

Configurez le proxy CMS WebRTC au-dessus d'Expressway

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configuration Steps](#)

[Étape 1. Intégrez le WB CMS sur Expressway-C](#)

[Étape 2. Activez activent Expressway-e et ajoutent le laisser-passer d'authentification à la base de données d'authentification locale](#)

[Étape 3. Changez le port de gestion d'Expressway-e \(facultatif\)](#)

[Étape 4. Ajoutez Expressway-e comme serveurs de TOUR pour le NAT Traversal de medias sur le serveur CMS](#)

[Vérifier](#)

[Étape 1. Sur Expressway-C, contrôle que le WB est correctement intégré](#)

[Étape 2. Vérifiez que le serveur de TOUR a été ajouté au serveur CMS](#)

[Étape 3. Vérifiez l'utilisation de relais de TOUR pendant l'appel actuel](#)

[Dépanner](#)

[Le client externe de WebRTC ne se connecte mais aucun support \(devant GLACER la panne\)](#)

[Le client externe de WebRTC n'obtient pas joignent l'option d'achat](#)

[Le client externe de WebRTC coincé \(sur des medias de chargement\) en se connectant au cospace et obtient alors réorienté à la page d'initiale WB](#)

[Le client externe de WebRTC incapable de joindre le cospace et obtient le d'avertissement \(incapable de se connecter - essayez de nouveau plus tard\)](#)

[Informations connexes](#)

Introduction

Ce document décrit les étapes pour configurer et dépanner Cisco rencontrant le serveur (CMS) WebRTC au-dessus d'Expressway.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Expressway X8.9.2 et plus tard

- Serveur 2.1.4 CMS et plus tard
- [Traduction d'adresses réseau \(NAT\)](#)
- Traversée utilisant des relais autour de NAT (TOUR)
- Utilitaires de traversée de session pour NAT (STUN)
- Système de noms de domaine (DNS)

Conditions préalables à la configuration :

- Le mobile de base et l'Accès à distance (MRA) ont associé des configurations (zone de traversée UC, tunnels de SSH) doivent être déjà activés et configurés sur Expressway, [ont cliquez ici](#) pour des guides MRA
- WebBridge (WB), Messagerie et présence Protocol (XMPP) et CallBridge extensibles configuré et activé sur le CMS, [ont cliquez ici](#) pour le guide de configuration
- TOURNEZ la touche option installée sur Expressway-e
- Le port TCP 443 s'est ouvert sur le Pare-feu de l'Internet public à l'adresse IP publique du l'Expressway-e
- Le port 3478 (demandes de TCP et UDP de TOUR) s'est ouvert sur le Pare-feu de l'Internet public à l'adresse IP publique du l'Expressway-e
- Le port 3478 (demandes de TCP et UDP de TOUR) s'est ouvert sur le Pare-feu du CMS à l'adresse IP privée du l'Expressway-e (si vous utilisez le Double-NIC sur Expressway-e)
- Enregistrements DNS externes pour le FQDN du WebBridge, résoluble à l'adresse IP du public-revêtement du l'Expressway-e
- FQDN WB interne d'enregistrement DNS résoluble à l'adresse IP du serveur CMS
- La réflexion NAT permise sur le pare-feu externe pour l'adresse IP publique du l'Expressway-e, [a cliquez ici](#) par exemple la configuration

Note: Des paires d'Expressway qui sont utilisées pour des services d'invité de Jabber ne peuvent pas être utilisées pour des services proxys CMS WebRTC.

[Composants utilisés](#)

Ce document n'est pas limité au logiciel et aux versions de matériel spécifiques, toutefois les exigences de version logicielle minimale doivent être répondues.

- Interface de programmation CMS (API)
- Facteur (api client)
- Expressway
- Serveur CMS

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

[Informations générales](#)

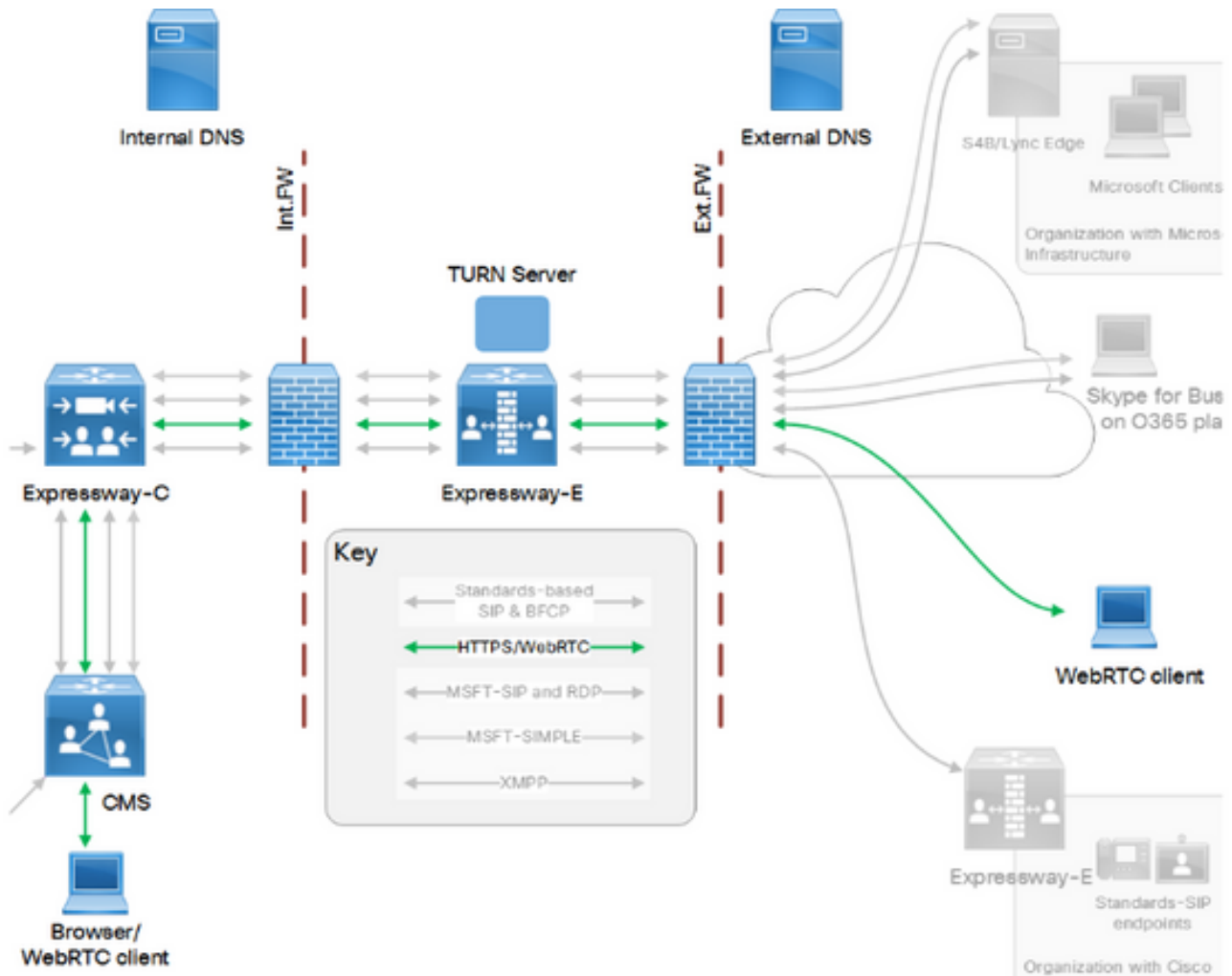
Le support de proxy de WebRTC a été ajouté à Expressway de la version X8.9.2, qui permet aux utilisateurs hors-lieu de parcourir à Cisco rencontrant la passerelle de Web de serveur.

Les clients externes et les invités peuvent gérer ou joindre les espaces sans besoin de n'importe

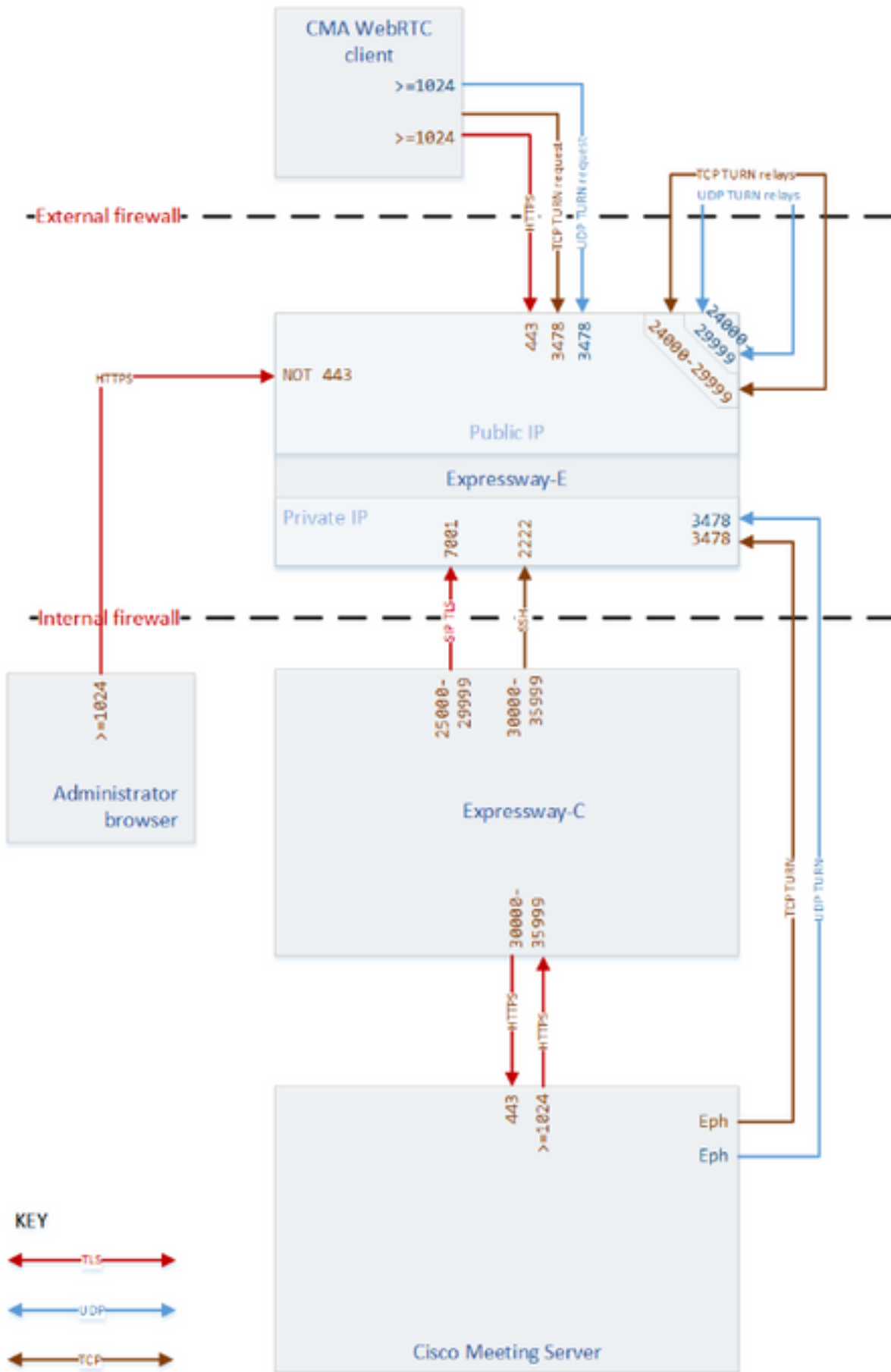
quel logiciel autre qu'un navigateur pris en charge. [A cliquez ici](#) pour une liste de navigateurs pris en charge.

Configurer

Diagramme du réseau



Cette image fournit un exemple des connexions circulant du proxy de Web pour CMS WebRTC :



Note: Vous devez configurer votre pare-feu externe pour permettre la réflexion NAT pour l'IP address public d'Expressway-e (les Pare-feu se méfient typiquement des paquets qui ont le même IP address de source et de destination).

Configuration Steps

Étape 1. Intégrez le WB CMS sur Expressway-C

- Navigation vers la **configuration > transmission unifiée > Cisco rencontrant le serveur**
- Proxy de Web de serveur de téléconférence d'enable**
- Écrivez le FQDN du WB dans le domaine d'**URI de client de compte d'invité**
- Cliquez sur en fonction la **sauvegarde**
- Ajoutez le FQDN du WB sur le certificat de serveur d'Expressway-e comme nom alternatif soumis (SAN), [avez cliquez ici](#) pour le guide de certificat d'Expressway.

Note: L'**URI de client de compte d'invité** doit être comme configuré sur le serveur WebAdmin (interface gui CMS de Web) sans préfixe de **https://**.

The screenshot shows the Cisco Meeting Server configuration interface. At the top, there are navigation tabs: Status, System, Configuration, Applications, Users, and Maintenance. Below these is the title 'Cisco Meeting Server'. The main configuration area is titled 'Meeting Server configuration'. Underneath, there is a section for 'Meeting Server Web Proxy' with a dropdown menu set to 'Enable' and an information icon. Below that, the 'Guest account client URI' field is highlighted with a red border and contains the text 'webbridge.alero.aca' with an asterisk and an information icon. At the bottom left, there is a 'Save' button.

Étape 2. Activez activent Expressway-e et ajoutent le laisser-passer d'authentification à la base de données d'authentification locale

- Navigation vers la **configuration > la traversée > le TOUR**
- Activez les services de TOUR, d'hors fonction à en fonction
- Choisi **configurez les qualifications de client de TOUR sur la base de données locale** et ajoutez les qualifications (le nom d'utilisateur et mot de passe)

Note: Si vous avez une batterie d'Expressway-e et ils sont tous à utiliser comme serveurs de TOUR, alors assurez pour l'activer sur tous les Noeuds.

Étape 3. Changez le port de gestion d'Expressway-e (facultatif)

- Navigation vers le **système > la gestion**
- Sous la **configuration de serveur Web**, changez le **port d'administrateur Web à 445 des options**

de déroulant, puis sélectionnez la **sauvegarde**

c. Répétez les étapes **3a à 3b** sur tout l'Expressway-e utilisé pour des services proxys de WebRTC

Note: Cisco recommande la gestion que le port soit changé parce que l'utilisation 443 de clients de WebRTC. Si les essais de navigateur de WebRTC au port d'accès 80, Expressway-e réoriente la connexion à 443.

Étape 4. Ajoutez Expressway-e comme serveurs de TOUR pour le NAT Traversal de medias sur le serveur CMS

a. Téléchargez et installez le facteur [d'ici](#).

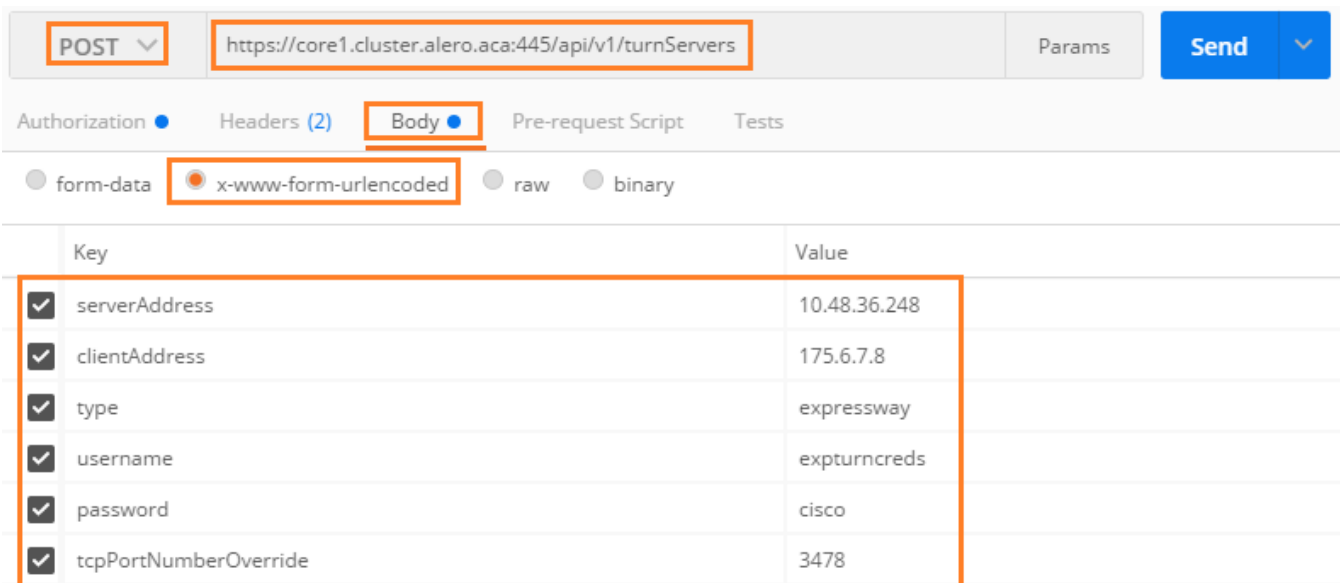
b. Écrivez l'URL d'accès API dans la barre d'adresses, par exemple ; **https://<Callbridge_fqdn>:445/api/v1/<entity>**

c. Envoyez un POST avec https://<Callbridge_fqdn>:445/api/v1/turnservers, après que vous ajoutiez ces champs dans le corps :

- **serverAddress** : (Adresse IP privée d'Expressway)
- **clientAddress** : (Adresse IP publique d'Expressway)
- **type** : (autoroute)
- **nom d'utilisateur** : (comme configuré dans étape 2c)
- **mot de passe** : (comme configuré dans étape 2c)
- **tcpPortNumberOverride** : 3478

d. Répétez l'étape **4c** pour que chaque serveur d'Expressway-e soit utilisé pour le TOUR

Ces images fournissent des exemples des étapes basées sur la configuration :



Key	Value
<input checked="" type="checkbox"/> serverAddress	10.48.36.248
<input checked="" type="checkbox"/> clientAddress	175.6.7.8
<input checked="" type="checkbox"/> type	expressway
<input checked="" type="checkbox"/> username	expturncreds
<input checked="" type="checkbox"/> password	cisco
<input checked="" type="checkbox"/> tcpPortNumberOverride	3478

POST Params

Authorization Headers (2) **Body** Pre-request Script Tests

form-data x-www-form-urlencoded raw binary

Key	Value
<input checked="" type="checkbox"/> serverAddress	10.48.79.129
<input checked="" type="checkbox"/> clientAddress	175.6.7.9
<input checked="" type="checkbox"/> type	expressway
<input checked="" type="checkbox"/> username	expturncreds
<input checked="" type="checkbox"/> password	cisco
<input checked="" type="checkbox"/> tcpPortNumberOverride	3478

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Étape 1. Sur Expressway-C, contrôlez que le WB est correctement intégré

a. Naviguez vers la **configuration > transmission unifiée > Cisco rencontrant le serveur**, et vous devez voir l'adresse IP du WB :

Status **System** Configuration Applications Users Maintenance

Cisco Meeting Server You are here: [C](#)

Meeting Server configuration

Meeting Server Web Proxy ⓘ

Guest account client URI ⓘ

Guest account client URI resolved to the following targets

Name	Address
webbridge.alero.aca	10.48.36.5

b. Naviguez vers la **configuration > transmission unifiée > HTTP permettent la liste > automatiquement ajouté des règles**, contrôlez que ceci a été ajouté aux règles :

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

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

Note: On ne s'attend pas à ce qu'il trouve le WB dans les Noeuds découverts parce que les règles sont simplement de tenir compte du proxy du trafic HTTPS au WB, et pas nécessairement pour la transmission unifiée.

c. Vérifiez que le tunnel de Protocole Secure Shell (SSH) pour le FQDN WB a été construit sur Expressway-C à Expressway-e et qu'il est en activité. Naviguez vers l'état > des transmissions unifiées > état unifié de tunnels de SSH de transmissions, vous devez voir que le FQDN du WB et de la cible doit être Expressway-e :

Target	Domain	Status	Peer
vcs-e.alero.local	webbridge.alero.aca	Active	10.48.36.247
vcs-e.alero.local	alero.lab	Active	10.48.36.247
vcs-e.alero.local	alero.local	Active	10.48.36.247
vcs-e2.alero.local	alero.lab	Active	10.48.36.247
vcs-e2.alero.local	webbridge.alero.aca	Active	10.48.36.247
vcs-e2.alero.local	alero.local	Active	10.48.36.247

Étape 2. Vérifiez que le serveur de TOUR a été ajouté au serveur CMS

a. Sur le WebUI, si vous utilisez un serveur simple d'Expressway, naviguez vers des logs > des journaux d'événements, la sortie affiche l'adresse IP du serveur de TOUR, comme dans l'exemple :

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

b. Si vous utilisez de plusieurs serveurs de TOUR d'Expressway, envoyez une demande GET avec un api client avec cette commande :

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

Note: Cette commande peut également être utilisée si vous avez un serveur simple de TOUR d'Expressway.

La sortie, dans le cas de plusieurs serveurs de TOUR d'Expressway, est semblable à celle dans cet exemple :

```
<?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. Pour vérifier l'état de chaque serveur de TOUR faites ce qui suit :

- Copiez l'id de turnServer de l'étape 2b
- Envoyez une demande GET avec l'api client avec cette commande :

```
https://<Callbridge_IP>:445/api/v1/turnservers/<turnServer id>/status
```

L'affiche des informations de sortie qui inclut le Round-Trip Time (DURÉE DE TRANSMISSION)

en quelques millisecondes (ms) a associé le serveur de TOUR. Il est importante pour la sélection de CB du meilleur serveur de TOUR l'utiliser ces informations.

La sortie ci-dessous affiche l'état pour le serveur de TOUR avec l'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>
```

La sortie ci-dessous affiche l'état pour le serveur de TOUR avec l'ID **eef94a2b-3bfa-40f7-b83c-ecce8df424e15** :

```
<?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>
```

Étape 3. Vérifiez l'utilisation de relais de TOUR pendant l'appel actuel

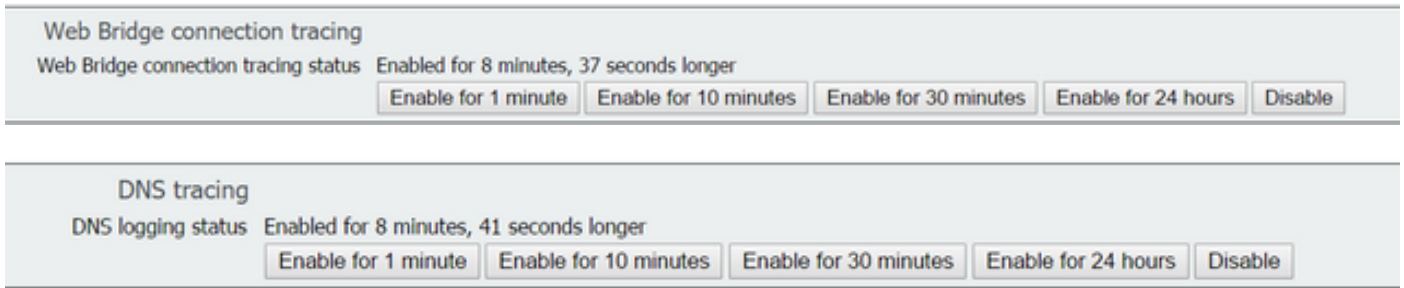
Au moment d'un appel vivant qui est fait avec l'utilisation du client de WebRTC, vous pouvez visualiser l'état de relais de medias de TOUR sur Expressway. Naviguez vers **l'utilisation de relais d'état > de TOUR**, puis sélectionnez la **vue**.

Dépanner

Cette section fournit les informations que vous pouvez employer pour dépanner votre configuration, quelques questions typiques de WebRTC et pannes possibles.

Des logs pour les connexions WB et la découverte de DN peuvent être activés sur le WebAdmin du serveur CMS :

- a. Connectez au **WebAdmin**
- b. Naviguez vers des **logs > a détaillé le suivi**
- c. Activez le **suivi** et les **DN de montage en pont de Web traçant** pour la durée désirée :



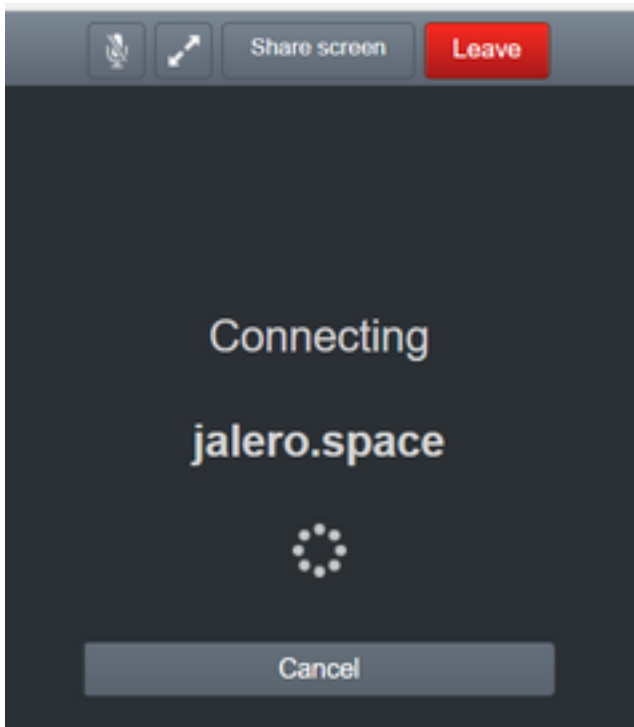
Le debug logging de console de Chrome et de Firefox peut être utilisé pour dépanner des pannes de connexion client de WebRTC, telles que des questions avec des medias et la Connectivité au WB. Ceci peut être rendu visible avec l'utilisation de la combinaison **Ctrl+Shift+C** de clavier.

Sur Chrome, utilisation **chrome://webrtc-internals/** ou environ : **webrtc** sur Firefox, sur un onglet distinct au moment d'un appel vivant pour afficher les diagnostics avancés, qui est utile pour dépanner des questions de medias avec WebRTC.

La capture de paquet de Whireshark sur le client de WebRTC fournissent également à quelques informations utiles au sujet du relais de medias le serveur de TOUR.

Le client externe de WebRTC ne se connecte mais aucun support (devant GLACER la panne)

Dans ce scénario, le client RTC peut résoudre l'ID d'appel à **jalero.space**, mais quand vous entrez dans votre nom et Joincall choisi, **le client affiche se connecter, comme** affiché sur l'image ci-dessous :



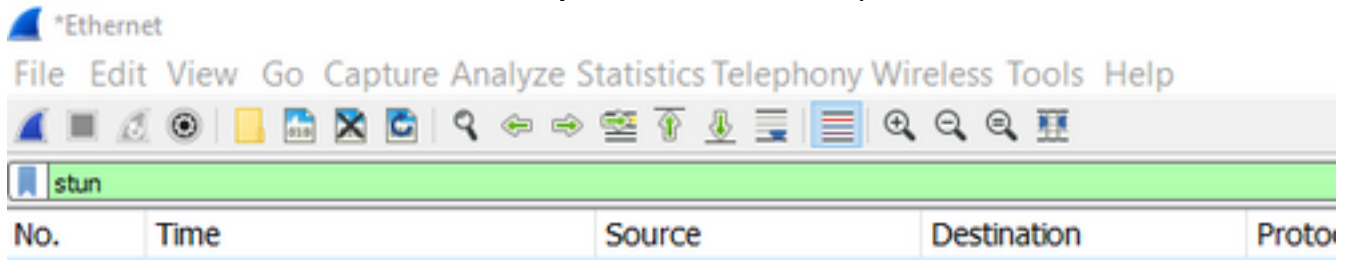
Après environ 30 secondes, il est réorienté à la page WB d'initiale.

Pour dépanner, faites ce qui suit :

- Commencez le wireshark sur le client RTC quand vous tentez un appel et quand la panne se produisent, arrêtent la capture
- Après que la question se produise, vérifiez les journaux d'événements CMS

Naviguez vers des logs > l'événement ouvre une session le CMS WebAdmin

- Filtrez les suivis de Wireshark avec **stupéfiant**, voient l'exemple ci-dessous :



Dans les suivis de Wireshark, vous voyez que le client envoie **allouent la demande** avec les qualifications configurées, au serveur de TOUR d'Expressway-e sur le port **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
```

Le serveur répond avec **allouent l'erreur** :

```
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
```

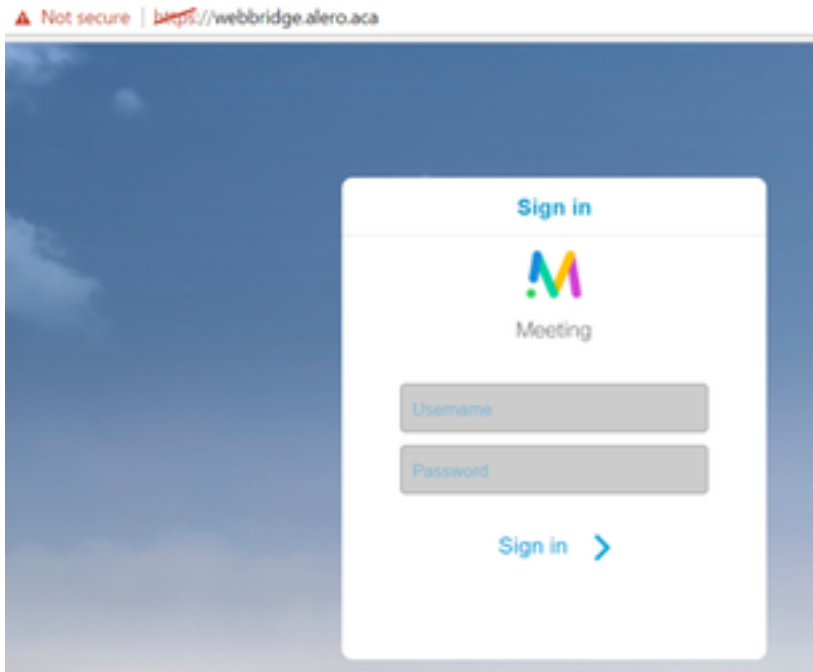
Dans les logs CMS, le message de log ci-dessous est affiché :

```
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
```

Solution :

Vérifiez les qualifications de TOUR configurées sur le CMS et assurez-vous qu'il apparie cela qui est configuré sur la base de données d'authentification locale d'Expressway-e.

Le client externe de WebRTC n'obtient pas joignent l'option d'achat



Sur l'état de Callbridge > la page générale, ceci est affichée :

```
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
```

Solution :

- Assurez-vous que le Callbridge peut résoudre le FQDN WB à l'adresse IP interne (le Callbridge ne doit pas résoudre ceci à l'adresse IP du l'Expressway-e)
- Videz le cache DNS sur le Callbridge, par l'intermédiaire de l'interface de ligne de commande (CLI), avec l'annulation de dn de commande
- Assurez-vous que le WB fait confiance au certificat de serveur de Callbridge (pas l'émetteur)

Le client externe de WebRTC coincé (sur des medias de chargement) en se connectant au cospace et obtient alors réorienté à la page d'initiale WB

Solution :

- Assurez-vous que le CMS peut résoudre l'enregistrement SRV **_xmpp-client** sur le réseau interne pour le domaine de CB
 - Collectez la capture Wireshark sur le client et le **diagnostic se connectant** comprenant le **tcpdump** sur Expressway-e tout en tentant de se connecter au client externe
- Naviguez vers la **maintenance > les diagnostics > le diagnostic se connectant** et assurez-vous que **tcpdump de prise tout en se connectant** est vérifié comme affiché sur l'image ci-dessous, avant que vous sélectionniez le **nouveau log de début** :

Diagnostic logging You are here: [Maintenance](#)

Logging status

Started logging at: Tuesday 31st of October 2017 02:01:01 PM (CET) logging started by admin@10.61.76.201

Stopped logging at: Tuesday 31st of October 2017 02:01:10 PM (CET)

Marker: ⓘ

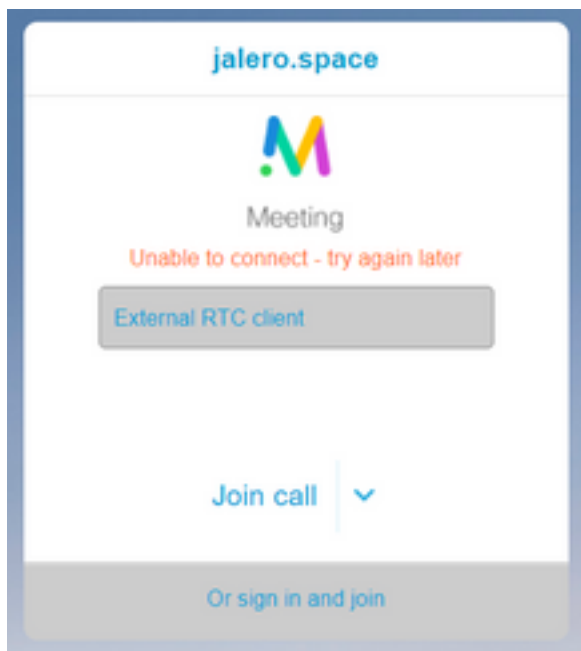
Take tcpdump while logging: ⓘ

Note: Assurez-vous que la capture Wireshark sur le périphérique du client et ouvrir une session Expressway-e sont commencés avant de reproduire l'appel manquant. Quand l'appel manquant a été reproduit, arrêtez et téléchargez ouvrir une session Expressway-e et la capture sur le client.

- Extrayez/défaites la fermeture éclair du paquet de log dowloaded d'Expressway-e et ouvrez le fichier **.pcap** pris sur l'interface de Public-revêtement
- Le filtre sur les deux captures de paquet avec **stupéfiant** Recherchez alors la demande obligatoire du client externe à l'adresse IP publique d'Expressway-e, **cliquent avec le bouton droit** et choisi **suivez > flot d'UDP**Habituellement la destination port de la **demande obligatoire du client** serait de l'ordre de **24000-29999**, qui est les **relais de TOUR met en communication la plage** sur Expressway-e
- Si aucune réponse aux **demandes obligatoires** n'est reçue du côté du client, contrôle sur la capture du l'Expressway-e si les demandes arrivent
- Si les demandes arrivent et Expressway-e répond au client, vérifiez si le FW externe permet le trafic UDP sortant
- Si les demandes n'arrivent pas, vérifiez le FW pour s'assurer que la plage de port ci-dessus ne sont pas bloquées
- Si Expressway-e est déployé avec un double contrôleur d'interface réseau (DUAL-NIC) avec le mode NAT statique activé, alors assurez-vous que la réflexion NAT est prise en charge et configurée sur votre FW externe

Le client externe de WebRTC incapable de joindre le cospace et obtient le d'avertissement (incapable de se connecter - essayez de nouveau plus tard)

Dans ce scénario, le client RTC peut résoudre l'ID d'appel à **jalero.space**, **mais** quand vous entrez dans votre nom et Joincall choisi, l'Unableto d'avertissement **se connectent - l'essai de nouveau plus tard** est affiché immédiatement :



Solution :

Vérifiez que le CMS, sur le réseau interne, peut résoudre toujours l'enregistrement SRV `_xmpp-client` pour le domaine de CB.

[Informations connexes](#)

- [Guide d'utilisation de port IP VCS/Expressway](#)
- [Support et documentation techniques - Cisco Systems](#)