OTT Deployment and Secured Internet with Collaboration Edge Expressway

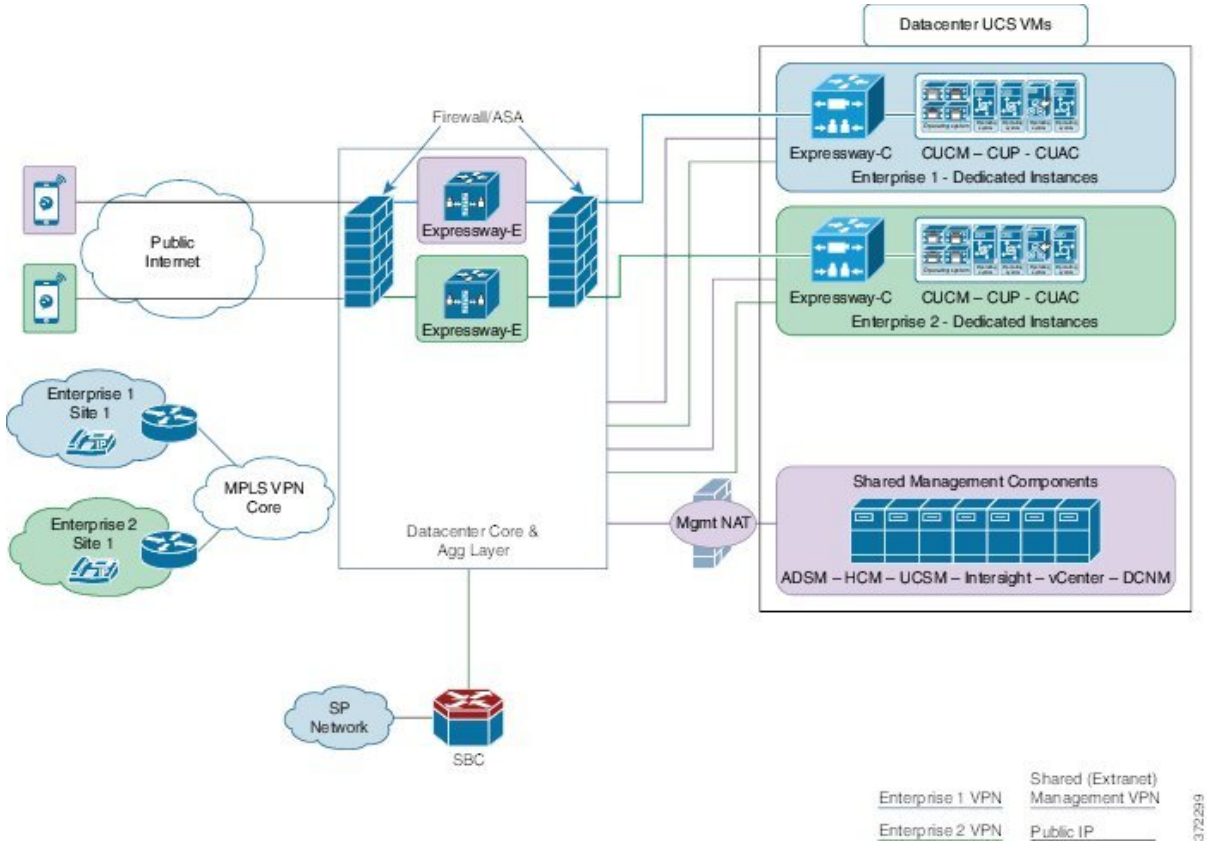
Cisco Expressway Over-the-Top Solution Overview

The Cisco Expressway product allows VPN-less connection from mobile 'Bring your own' devices and allows a user to access all the collaboration tools they have in the office environment when they are outside of the office.

Cisco Unified Communications mobile and remote access is a core part of the Cisco Collaboration Edge Architecture. It allows endpoints such as Cisco Jabber to have their registration, call control, provisioning, messaging and presence services provided by Cisco Unified Communications Manager (Unified CM) when the endpoint is not within the enterprise network. The Expressway provides secure firewall traversal and line-side support for Unified CM registrations.

The following diagram shows the Cisco Expressway architecture for Cisco HCS.

Figure 1: Cisco Expressway Architecture



Supported Functionality

The following Cisco Jabber functions are supported without a VPN connection:

- IM and Presence
- Make and receive voice and video calls
- Mid call control (transfer, conference, mute, hold, park, handoff to mobile , and so on)
- Communications history (view placed, missed, received calls)
- Directory search: The HTTP proxy will allow Jabber to use the CUCM User Data Service (UDS)
- Escalate to Web conference (MeetingPlace / Webex)
- Screen share / file transfer when Jabber is in SSO mode
- Visual Voicemail (view, play, delete, filter by, sort by over HTTP)

Endpoint Support

The Cisco Collaboration Edge Architecture provides enabling for any-to-any collaboration for many types of endpoint devices. For the Cisco Expressway implementation in Cisco Hosted Collaboration Solutions the following endpoints are supported:

- Jabber Desktop - Windows
- Jabber Mobile - iPhone, Android, and iPad
- Hard endpoints - EX60, EX90
- Cisco DX Series endpoints
- 7800 Series IP phones
- 8800 Series IP phones

Note DX/78XX/88XX endpoints have a fixed certificate trust list that is not configurable by the administrator. The Cisco Collaboration Edge Architecture needs to have a certificate signed by a real certificate authority.

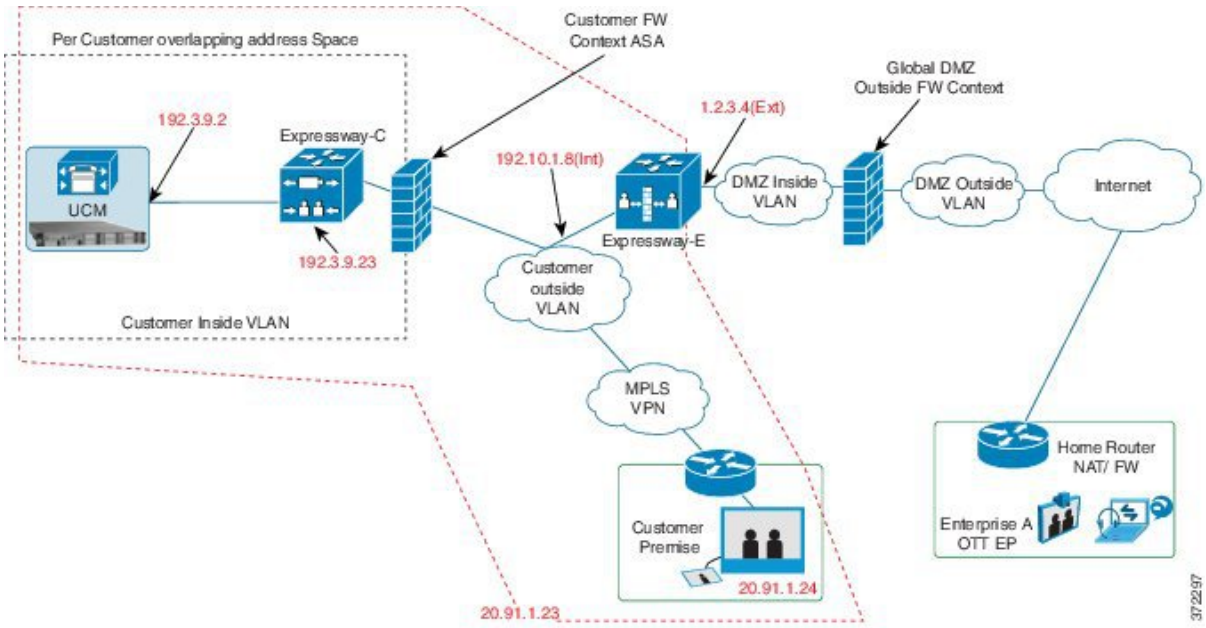
Design Highlights

The Cisco Expressway OTT Solution provides the following design highlights:

- Expressway-E is treated as an SBC and like any other endpoint is routed through the Firewall.
- Unified CM provides call control for both mobile and on-premises endpoints.
- Signaling traverses the Expressway solution between the mobile endpoint and UCM.
- Media traverses the Expressway solution and is relayed between endpoints directly; all media is encrypted between the Expressway-C and the mobile endpoint.

The following diagram illustrates these highlights.

Figure 2: Cisco Expressway Design Highlights



Expressway Sizing and Scaling

The Expressway-E and Expressway-C platforms can be deployed in clusters of four (for n+2 redundancy) with the possibility of deploying multiple clusters if necessary. Clusters of six VMs can accommodate up to four times the maximum call capacity.

The three deployment options (distributed as OVAs) have the following specifications:

Deployment size	vCPU	Reserved CPU resource	Reserved RAM	Diskspace	NIC
Small	2 core	3600 MHz (2 x 1.8 GHz)	4 GB	132 GB	1 Gb
Medium	2 core	4800 MHz (2 x 2.4 GHz)	6 GB	132 GB	1 Gb
Large	8 core	25600 MHz (8 x 3.2 GHz)	8 GB	132 GB	1 Gb

For more information, see https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/install_guide/Cisco-Expressway-Virtual-Machine-Install-Guide-X12-5-4.pdf.

Virtual Machine Options

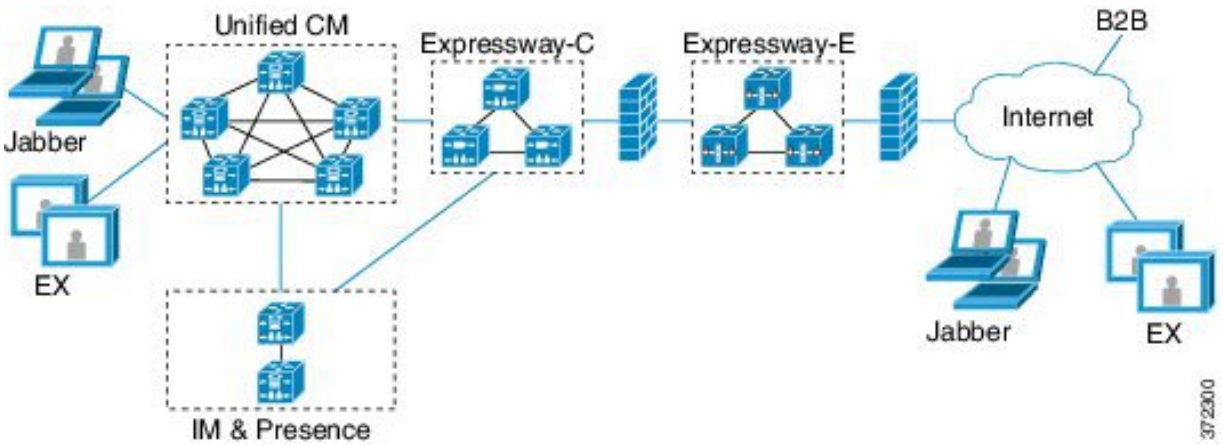
In Large PoD HCS, it is expected that Expressway-C and Expressway-E will run on B-series blades. The above resource needs should be considered in the HCS recommendation for scaling/sizing.

For information on Expressway VM sizing options see *Cisco Hosted Collaboration Solution Compatibility Matrix*.

Cisco HCS Clustered Deployment Design

In this scenario each network element is clustered in the tested design. Other Cisco Expressway deployment options are available in the Cisco Expressway documentation. In HCS verification, only the Cisco Expressway-C was clustered.

Figure 3: Cisco HCS Clustered Deployment



Network Elements

Internal Network Elements

The internal network elements are devices which are hosted on the organization's local area network.

Elements on the internal network have an internal network domain name. This internal network domain name is not resolvable by a public DNS. For example, the Expressway-C is configured with an internally resolvable name of vcsc.i nternal-domain.net, which resolves to an IP address of 10.0.0.2 by the internal DNS servers.

Cisco Expressway Control

The Expressway-C is a SIP Registrar & Proxy and H.323 Gatekeeper for devices that are located on the internal network.

Expressway-C is configured with a traversal client zone to communicate with the Expressway-E to allow inbound and outbound calls to traverse the NAT device.

DNS

DNS servers are used by Expressway-C to perform DNS lookups (resolve network names on the internal network).

DHCP Server

The DHCP server provides host, IP gateway, DNS server, and NTP server addresses to endpoints located on the internal network.

Router

The router device acts as the gateway for all internal network devices to route towards the DMZ (to the NAT device internal address).

DMZ Network Element

Expressway-E

Expressway-E is a SIP Registrar & Proxy and H.323 Gatekeeper for devices that are located outside the internal network (for example, home users and mobile worker registering across the internet and 3rd party businesses making calls to, or receiving calls from this network).

Expressway-E is configured with a traversal server zone to receive communications from Expressway-C in order to allow inbound and outbound calls to traverse the NAT device.

Expressway-E has a public network domain name. For example, Expressway-E is configured with an externally resolvable name of vcse.example.com (which resolves to an IP address of 192.0.2.2 by the external / public DNS servers).

External Network Elements

EX60

This is an example remote endpoint that is registering to the Cisco Expressway via the internet.

DNS (Host)

This is the DNS owned by the service provider that hosts the external domain (DNS (external 1 & external 2). This is also the DNS used by the Cisco Expressway to perform DNS lookups.

NTP Server Pool

An NTP server pool that provides the clock source used to synchronize both internal and external devices.

NAT Devices and Firewalls

The example deployment includes:

- The NAT (PAT) device performing port address translation functions for network traffic routed from the internal network to addresses in the DMZ (and beyond - towards remote destinations on the internet).
- The firewall device on the public-facing side of the DMZ. This device allows all outbound connections and inbound connections on specific ports.
- The home firewall NAT (PAT) device which performs port address and firewall functions for network traffic originating from the EX60 device.

SIP Domain

- DNS SRV records are configured in the public (external) and local (internal) network DNS server to enable routing of signaling request messages to the relevant infrastructure elements (for example, before an external endpoint registers, it will query the external DNS servers to determine the IP address of the Cisco Expressway).
- The internal SIP domain is the same as the public DNS name. This enables both registered and non-registered devices in the public internet to call endpoints registered to the internal and external infrastructure (Expressway-C and Expressway-E).

Jabber Client SSO OTT

You can enable Single Sign-On for Jabber client endpoints that access unified communications services from outside of the network (over the top, OTT). Single Sign-on OTT relies on the following:

- The secure traversal capabilities of the Expressway pair at the edge of the network
- The trust relationship between the customer provisioning authority and the external identity provider.

Endpoints connect using one identity and one authentication mechanism to access multiple unified communications services. Authentication is owned by the IdP. No authentication occurs at the Expressway or at the internal unified communications services.

Cisco Jabber determines whether it is inside your network before it requests a unified communications service. When Jabber is outside of the network, it requests the service from the Expressway-E on the edge of the network. If SSO is enabled at the edge, the Expressway-E redirects Jabber to the IdP with a request to authenticate the user.

The IdP challenges Jabber to identify itself. After the identify is authenticated, the IdP redirects the Jabber service request to the Expressway-E with a signed assertion that the identity is authentic.

Because the Expressway-E trusts the IdP, it passes the request to the appropriate service inside the network. The unified communications service trust the IdP and the Expressway-E, so it provides the requested service to the Jabber client.

The provisioning of Jabber Client SSO involves such tasks as downloading the federation metadata file, configuring Unified CM and Cisco Unity Connection, configuring SAML SSO, and configuring AD FS. For more information, see the *Cisco Unified Communications Domain Manager Maintain and Operate Guide*.

This feature is supported in the following deployment models:

- IdP and the directory are in the customer premises, with LDAP synchronization from the Directory server to CUCM and then to Cisco Unified Communications Domain Manager.
- IdP and the directory are in the customer premises, with LDAP synchronization from the Directory server to CUCM and then to Cisco Unified Communications Domain Manager.
- IdP and the directory are in a per-customer domain in the Data Center, with LDAP synchronization from the Directory server to CUCM and then to Cisco Unified Communications Domain Manager.
- IdP and the directory are in a per-customer domain in the Data Center, with LDAP synchronization from the Directory server to CUCM and then to Cisco Unified Communications Domain Manager.

References

For information about SSO for Jabber clients, see the *Cisco Hosted Collaboration Solution Customer Onboarding Guide*.

For information about SSO for Cisco collaboration solutions, see the *SAML SSO Deployment Guide for Cisco Unified Communications Applications*: http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

BtoB Calls Shared Edge Expressway

Cisco Expressway Over-the-Top Solution Overview

Cisco Expressway enables secure connectivity options that allow dialing to and from non-HCS enterprises reachable through the internet.

Cisco HCS currently provides connectivity to the PSTN network and managed conferencing services through a managed connectivity. As part of the evolution of the Cisco HCS architecture, URI-based B2B connectivity to internet users is supported in Cisco HCS to allow tenants to use URIs to dial and receive calls from any non-HCS enterprise users through the internet. This is achieved by deploying a shared Expressway-E and Expressway-C products behind the session border controller, or SBC.

Expressway-E is configured to route any URI out in the internet by doing a DNS SRV resolution and route securely.

From the HCS Endpoint the dialed URIs if they do not belong to the dialing tenant are routed on a dedicated adjacency to the SBC where special call-policies are configured which route these URI's to Expressway-C for onward routing to the user on Internet through Expressway-E.

Options are available within the call-policies to select all or block certain URIs within the SBC:

- This feature allows all HCS tenants to use URIs to dial and receive calls from any non-HCS Enterprise users thru the internet. Rich media licenses are therefore shared on the Expressway products. This is a trunking-based solution.
- This feature differs from the Collaboration Edge/OTT Expressway feature where Jabber and TC-based endpoints register via the internet and are configured per HCS customer. This is a registration-based solution.

Supported Functionality

The following functions of Cisco Expressway are supported within Cisco Hosted Collaboration Solution:

- Non-HCS Enterprise users can dial into Cisco HCS using the HCS user's URI.
- Cisco HCS users can dial non-HCS video users using URIs.

Endpoint Support

- All Cisco HCS supported Video Endpoints can make and receive calls using Shared Expressway.
- Remote non-HCS endpoints must conform to Cisco Telepresence Interface specifications to successfully make and receive video calls.

Design Highlights

The Cisco Shared Expressway for Business to Business calling solution features the following design highlights:

- Expressway-E is treated as a session border controller (SBC), and like any other endpoint, is routed through the firewall. Expressway-E is deployed in the DMZ with one interface (NIC) facing the internet and the other interface (NIC) connected to the Expressway-C.
- SBC peers with the shared Expressway-C and provides the connectivity to each tenant's leaf cluster over a dedicated adjacency exclusively used for URI dialing.
- Cisco Unified Communications Manager is configured with a dedicated trunk toward the SBC for URI dialing.
- Cisco Unified Communications Manager is provisioned with wildcard SIP route patterns to route to SBC.
- SBC performs onward routing.
- Signaling traverses the Expressway solution between the Internet non-HCS Endpoint and SBC.
- All media is encrypted between the Expressway-E and the remote non-HCS endpoint.

Virtual Machine Options

For a Large PoD deployment of Cisco Hosted Collaboration Solution, it is expected that Expressway-C and Expressway-E will run on B-series blades. These resource needs should be considered in the recommendations for Cisco HCS scaling/sizing.

In an SMB deployment of Cisco HCS, it is possible to use the C-series server for both Expressway-E and Expressway-C. It is also possible to run Expressway-E on a C-series server, and run Expressway-C on B-series along with other applications.

For information on Cisco Expressway VM sizing options, see the *Cisco Hosted Collaboration Solution Compatibility Matrix*.

Network Elements

Internal Network Elements

The internal network elements are devices which are hosted on the organization's local area network.

Elements on the internal network have an internal network domain name. This internal network domain name is not resolvable by a public DNS. For example, the Expressway-C is configured with an internally resolvable name of `vcsc.internal-domain.net`, which resolves to an IP address of 10.0.0.2 by the internal DNS servers.

Element	Description
Cisco Expressway Control	Expressway-C is configured with a traversal client zone to communicate with the Expressway-E to allow inbound and outbound calls to traverse the NAT device.
DNS	DNS servers are used by Expressway-C to perform DNS lookups (resolve network names on the internal network).

DMZ Network Elements

Element	Description
Expressway-E	Expressway-E in Business-to-Business deployment is used to terminate or connect to third-party enterprises through the Internet to receive and make Video calls using URI based routing. Expressway-E is configured with a traversal server zone to receive communications from Expressway-C in order to allow inbound and outbound calls to traverse the NAT device. Expressway-E has a public network domain name. For example, Expressway-E is configured with an externally resolvable name of `vcse.example.com` (which resolves to an IP address of 192.0.2.2 by the external/public DNS servers).

External Network Elements

Element	Description
DNS (Host)	This is the DNS owned by the service provider that hosts the external domains (DNS). This is also the DNS used by Cisco Expressway to perform DNS lookups.
NTP Server Pool	An NTP server pool that provides the clock source used to synchronize both internal and external devices.
NAT Devices and Firewalls	The example deployment includes: • The NAT(PAT) device performing port address translation functions for network traffic routed from the internal network to addresses in the DMZ (and beyond- towards remote destinations on the internet). • The firewall device on the public-facing side of the DMZ. This device allows all outbound connections and inbound connections on specific ports.
SIP Domain	• DNS SRV records are configured in the public (external) and local (internal) network DNS server to enable routing of signaling request messages to the relevant infrastructure elements (for example, third-party enterprises query an external DNS for Cisco HCS enterprise Domains to determine the IP address of the shared expressway-E.). • The internal SIP domain is the same as the public DNS name. This enables both registered and non-registered devices in the public internet to call endpoints registered to the internal and external infrastructure.