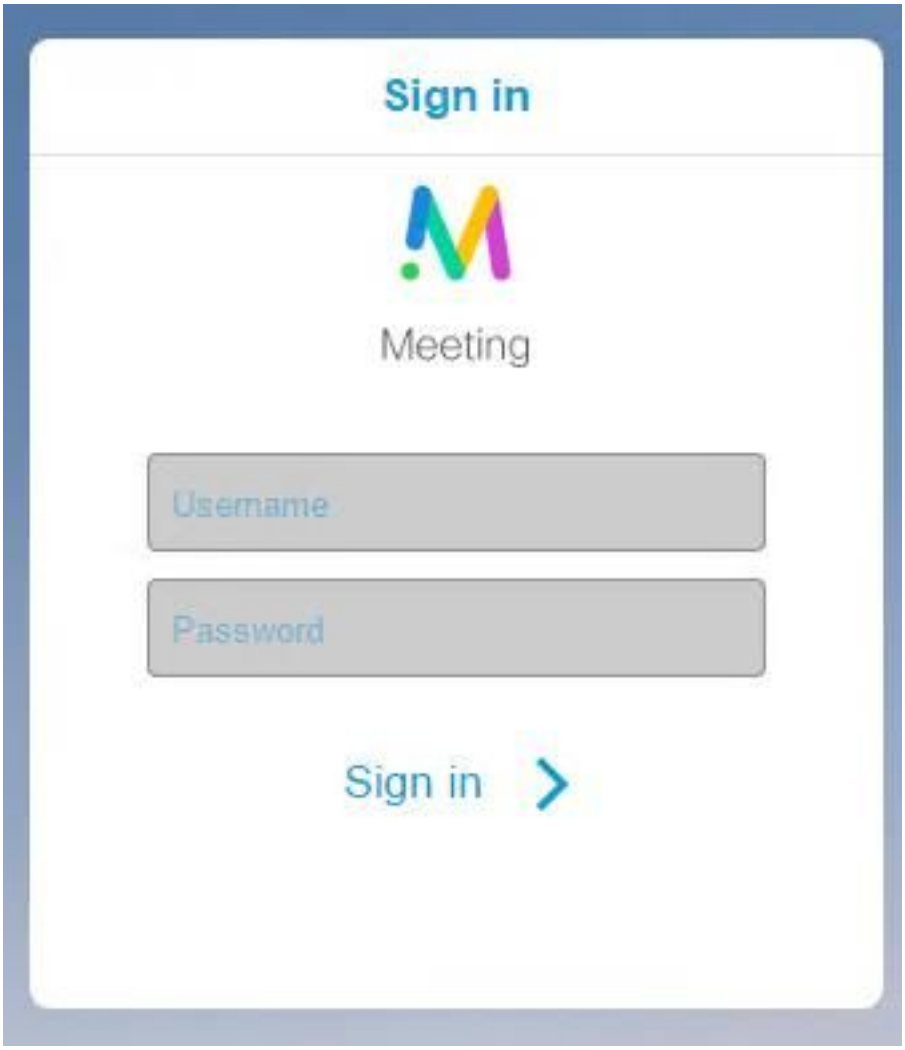
Etapa 4. Junte-se a outro dispositivo e você deve ver ambos os dispositivos conectados na conferência como mostrado na imagem.

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

O botão Participar de chamada não é exibido

O botão **Participar da chamada** não é mostrado quando você abre a página da webbridge e o erro mostrado na segunda imagem é exibido quando você entra na página da Web do CMS como mostrado na imagem.



Fault conditions

Date	Time	Fault condition
2017-05-20	18:15:28.769	Web bridge connection to "cmsweb.cms.octavio.local" failed (connect failure)

O problema acontece quando a webbridge não se comunica corretamente com a call bridge.

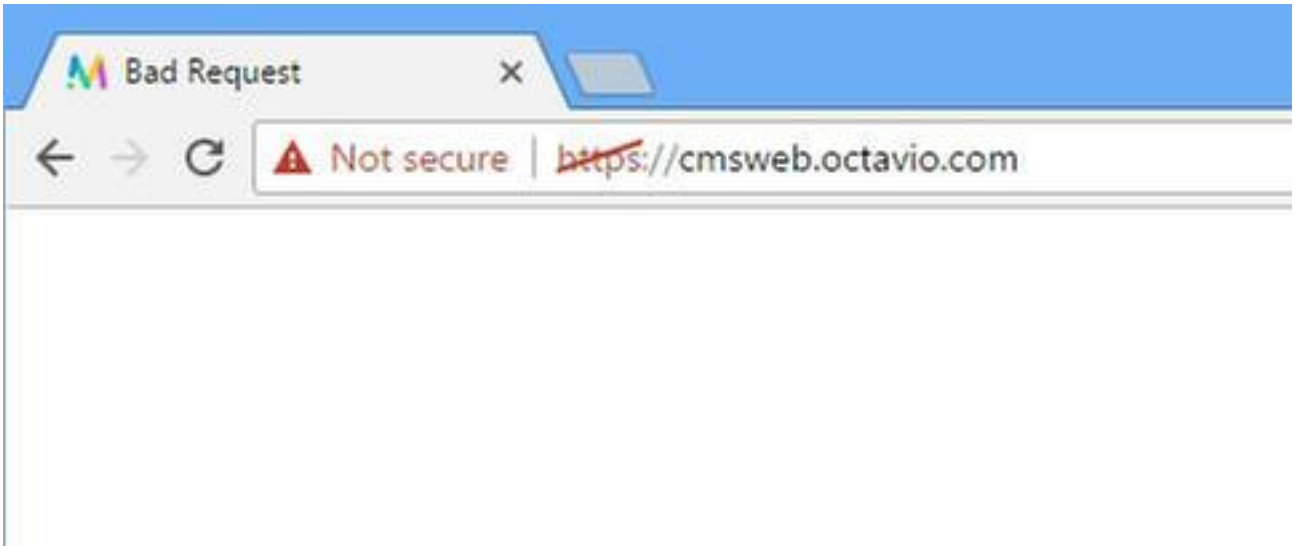
Solução

- Verifique se o URL da webbridge está configurado corretamente na página da Web do administrador do CMS. Navegue até **Configuration > General** para esse fim.
- O webbridge e o callbridge devem confiar um no outro, verifique se o pacote de confiança é adicionado à configuração do webbridge como mostrado nas imagens:

```
proxyWebRTC> webbridge
Enabled                    : true
Interface whitelist        : a:443
Key file                   : webbridge.key
Certificate file           : webbridge.cer
CA Bundle file             : root.cer
Trust bundle               : none
HTTP redirect              : Enabled
Clickonce URL              : none
MSI download URL           : none
DMG download URL           : none
iOS download URL           : none
proxyWebRTC>
proxyWebRTC>
```

Note: O pacote de confiança é o certificado de ponte de chamada.

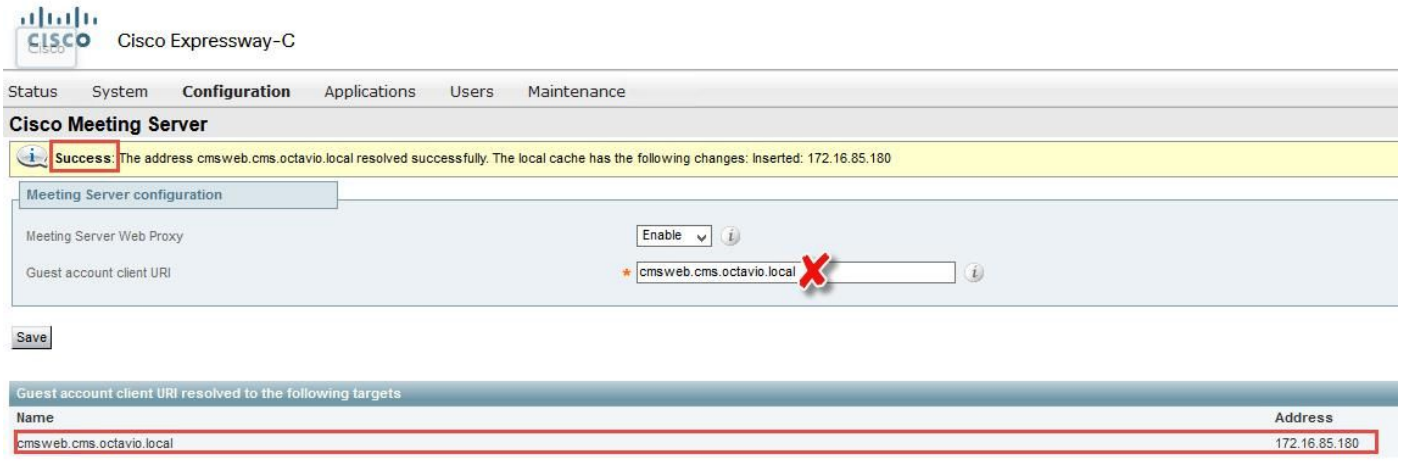
A página WebRTC mostra 'Solicitação inválida'



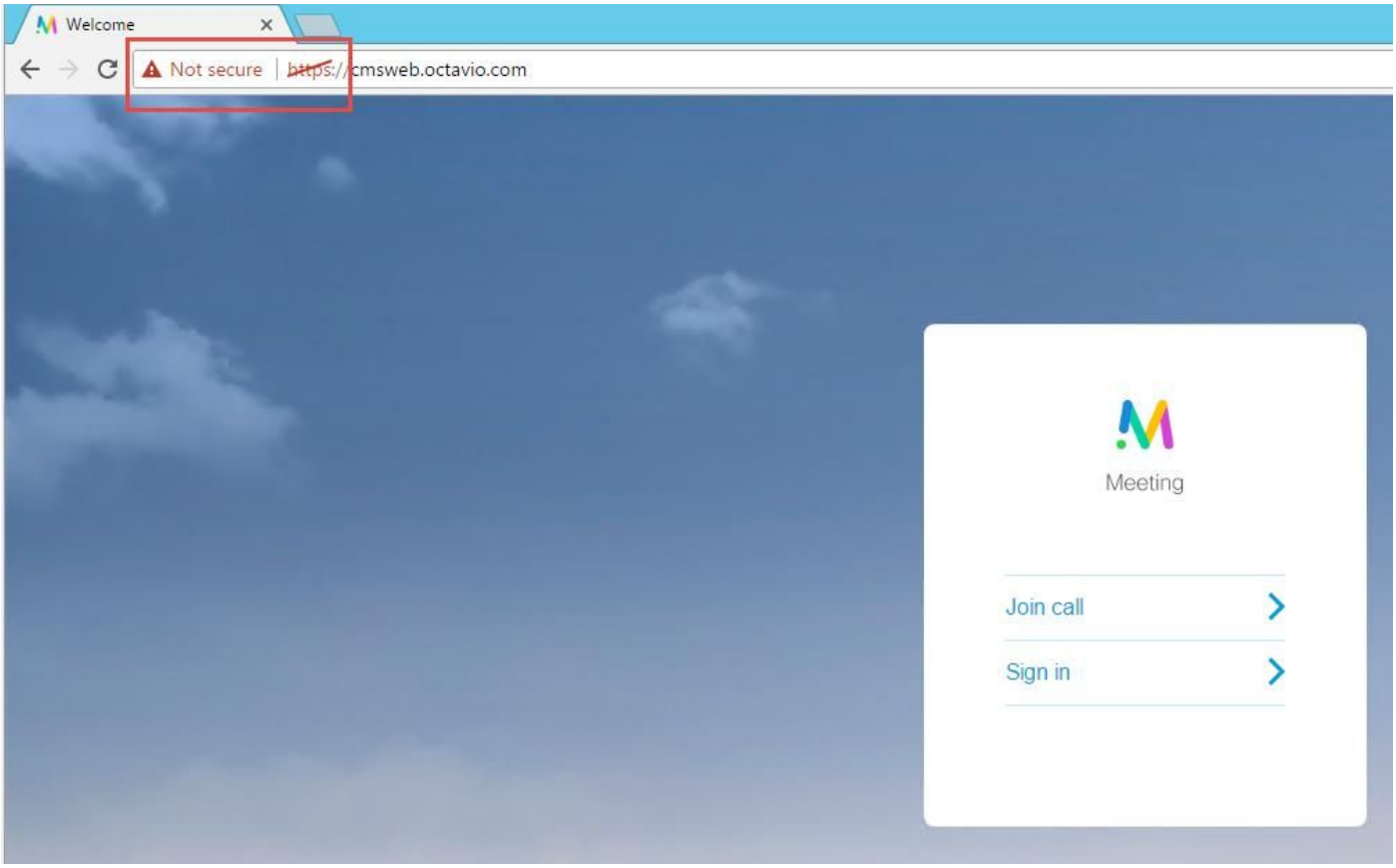
Solução

- Verifique se a URI do cliente de conta de convidado correta está configurada no Expressway-C. Navegue até **Configuration > Unified Communication > Cisco Meeting Server** para esse fim.

Se o URL interno estiver configurado no URL do cliente de conta de convidado, o Expressway-C o resolverá, pois há um registro criado no servidor DNS, mas isso pode causar a mensagem de erro "solicitação inválida" no navegador da Web. Neste caso de exemplo, o URL interno é configurado para mostrar o erro como mostrado na imagem.

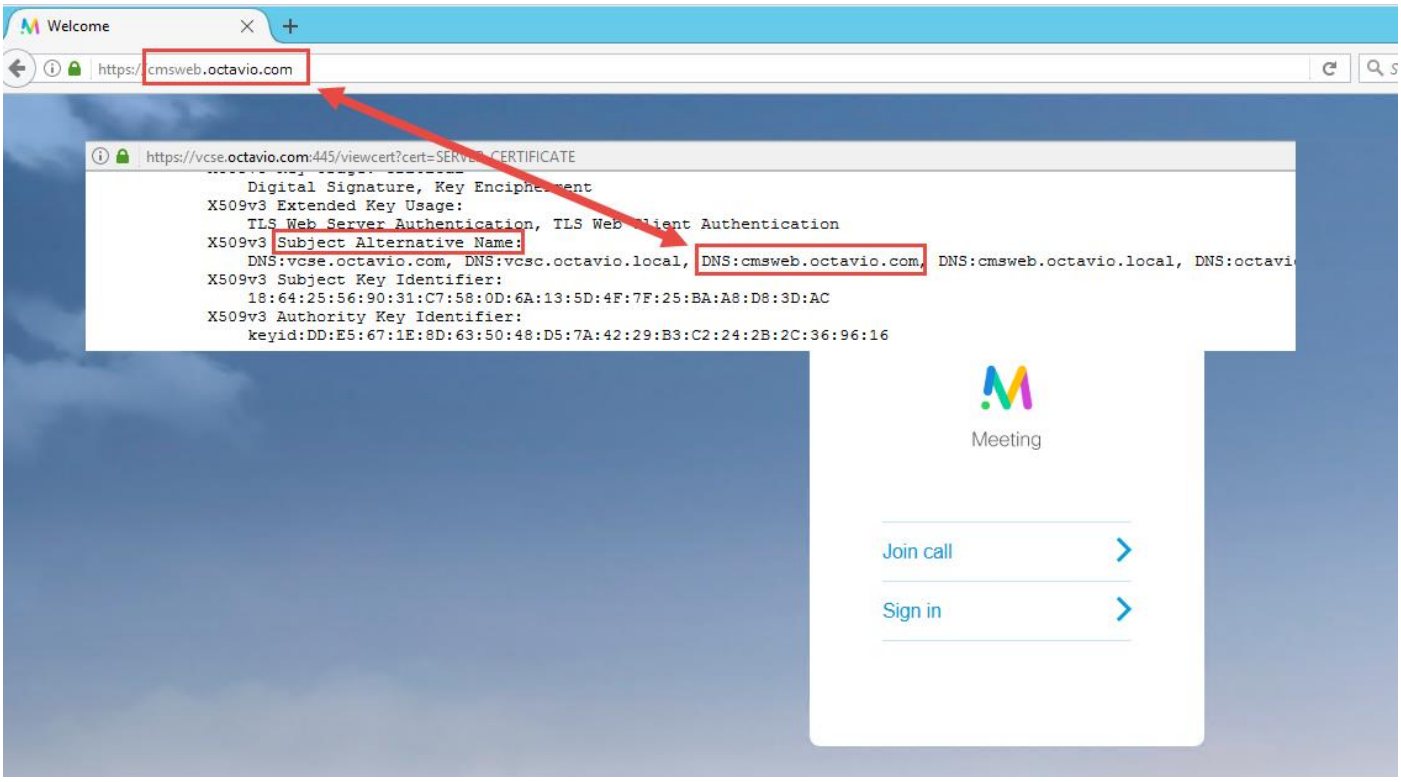


Cliente WebRTC mostra conexão não segura

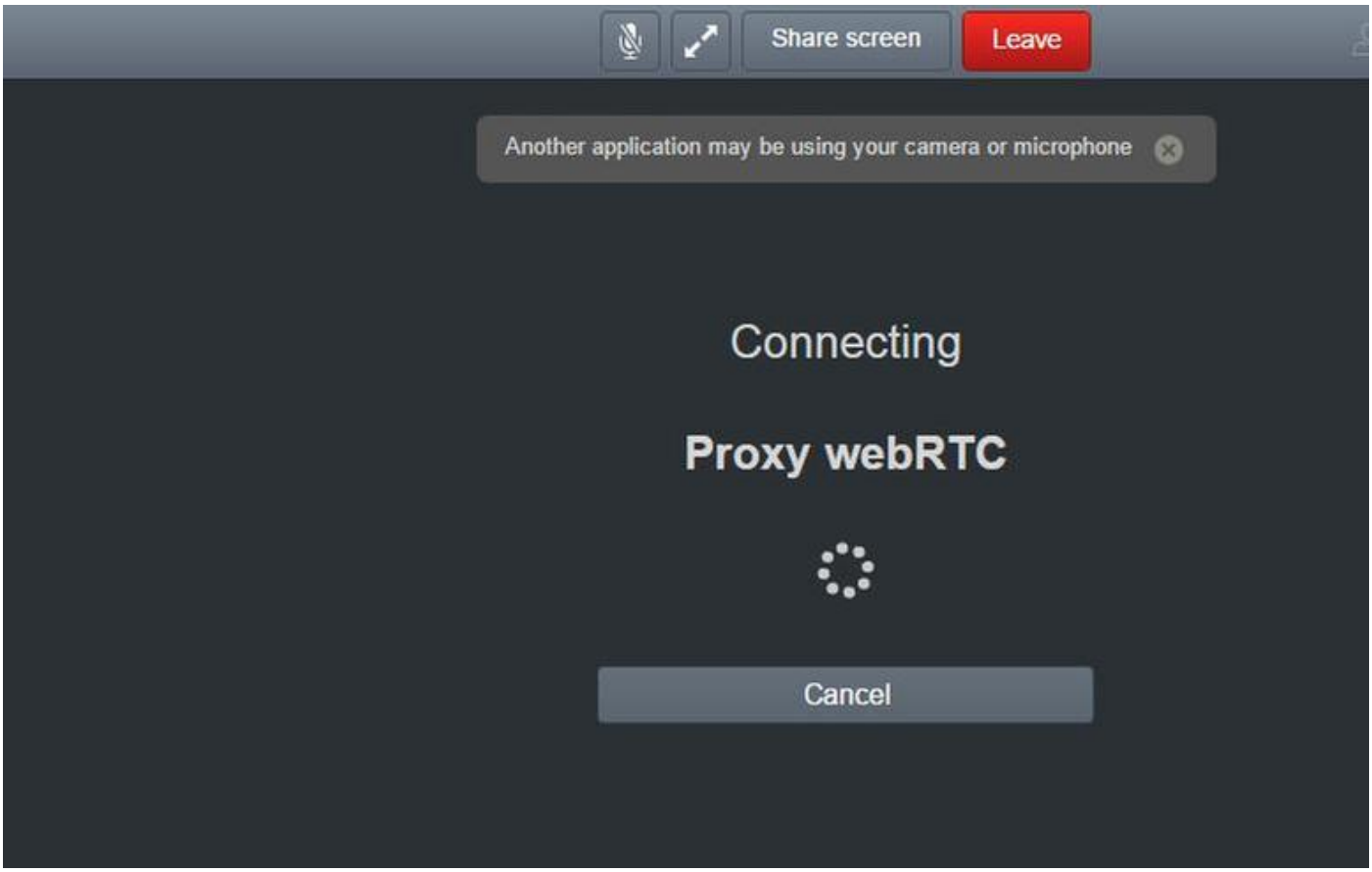


Solução

- O certificado é autoassinado, o que faz com que o servidor não confie na origem. Altere o certificado no Expressway-E para uma autoridade de certificado de terceiros suportada.
- Verifique se o URL externo da webbridge é adicionado como uma SAN no certificado do servidor Expressway-E como mostrado na imagem.



O cliente WebRTC se conecta, mas nunca se conecta e, em seguida, o tempo limite é excedido e desconecta



O nome de usuário ou a senha do servidor TURN estão configurados incorretamente no expressway-E ou no CMS via API. Os registros contêm os erros mostrados na imagem.

2017-05-20	19:43:14.133	Info	web bridge link 3: new guest login request 21 received
2017-05-20	19:43:14.133	Info	guest login request 21: passcode resolution scheduled
2017-05-20	19:43:14.133	Info	guest login request 21: resolution in progress
2017-05-20	19:43:14.135	Info	guest login request 21: credential storage scheduled (queue length: 1)
2017-05-20	19:43:14.135	Info	created guest account with user ID "guest3804072848@cms.octavio.local"
2017-05-20	19:43:14.135	Info	guest login request 21: credential storage executed
2017-05-20	19:43:14.135	Info	guest login request 21: credential storage in progress
2017-05-20	19:43:14.137	Info	guest login request 21: successfully stored credentials
2017-05-20	19:43:14.163	Info	web bridge link 3: guest login request 21: response written
2017-05-20	19:43:14.231	Info	successful login request from guest3804072848@cms.octavio.local
2017-05-20	19:43:14.930	Info	instantiating user "guest3804072848@cms.octavio.local"
2017-05-20	19:43:14.934	Info	new session created for user "guest3804072848@cms.octavio.local"
2017-05-20	19:43:18.805	Info	call 6: allocated for guest3804072848@cms.octavio.local "Web client" conference participation
2017-05-20	19:43:18.805	Info	call 6: setting up combined RTP session for DTLS (combined media and control)
2017-05-20	19:43:21.805	Warning	call 6: ICE failure; relay candidate creation timeout

O erro também pode ser confirmado com uma captura de pacote. Execute o Wireshark no PC onde o cliente WebRTC é executado. Depois de ter a captura de pacotes, filtre os pacotes pelo STUN. Você deve ver os erros mostrados na imagem.

O PC envia uma solicitação de alocação e o endereço NAT do Expressway responde com a mensagem 'Falha na verificação de integridade'.

Solução

Para corrigir o erro, revise o nome de usuário e a senha. Eles devem ser configurados corretamente nos parâmetros do servidor TURN conforme mostrado nas imagens.