Cisco Expressway Web Proxy for Cisco Meeting Server

Deployment Guide

First Published: December 2016

Last Updated: February 2020

Expressway X8.10

Preface

Change History

Table 1 Deployment Guide Change History

Date	Change	Reason
February 2020	Clarify *Web Proxy for Meeting Server Configuration Summary* section to include requirement for another forward lookup zone (if no split DNS).	Documentation defect
November 2018	Removed a misleading note about WebRTC client behavior.	Documentation defect
May 2018	Updated the limitation on usage of port 8443 for web administration. Clarify to use private address of the internal NIC if two NICs are used on the Expressway-E.	Documentation defect
December 2017	Refinements to media flows and DNS records topics	Information improvement
November 2017	New document dedicated to Web Proxy for Cisco Meeting Server	Information improved for X8.10
December 2016	First release of information, in shared document *Cisco Expressway Options with Cisco Meeting Server and/or Microsoft Infrastructure*	New feature in X8.9

Related Documents

- For installing Expressway:
  - *Cisco Expressway Virtual Machine Installation Guide* on the Expressway installation guides page.
  - *Cisco VCS Virtual Machine Installation Guide* on the VCS installation guides page.
  - *Cisco Expressway CE1100 Appliance Installation Guide* on the Expressway installation guides page.
  - *Cisco Video Communication Server CE1100 Appliance Installation Guide* on the VCS installation guides page.
- Cisco Meeting Server installation guides page
- Cisco Meeting Server configuration guides page
- *Expressway Administrator Guide*

  VCS Administrator Guide
- For certificates on Expressway:

  See *Cisco Expressway Certificate Creation and Use Deployment Guide* on the Expressway configuration guides page.

  See *Cisco VCS Certificate Creation and Use Deployment Guide* on the VCS configuration guides page.
- For clustering Expressway:

  See the *Cisco Expressway Cluster Creation and Maintenance Deployment Guide*, for your version, on the Cisco Expressway Series configuration guides page.
- For firewall configuration:

  See the *Cisco Expressway IP Port Usage Configuration Guide*, for your version, on the Cisco Expressway Series configuration guides page.

Contents

Introduction

This Expressway guide also now applies to VCS. Any VCS-specific information is noted where necessary in the guide. (Older VCS guides on Cisco.com are still valid for the VCS versions they apply to—as specified on the title page of each guide.)

The Meeting Server Web Proxy enables external users to join or administer Meeting Server spaces using their browser. All the external user needs is the URL to the space and their credentials for accessing the Meeting Server.

Scope and Purpose

This document describes how to use Cisco Expressway Series as a Web Proxy for Cisco Meeting Server. This reverse proxy enables Cisco Meeting WebRTC Apps to join Cisco Meeting Server spaces, via the web bridge.

Expressway cannot currently traverse calls from other variants of Cisco Meeting App when they are outside the network. This functionality can be provided by using the Meeting Server Load Balancer and TURN server components.

See *Deploying the Trunk and the Load Balancer* and *Configuring TURN Servers* in the Meeting Server deployment guides, on the Cisco Meeting Server configuration guides page.

Terminology and Example Values

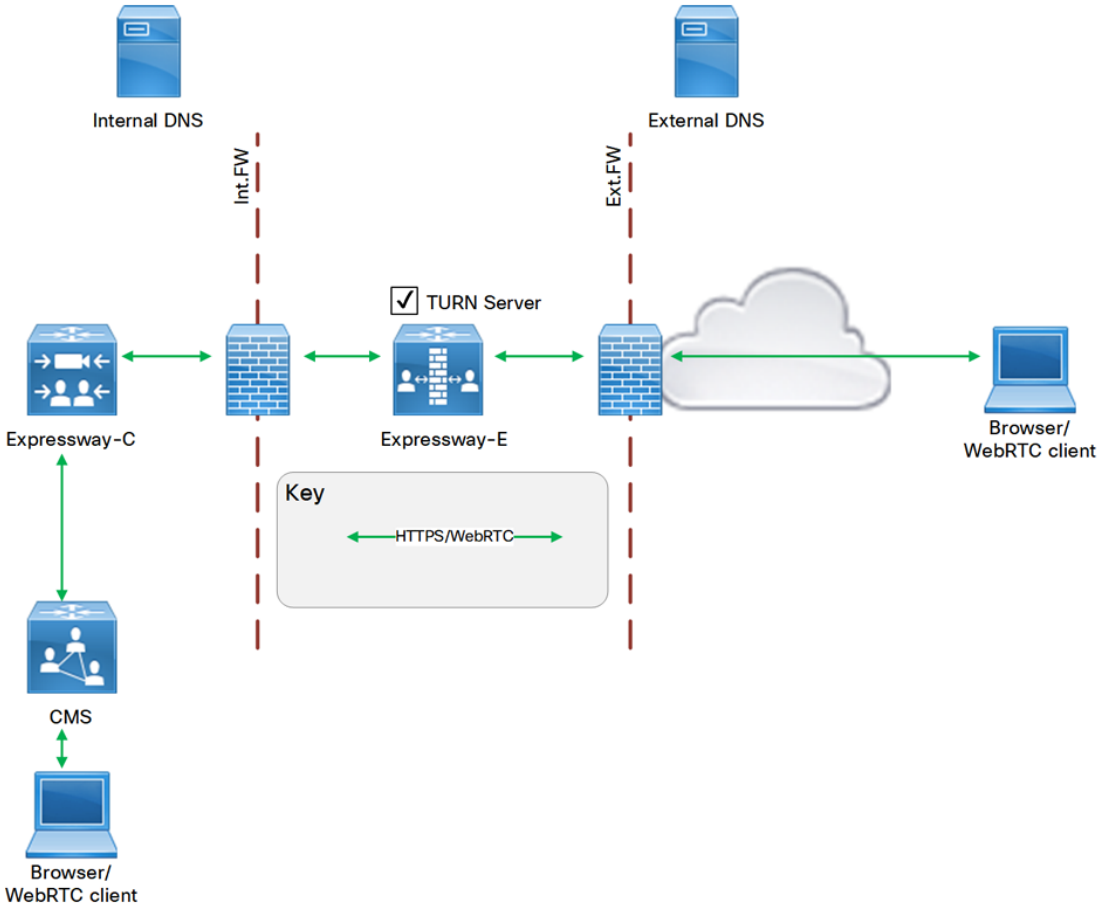
Note: Do not use the domain names and other example values from this document in your test or production deployments. You must change the example values to represent your own environment.

- *Web Proxy for Meeting Server*: A reverse https proxy on the Expressway traversal pair used only for a specified address.
- *Guest account client URI*: A name that you enter on the Expressway-C to represent the Web Bridge listening interfaces on the Cisco Meeting Server. It corresponds to the **Guest account client URI** on the Meeting Server web bridge settings. We use the example value *join.ciscoexample.com*.
- *Outbound* and *Inbound*: Generally, calls initiated from inside your organization's network to another organization or remote user are Outbound. Calls initiated from outside your organization's network, to users or spaces in your network, are Inbound.

  We also use these terms in the specific context of particular systems. In these cases, you can infer the call direction from the text and supporting diagrams.
- Cisco Meeting App has the following variants:
  - *Cisco Meeting WebRTC App*: A thin client that runs in a browser to connect to spaces. Also called "web app", "thin client", "web client", "WebRTC app".
  - *Cisco Meeting App (Windows)*: A thick client that runs on Microsoft Windows (out of scope for this document).
  - *Cisco Meeting App (iOS)*: A thick client that runs on Apple iOS (out of scope for this document).
  - *Cisco Meeting App (OS X)*: A thick client that runs on Apple OS X (out of scope for this document).

Configure Meeting Server Web Proxy

Deployment Map



Note: See separate diagrams showing Web Proxy for Meeting Server Media Flows, page 15 later in this document.

Technical Overview of Web Proxy for Meeting Server

The Web Proxy allows traffic from the internet destined for Meeting Server web bridges. Typically this is to allow guest access to spaces on the Meeting Server, but can also be used for administering your spaces.

To allow Cisco Meeting WebRTC Apps to call into Meeting Server spaces from outside your network, you need to enable the Web Proxy. This is currently controlled by the *Mobile and Remote Access* mode on the Expressway-C and the Expressway-E, but you do not need to completely configure MRA.

Signaling and media

The call control between the app and the Meeting Server is not SIP, so you do not need to create any SIP domains on the Expressway-C. You can ignore the warning on **Status > Unified Communications** that states "*There are no Unified Communications domains configured.*".

The solution needs TURN media relays, so you will need to configure Meeting Server with your TURN server details.

You can use the TURN server on Expressway-E, provided that you can listen externally on TCP and UDP 3478 and that your guests can connect to those ports on the Expressway-E's public IP address.

See Which TURN Server To Use?, page 11.

Co-existence

The Web Proxy for Meeting Server can co-exist on the Expressway with the following services:

- Mobile and Remote Access
- Business to Business AV Federation (including with Microsoft infrastructure, but not "Gateway Expressway")
- IM&P Federation with Microsoft chat clients (not "SIP Broker" federation)
- Registrar

The Web Proxy for Meeting Server **cannot** co-exist on the Expressway with the following services:

- Jabber Guest
- Microsoft interoperability service (as controlled by the Microsoft Interoperability key on Expressway; this means the "Gateway Expressway" deployment and/or the "SIP Broker" deployment)

Split DNS?

If you have split DNS in your environment, then we recommend using different A records for the web bridge internally and externally. Browsers outside your network will need to resolve the Expressway-E's public address when looking up the domain of the Guest account client URI eg. *join.ciscoexample.com* domain, but browsers inside your network should resolve the listening interface of the Meeting Server web bridge instead.

If you can't split the DNS, you'll need to configure your firewall to allow browsers inside the network to resolve and reach the public address of the Expressway-E.

See DNS Records, page 18

Server Certificates

The Expressway-E certificate must list the Guest account client URI as a SAN.

Limitations

- We do not currently support traversal of Cisco Meeting App (XMPP) calls across the Expressway pair to the Meeting Server.

  If Cisco Meeting WebRTC App users attempt to use unsupported browsers, they will be redirected to download the Cisco Meeting App, which will not work without installing the loadbalancer component on Cisco Meeting Server Edge. We recommend using the Cisco Meeting WebRTC App with a supported browser.

- Partial support for clustered Meeting Server web bridges: Load balancing is supported but redundancy is not.

  Expressway-C uses round-robin to distribute WebRTC App signaling traffic to multiple Meeting Servers, based on its DNS lookup of the **Guest account client URI**. However, the Expressway-C does not currently adapt if any of the returned web bridge addresses are unreachable.
- The Web Proxy listens to the internet on TCP port 443 on the Expressway-E. This port is not configurable and overlaps with the default web administration port.

  The same port can be used for both purposes, and we distinguish the traffic destined for Meeting Server, but we strongly recommend that you change your web administrator access port on the Expressway-E. This means that you can prevent access to the web interface from the internet, while still allowing guest access to spaces.

  TCP 443 is also a desirable listening port for TCP TURN requests originating from restricted networks. See Which TURN Server To Use?, page 11.
- Expressway cannot currently proxy to web bridges that have IPv6 addresses.

Prerequisites

Supporting Systems Configuration

- DNS. An internal DNS configured with forward and reverse lookups for Expressway-E, Expressway-C, and Cisco Meeting Server.
- External DNS. An external DNS configured with forward lookup for the Expressway-E cluster FQDN.

  Note: The Web Proxy for Meeting Server is affected if you cannot make different entries for internal DNS and external DNS. See DNS Records, page 18
- NTP. All servers must be internally synchronized to the same time source.

Software Versions

- Expressway X8.9.2 or later (X8.10 or later recommended)
- Cisco Meeting Server 2.1.2 or later
- Meeting Server web bridge 2.1.4 or later is the minimum target for Expressway's Web Proxy for Meeting Server

Core Systems Basic Configuration

- Install and basic configuration of Cisco Meeting Server
- Install and basic configuration of Expressway (traversal pair)
- Create and install certificates onto Expressway pair
- [Optional] Cluster the Expressway

See Related Documents, page 2, for links to these documents.

Web Proxy for Meeting Server Configuration Summary

1. Install and configure Meeting Server, Expressway-C, and Expressway-E.
2. Apply a server certificate to the Meeting Server.
3. Apply server certificates to the Expressway-C and Expressway-E.

   The **Guest account client URI**, eg. *join.ciscoexample.com*, must be one of the Expressway-E certificate's subject alternate names (SAN).
4. Create an external DNS A record for resolving the Guest account client URI to the Expressway-E's public IP address.

   For example, create the record `join.ciscoexample.com` to target the Expressway-E's public interface.

5. Depending on whether you can split your DNS, do one of the following:
   - **If you can split DNS**: Create an A record on the internal DNS to resolve the **Guest account client URI** to the Meeting Server Web Bridge private IP address.

     You can create multiple A records if you have multiple Web Bridges sharing one **Guest account client URI**. You could use an SRV record `_cms-web._tls.join.ciscoexample.com.` instead, if you want better control over load distribution.
   - **If you cannot split DNS**:

     Internal browsers will resolve the Expressway-E's public address when looking up the Guest account client URI. You may need to configure your firewall to allow these connections (outside the scope of this document).

     1. You must create another forward lookup zone for the Guest account client URI on the internal DNS utilized by Expressway-C.

        Example: if your join A record was `join.ciscoexample.com` this would be the forward lookup zone created on the DNS server.
     2. You must create a DNS SRV record for resolving the Guest account client URI to the FQDNs of the Meeting Server Web Bridges.
        Example: create the record `_cms-web._tls.join.ciscoexample.com.` to target the Meeting Server FQDN, eg. `cms[1|2|3].ciscoexample.com` on port 443.
     3. Also create DNS A records to resolve the Meeting Server FQDNs, eg. `cms[1|2|3].ciscoexample.com` to the Meeting Server Web Bridge private IP addresses.

     See DNS Records, page 18.
6. Create Unified Communications traversal zones on Expressway-C and Expressway-E. (**Configuration > Zones > Zones**)

   You can reuse the existing Unified Communications zones if you already have MRA .
7. Enable the TURN server on either:
   - Expressway-E (**Configuration > Traversal > TURN**)

     In this case, point the Meeting Server to the Expressway-E TURN server. (on Meeting Server, go to **Configuration > General**). See Configure Meeting Server to Use Expressway-E for TURN Services, page 13
   - Meeting Server Edge Server, if you already have this installed.

     See the deployment guides on the Cisco Meeting Server configuration guides page to configure the TURN server on Cisco Meeting Server Edge.

     See Which TURN Server To Use?, page 11.
8. Change the Meeting Server listening port for administration UI to something other than 443.

   Use the MMP command `webadmin listen`. See the *Cisco Meeting Server MMP Command Line Reference* for details.
9. Enable XMPP call bridge on Meeting Server.
10. Enable web bridge on Meeting Server and enter **Guest account client URI**, **Guest account JID domain**, and **Web Bridge URI**.

    The **Guest account client URI** must match the **Web Bridge URI** and the Expressway-E SAN.
11. Enable MRA mode on the Expressway-C. (**Configuration > Unified Communications > Configuration**)

12. Expressway-C: Enable the **Meeting Server Web Proxy** and enter the **Guest account client URI**. (**Configuration > Unified Communications > Cisco Meeting Server**)

    This corresponds with the **Guest account client URI** on the Meeting Server web bridge settings.

    Note: If you change the DNS entries for the guest account client URI, you must click **Refresh** on this page. To change the URI, edit the address field and click **Save**.

    See Configure Meeting Server Web Proxy on Expressway-C, page 14
13. Enable MRA mode on the Expressway-E. (**Configuration > Unified Communications > Configuration**).
14. Change the web administration listening port on the Expressway-E. (**System > Administration**). This requires a restart.

    [Strongly recommended] Create a firewall rule to block access to the new administration port on the Expressway-E public interface.

    Note: The UI limits your port choices and you may wish to use a different port. If so, you can use the CLI command `xConfiguration Management Interface Port: nnnn` to set the port to your chosen value. If your Meeting Server and Expressway deployment is co-existing with MRA, you must not use port 8443 for web administration. Also, you need to be careful not to choose a port that is already in use, because there is no check when you run the CLI command.

    When you need to administer the Expressway-E (from inside the network), you should append the new port number to the address in the browser. If you changed the port to 7443 for example, then *https://expe.ciscoexample.com:7443* takes you to the Expressway-E login page, but *https://expe.ciscoexample.com* is refused.

URL for Cisco Meeting Server Web Proxy and MRA Domain Must be Different

If you use both the Cisco Meeting Server Web Proxy service and MRA on the same Expressway, the following configuration items must be assigned different values per service.

Note: If you try to use the same value, the service that was configured first will work, but the other one will fail:

- MRA domain(s): The domain(s) configured on Expressway and enabled for Unified CM registration.
- Cisco Meeting Server Web Proxy URL link: Defined in the Expressway "**Guest account client URI**" setting on the **Expressway > Configuration > Unified Communications > Cisco Meeting Server page**.

Create Unified Communications Zones

Note: You must reuse the existing Unified Communications zones if your Expressway pair is already configured for MRA (skip this step).

1. On each system in the Expressway pair, go to **Configuration > Zones > Zones**.
2. Click **New**.

3. Configure the following fields (leave all other fields with their default values):

Field Name	Expressway-C	Expressway-E
Name	`WebProxyTraversalClient` for example	`WebProxyTraversalServer` for example
Type	*Unified Communications*	*Unified Communications*
Connection credentials section		
Username	`exampleauth` for example	Match the credential entered on Expressway-C. Such as `exampleauth`
Password	`ex4mpl3.c0m` for example	a. Click **Add/Edit local authentication database** b. In the dialog box, click **New** and enter the **Name** and **Password** values. Using our examples, these would be `exampleauth` and `ex4mpl3.c0m`. c. Click **Create credential**.
H.323 section		
Mode	*Off*	*Off*
SIP section		
Port	7001	7001
TLS verify subject name	Not applicable	Enter the name to look for in the traversal client's certificate. This must be in either the Subject Common Name or the Subject Alternative Name attributes. If you have a cluster of traversal clients (Expressway-Cs), specify the cluster name here and ensure that it's included in each client certificate.
Authentication section		
Authentication policy	*Do not check credentials*	*Do not check credentials*
Location section		
Peer 1 address	Enter the FQDN of the Expressway-E.	Not applicable
Peer 2…6 address	(Clustered Expressway-Es only.) Enter the FQDNs of each additional peer.	Not applicable

4. Click **Create zone**.

Which TURN Server To Use?

With the infrastructure scenario in this document, it is possible that two different TURN servers could be available:

- Expressway-E TURN server
- Meeting Server Edge TURN server

Recommendations

If you are using Cisco Meeting App ("thick client") outside of the network: The Cisco Expressway pair cannot proxy the XMPP signaling for this client so you must use the Meeting Server Edge. In this case, because you already have the Edge server, we recommend that you use its TURN server for the WebRTC App media. You will not be affected by the lack of fallback to TCP 443 described in "Limitations" below.

If you do not have a Cisco Meeting Server Edge: You can use the Expressway-E TURN server for the WebRTC App media. This is subject to some limitations in X8.10, but we are working to address those limitations, to make this the preferred deployment.

Expressway-E TURN server (recommended for this deployment)

- The Expressway-E has an embedded TURN server which listens on a configurable port which defaults to 3478. It listens for both TCP and UDP TURN requests on this port.
- The configurable TURN listening port can be 443 or within 1024-65000 for Small or Medium systems.
- A large Expressway-E listens on the range 3478-3483 (inclusive) by default.
- The configurable range for the TURN listening ports must be in 1024-65000 for Large systems.
- You must override the TCP TURN port that the WebRTC App uses, to 3478, if you are using Expressway-E X8.10 as a TURN server. You must use the Meeting Server API because the setting is not exposed on the UI.

Meeting Server Edge TURN server (optional for this deployment)

- By default, the Meeting Server TURN server listens on ports 443 and 3478. It listens for TURN requests made using UDP or TCP.
- You must use MMP to configure the TURN service on Meeting Server Edge.

Meeting Server call bridge and WebRTC App as TURN clients

- You can point the Meeting Server call bridge and WebRTC App to different TURN server addresses, using the call bridge API or the UI. (Labeled Server address and Client address). This could be to the private and public interfaces of the Expressway-E, respectively.
- If the Cisco Meeting WebRTC App cannot make a UDP TURN request to 3478, it connects to the configurable TCP port number. The default is 443 if no TCP override port is configured.
- You can override the TCP TURN port that the WebRTC App uses. You can change it to any port number (eg. 3478), but you must use the API. The setting is not exposed on the UI.
- Other versions of Cisco Meeting App do not currently use TCP for media (only UDP).
- The Meeting Server call bridge always requests TURN allocations from the server address on UDP 3478. It does not fall back to TCP, and only requires TCP TURN when providing content share capabilities in Microsoft Skype for Business interop calls (beyond scope of this document).

DNS

Publish the TURN server listening address in the external DNS. See DNS Records, page 18

Limitations

- **Expressway-E cannot currently listen on TCP 443 for both the signaling and the TCP TURN requests from the WebRTC App.** In most cases, the WebRTC App makes TURN requests on UDP 3478. However, if that port is blocked for outgoing connections from the browser's location - eg. on some free WiFi networks - then the WebRTC App falls back to making a TCP TURN request. It makes this outbound connection on TCP 443 by default.

The impact of this limitation is that users will not be able to join meetings from some free WiFi networks. If your clients are experiencing this set of circumstances, you have the following options:

- Use a Meeting Server Edge TURN server, which listens on TCP 443 by default.
- Override the TCP fallback port to 3478 (although TCP 3478 may also be blocked outbound from the browser's network).
- Use two Expressway-Es to complete the deployment: One that acts as a TURN server, configured to listen for TCP and UDP TURN requests on 443, and the other to proxy the signaling from the WebRTC App.

- **A Large Expressway-E cannot be configured to listen for TURN requests on 443.**

Configure Meeting Server to Use Expressway-E for TURN Services

You can use the Meeting Server UI to point the call bridge and the clients at a TURN server (as described here), or you can use the API to modify the `/turnServers` node. If you need to modify the TCP override port, you must use the API.

See *Cisco Meeting Server API Reference Guide* on the Cisco Meeting Server programming guides page.

1. Go to **Configuration > General**.
2. Enter the following values:

Fieldname	Example value / description
TURN Server address (CMS)	The Meeting Server uses this address for TURN requests. If you are using Expressway-E TURN server, then it must be the private address of the Expressway-E. If you use two network interfaces on the Expressway-E, then it must be the private address of the internal NIC. You can use an IP address or FQDN in this field.
TURN Server address (CMA)	This is the address that the Cisco Meeting App and the Cisco Meeting WebRTC App use for TURN requests. If using the Expressway-E TURN server, then it should be the public address of the Expressway-E. You can use an IP address or FQDN in this field.
Username	An account to represent the Meeting Server on the TURN server. You must create the corresponding account on the TURN server.
Password	A secret used to authenticate this account. You must share the secret with the corresponding account on the TURN server.
Confirm password	Re-enter the value from the previous field.

3. Submit the configuration.

   The port defaults to 3478 (UDP & TCP) if Meeting Server detects the Expressway-E TURN server.

   There is also a configurable "fallback" port that defaults to 443 (TCP). Cisco Meeting WebRTC Apps can use the fallback port if their UDP requests do not succeed. You cannot override the TCP fallback port with the UI. If you need to change this port, you must modify the `/turnServers` node with the API.

Modify the `/turnServers` node of the Call Bridge configuration using the API

1. Create an API access account on the Cisco Meeting Server if you don't already have one. (Use the Mainboard Management Processor [MMP] to create a user account with type "`api`".)
2. Verify that your browser can connect to the Meeting Server with this account.
3. Install a browser add-on that can POST to the Meeting Server, such as Firefox Poster or Chrome Postman.

4. POST the following key-value pairs to the `/turnServers` node to create the entry for the Expressway-E's TURN server:

Table 2 TURN Server Parameters Required by Meeting Server

Key name	Suggested value
serverAddress	Private address of the Expressway-E
clientAddress	Public address of the Expressway-E
username	Specify a name. Remember the name, which you'll need to create the account on Expressway-E
password	Specify a password. Remember the password, which you'll need to create the account on Expressway-E
type	standard
tcpPortNumberOverride	3478 **Note:** You must configure TCP port override to 3478 if you are using Expressway-E X8.10. The Expressway-E will not service TURN requests on the default of TCP 443, because that port is receiving the signaling from the Cisco Meeting WebRTC App. See Which TURN Server To Use?, page 11

5. To verify the TURN server has been created, send a GET request to the /turnServers node, eg: `https://cms1.example.com:7443/api/v1/turnServers`

Configure Meeting Server Web Proxy on Expressway-C

1. Sign on to the Expressway-C.
2. Go to **Configuration > Unified Communications > Configuration**.
3. Switch **Unified Communications mode** to *Mobile and Remote Access* and click **Save**.
4. Go to **Configuration > Unified Communications > Cisco Meeting Server**.
5. Switch **Meeting Server Web Proxy** to *Enable*.
6. Enter the **Guest account client URI**.
7. Click **Save**.

   The Expressway-C is now ready to proxy https traffic between the Meeting Server and the Expressway-E.

Configure Meeting Server Web Proxy on Expressway-E

To allow Cisco Meeting WebRTC Apps to call into Meeting Server spaces, you need to enable the Meeting Server Web Proxy. This is currently controlled by the Mobile and remote access mode on the Expressway-C and the Expressway-E, but you do not need to completely configure MRA.

You do not need to create any SIP domains on the Expressway-C, and you can ignore the warning on **Status > Unified Communications** that states "*There are no Unified Communications domains configured.*".

1. Sign on to the Expressway-E.
2. Go to **Configuration > Unified Communications > Configuration**.
3. Switch **Unified Communications mode** to *Mobile and Remote Access* and click **Save**.
4. Click **Save**.

   The Expressway-E is now ready to proxy https traffic between a web browser in the internet and the Meeting Server on-premises, via the Expressway-C.

Change Expressway-E Administration Port

You should do this if you are enabling CMS Web Proxy, so that you don't unintentionally make the administrative interface accessible from the internet.

1. Go to **System > Administration** on the Expressway-E UI.
2. Locate the **Web administrator port** setting.
3. Change the value to *7443*.

   You can change the port to anything in the range `1..65535` using the CLI command `xconfiguration Management Interface Port:<port>`. Be careful to avoid losing access to the UI, or overlapping other ports.
4. Restart the Expressway-E.

You should also configure your firewall to block access to the new administrative port on the public IP address(es).

Web Proxy for Meeting Server Media Flows

Figure 1 Media Flow Between Internal WebRTC App and Meeting Server

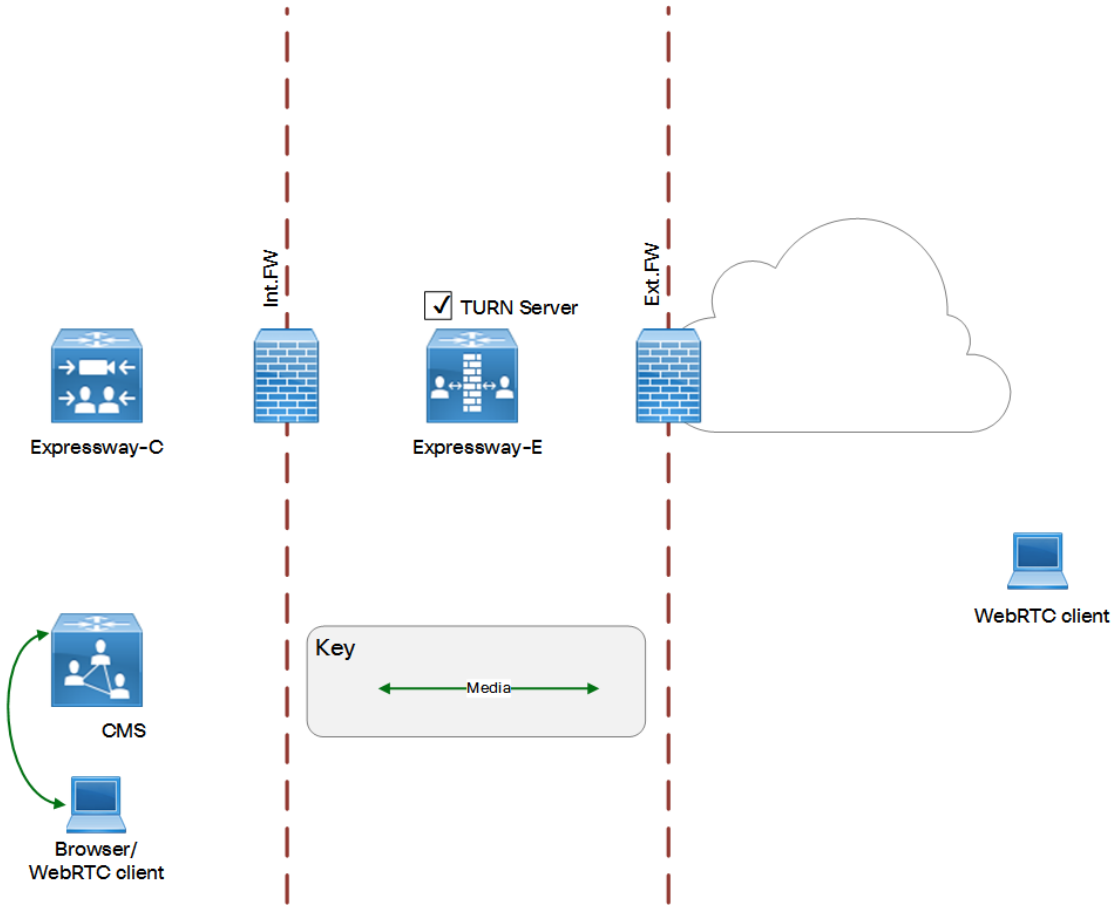


Figure 2 Media Flow Between External WebRTC App and Meeting Server, Single-NIC Expressway-E

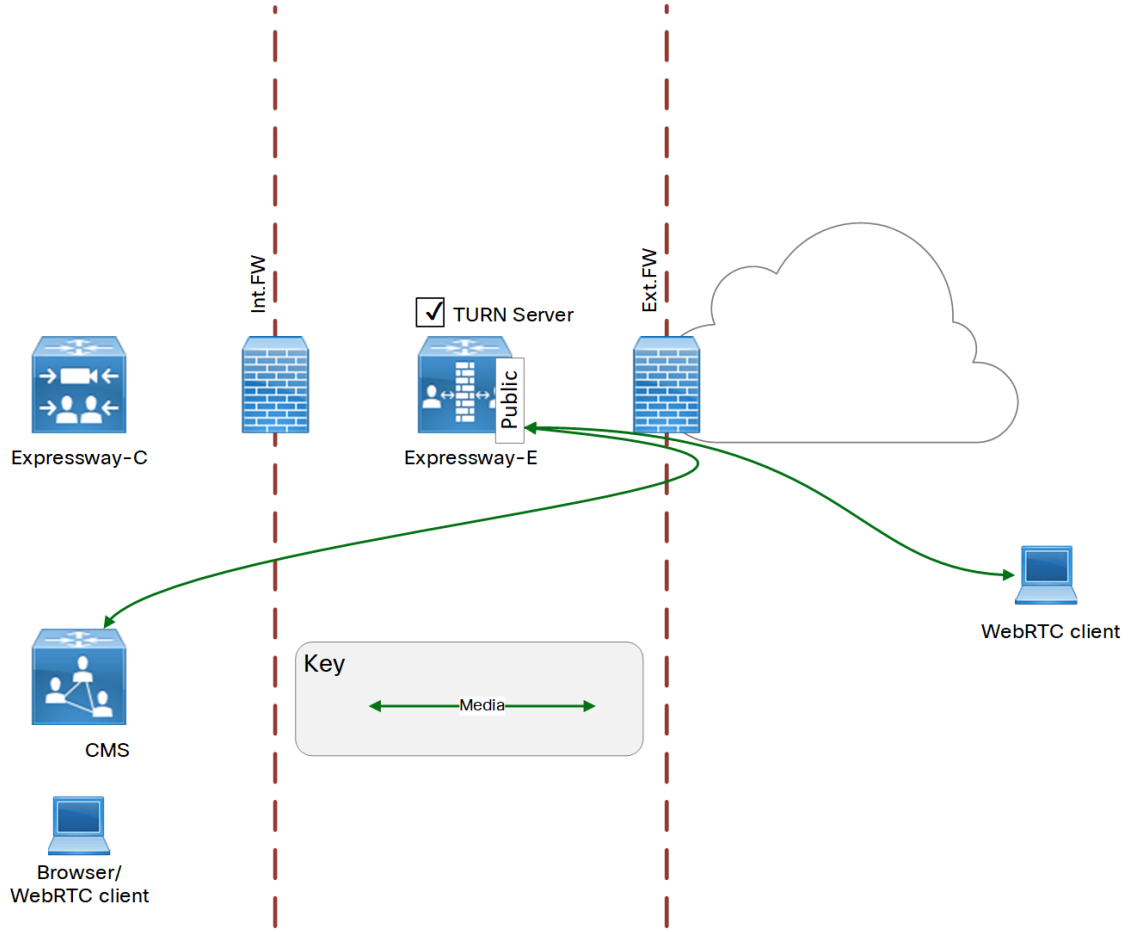
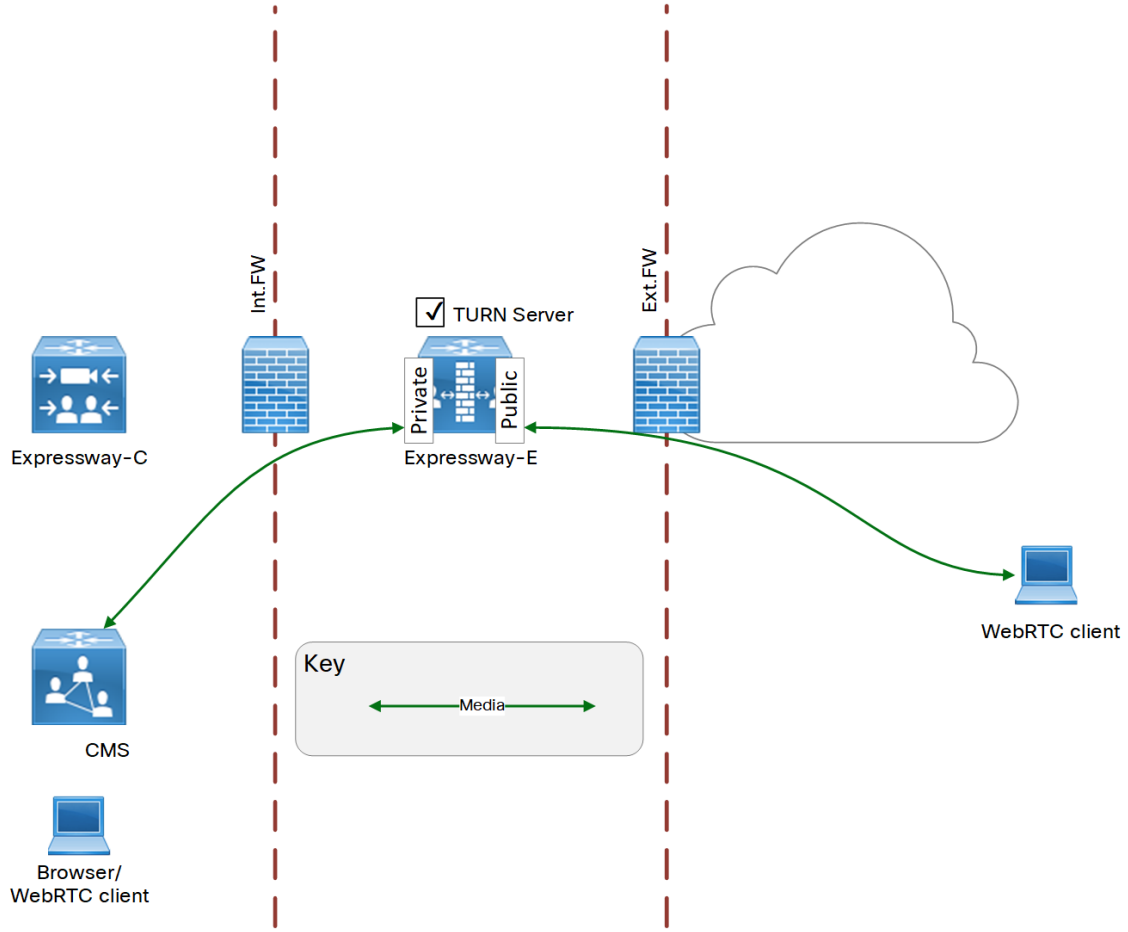


Figure 3 Media Flow Between External WebRTC App and Meeting Server, Dual-NIC Expressway-E



DNS Records

Table 3 External DNS Configuration Summary (Assumes Split or Private DNS)

Purpose	Record type	Example entry	Port	Resolves to target
Resolve Expressway-E cluster FQDN to peer IP addresses	A/AAAA	`expe.ciscoexample.com`		Public IP address of one Expressway-E cluster peer. Create one record for each peer in the Expressway-E cluster (Up to 6 records).
[Minimum requirement for external DNS] Enable guest browsers to find the Expressway-E reverse proxy **Note:** If you can split DNS, then we recommend you create a more direct mapping to the web bridge in your internal DNS.	A/AAAA	*`join.ciscoexample.com`* (the **Guest account client URI** on the web bridge settings of the Meeting Server)		Public IP addresses of Expressway-E peers. Create one record for each peer in the Expressway-E cluster (Up to 6 records).
Enable guest browsers to find the TURN server	A/AAAA	The public address of the TURN server. Corresponds with the value you entered for **TURN Server address (CMA)** / `clientAddress` in the Meeting Server TURN server configuration.		Expressway-E public IP address or Meeting Server Edge TURN server.

If you can split your DNS to give different results internally, then we recommend that you create internal records for the following purposes. These records must be resolvable by Expressway-C.

Table 4 Internal DNS Configuration Summary (Assumes Customizable Split or Private DNS)

Purpose	Record type	Example entry	Port	Resolves to
Resolves private IP address of Web Bridge listening interface. This allows on-premises Cisco Meeting WebRTC Apps to connect to the web bridge.	A	*`join.ciscoexample.com`* (the **Guest account client URI** on the web bridge settings of the Meeting Server)		IP address of the web bridge interface. IPv6 not supported.
[Optional for internal DNS] Resolves service requests for the Meeting Server web bridge to individual Meeting Server FQDNs.	SRV	`_cms-web._tls.`*`join.ciscoexample.com`*.	443	Internal FQDN of the Cisco Meeting Server web bridge, eg. `cms1.ciscoexample.com`.

Table 5 Modifications Required If You Cannot Customize Internal DNS

Purpose	Record type	Example entry	Port	Resolves to
[This external DNS record is required if you cannot split DNS. The external rule is not recommended if you can split DNS] Resolves service requests for the Meeting Server web bridge to individual Meeting Server FQDNs. These SRV records are specifically used by the Expressway-C to find the internal Meeting Server web bridge details. **Note:** If you can split DNS, then we recommend you do not put this service record in the public DNS; this is an avoidable leak of information about internal servers.	SRV	`_cms-web._tls.` *`join.ciscoexample.com`* `.`	443	Internal FQDN of the Cisco Meeting Server, eg. `cms1.ciscoexample.com.`
[This external DNS record is required if you cannot split DNS. The external rule is not recommended if you can split DNS] This allows on-premises WebRTC App users, and the Expressway-C, to connect to the web bridge(s).	A	*`cms1.ciscoexample.com`* (FQDN of the Meeting Server)		(Private) IP address of the web bridge listening interface. IPv6 not supported.

Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

© 2016-2018,2020 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)