

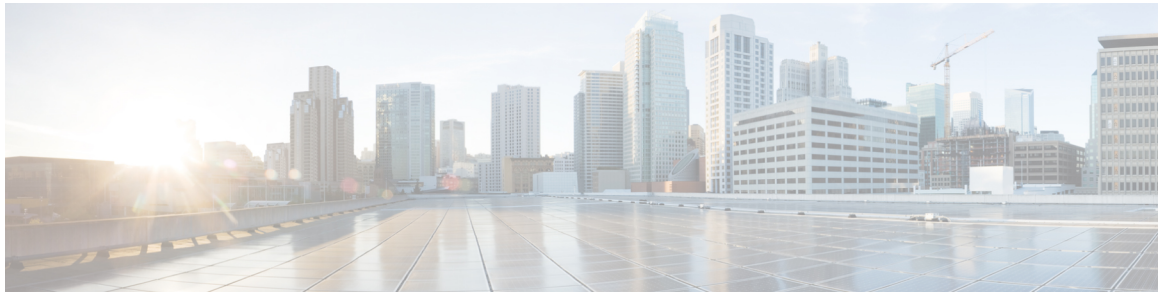


Cisco Webex Contact Center Voice Onboarding Guide

First Published: 2020-12-02

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

PREFACE

Preface	vii
Change History	vii
About this Guide	vii
Audience	vii
Related Documents	viii
Conventions	viii
Communications, Services, and Additional Information	ix
Documentation Feedback	ix

CHAPTER 1

Provision Voice for Cisco Webex Contact Center	1
Overview	1

CHAPTER 2

Webex Contact Center Call Flow	5
Inbound Call to an IVR	5
Inbound Call to an Agent	6
Conference and Consult Transfer	7
Callback or Outbound Call to PSTN	8

CHAPTER 3

CUBE License and Sizing Requirements	11
Cube Licensing	11
CUBE Session Sizing	11

CHAPTER 4

Types of Connectivity	13
Public Internet	13

	Private Connectivity	16
	Non-Standard Deployments	18
<hr/>		
CHAPTER 5	Component Redundancy	21
	Redundancy Across Enterprise Data Centers Within a Geographic Region	21
<hr/>		
CHAPTER 6	Enterprise CUBE to Webex Contact Center Configuration Example	23
	Basic Configuration	23
	Common Configuration	24
<hr/>		
CHAPTER 7	Secure SIP Trunk Between CUBE and Webex Contact Center	27
	Example Configure SIP TLS	27
<hr/>		
CHAPTER 8	Configure SIP Trunk for Your Tenant	29
	Before you Configure	29
	Provision Your Tenant	29
	Webex Contact Center Regions	29

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 of this document are considered uncontrolled. See the current online version for the latest version.

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

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.



Preface

- [Change History, on page vii](#)
- [About this Guide, on page vii](#)
- [Audience, on page vii](#)
- [Related Documents, on page viii](#)
- [Conventions, on page viii](#)
- [Communications, Services, and Additional Information, on page ix](#)
- [Documentation Feedback, on page ix](#)

Change History

This table lists changes made to this guide. Most recent changes appear at the top.

Change	See	Date
Included a new chapter	Types of Connectivity, on page 13	December 2020
Initial Release of Document		

About this Guide

This document describes the setup of a Cisco Unified Border Element (CUBE) as the session border controller (SBC) at the customer enterprise that connects to Cisco Webex Contact Center.

Audience

This document is intended for users who use Cisco Webex Contact Center.

Related Documents

To view the list of Cisco Webex Contact Center documents, go to page <https://www.cisco.com/c/en/us/support/customer-collaboration/webex-contact-center/series.html>.

To view Cisco Webex Contact Center developer documents and API references, go to page <https://apim-dev-portal.devus1.ciscoccservice.com/documentation/getting-started>.

Conventions

This guide uses the following conventions.

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example: <ul style="list-style-type: none">• Choose Edit > Find• Click Finish.
<i>italic</i> font	Italic font is used to indicate the following: <ul style="list-style-type: none">• To introduce a new term. Example: A <i>skill group</i> is a collection of agents who share similar skills.• For emphasis. Example: <i>Do not</i> use the numerical naming convention.• An argument for which you must supply values. Example: IF (<i>condition, true-value, false-value</i>)• A book title. Example: See the <i>Cisco Webex Contact Center Getting Started Guide</i>.

Convention	Description
window font	<p>Window font, such as Courier, is used for the following:</p> <ul style="list-style-type: none">• Text as it appears in code or information that the system displays. Example: <pre><html><title> Cisco Systems, Inc. </title></html></pre>• File names. Example: <code>tserver.properties.</code>• Directory paths. Example: <code>C:\Program Files\Adobe</code>

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Documentation Feedback

Provide your comments about this document to: mailto:contactcenterproducts_docfeedback@cisco.com.



CHAPTER 1

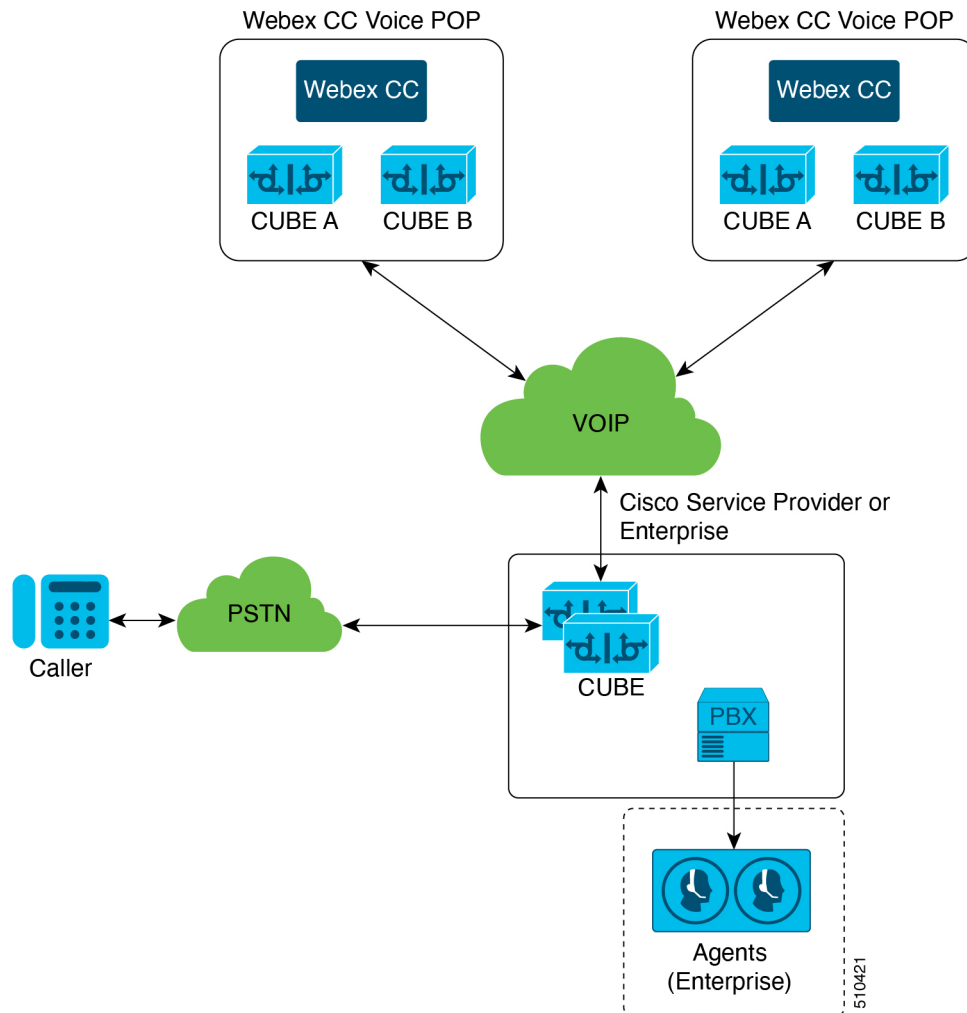
Provision Voice for Cisco Webex Contact Center

- [Overview, on page 1](#)

Overview

This document describes the setup of a Cisco Unified Border Element (CUBE) as the session border controller (SBC) at the customer enterprise that connects to Cisco Webex Contact Center. Enterprise CUBE connects to a carrier for PSTN or VoIP connectivity on one side and to Webex Contact Center on the other side to enable cloud contact center services. Both inbound and outbound calls to Webex Contact Center route through your enterprise CUBE. The customer provides the SIP trunk, activated bidirectionally by both the service provider and Webex Contact Center, to enable the call traffic between the platforms. For more information about CUBE, see [Information About Cisco Unified Border Element](#).

Figure 1: Cisco Service Provider or Enterprise Architecture



Either the service provider or the customer enterprise can own and operate the CUBE and the PBX. In this case:

- All inbound calls to Webex Contact Center come through the carrier at the enterprise CUBE.
- Webex Contact Center sends all outbound calls, whether to customers or agents, through the enterprise CUBE.
- Webex Contact Center works with the service provider to bill the customer directly for PSTN usage, without going through Webex Contact Center billing.

Webex Contact Center supports CUBE, Virtual CUBE (vCUBE) and third-party SBC.

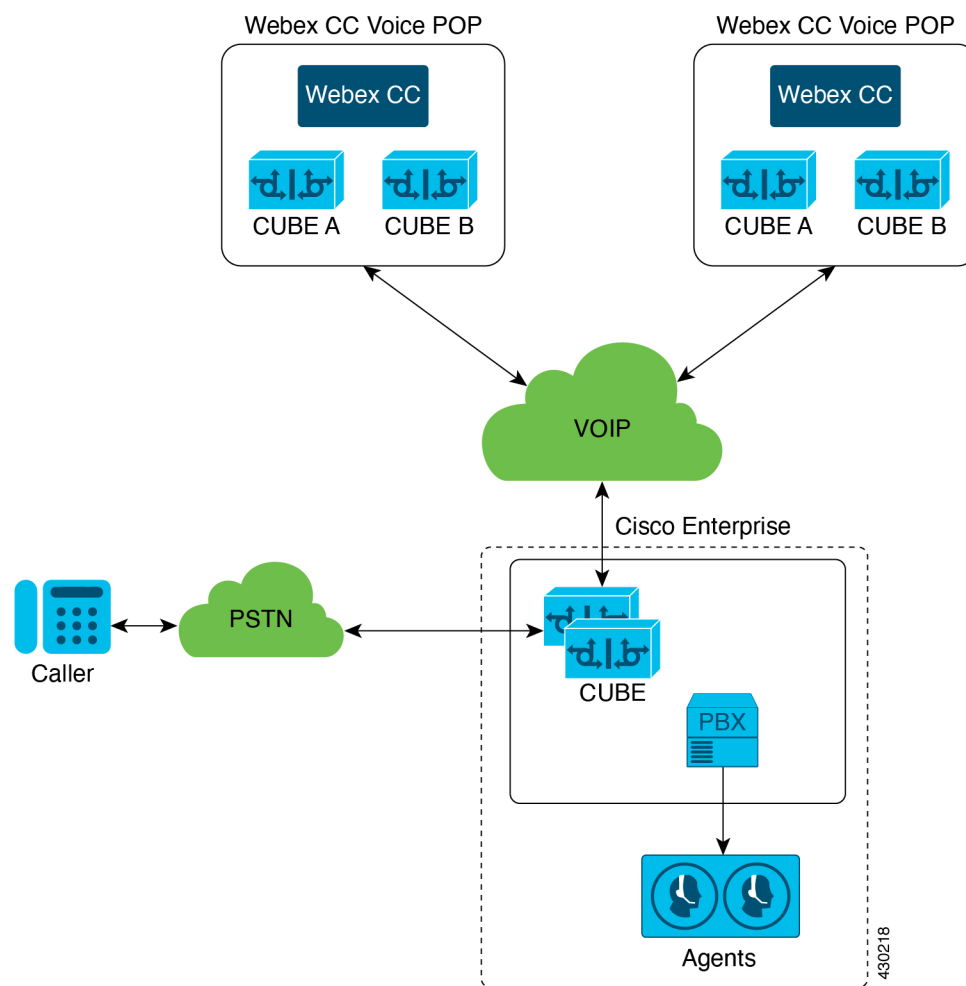
When the service provider owns the SBC and PBX, Webex Contact Center provides a SIP header identifying the customer enterprise to the service provider. Service providers configure specific SIP header through the Application Service Provider dashboard.

Webex Contact Center supports these SIP headers:

- Diversion
- PAI
- OTG
- DTG
- TGRP
- RPID

In some cases, the customer enterprise owns and operates the CUBE and the PBX, which eliminates the need for a SIP header.

Figure 2: Customer Enterprise Architecture





CHAPTER 2

Webex Contact Center Call Flow

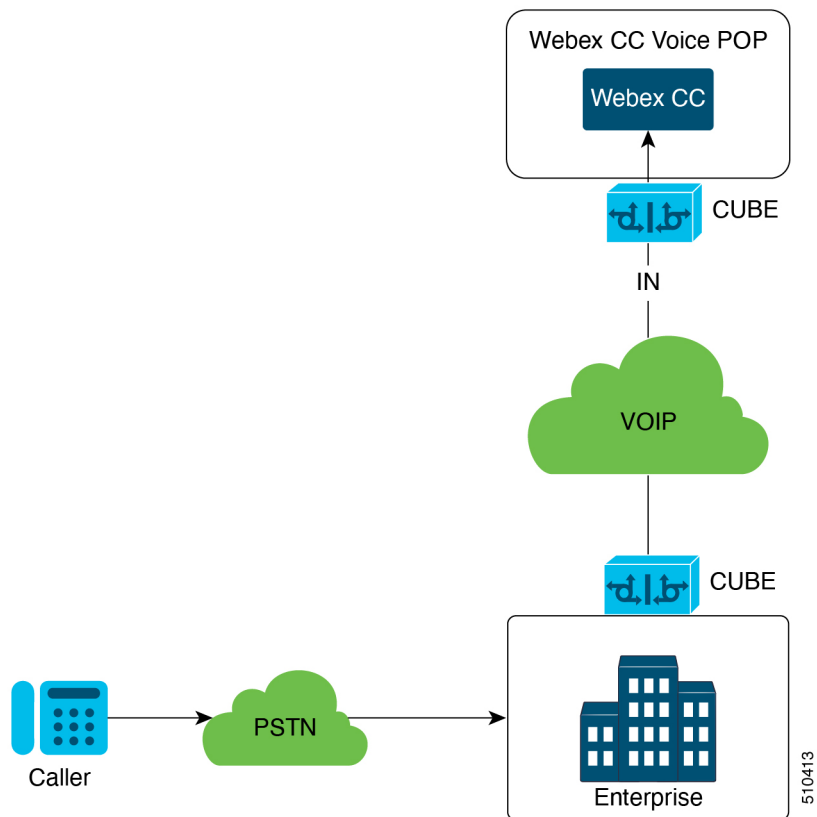
Inbound and outbound calls to Webex Contact Center come through a carrier, which is routed through the Enterprise and CUBE. Every call can include multiple sessions, depending on the call flow. Typical call flows include:

- [Inbound Call to an IVR, on page 5](#)
- [Inbound Call to an Agent, on page 6](#)
- [Conference and Consult Transfer, on page 7](#)
- [Callback or Outbound Call to PSTN, on page 8](#)

Inbound Call to an IVR

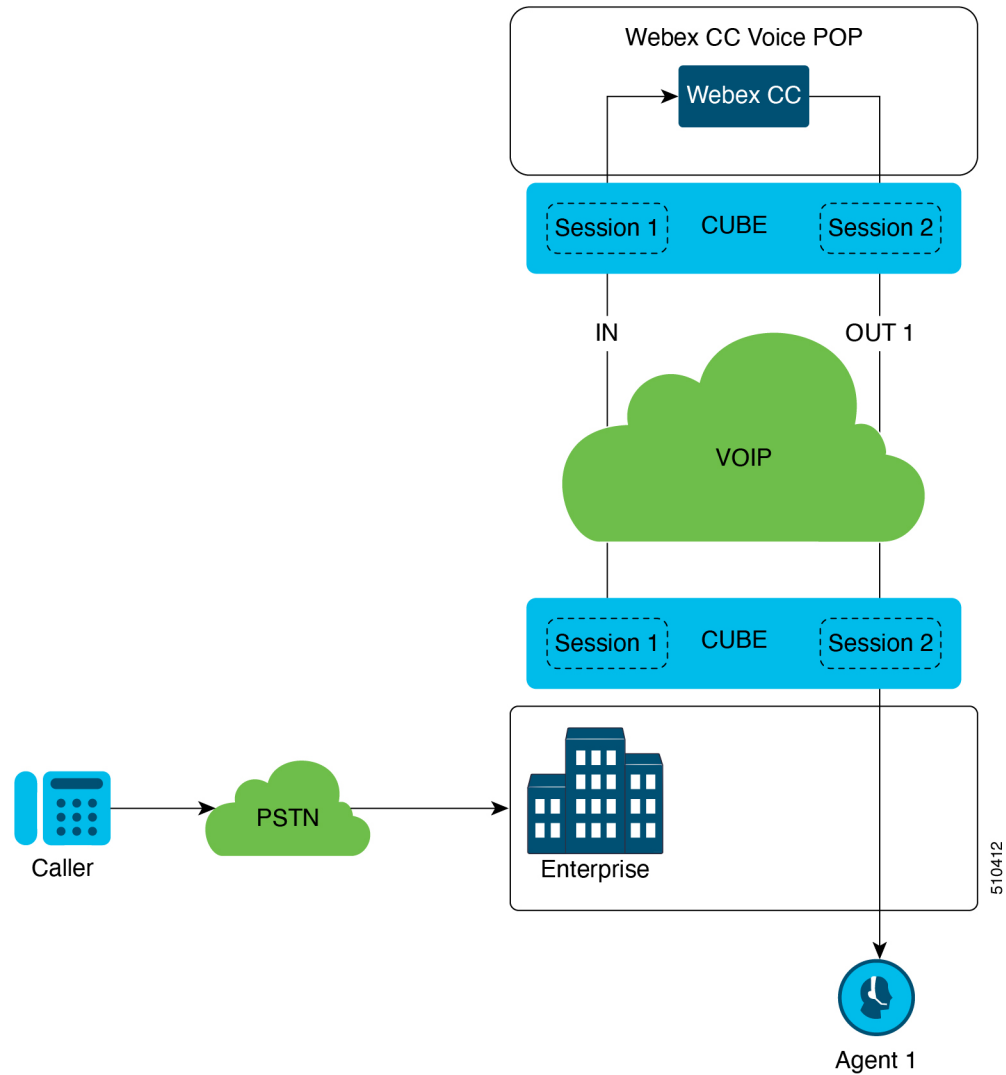
An inbound call from the caller to the Webex Contact Center Voice POP creates a single session in the enterprise CUBE and a single session in the Webex Contact Center CUBE.

Figure 3: Inbound Call to IVR



Inbound Call to an Agent

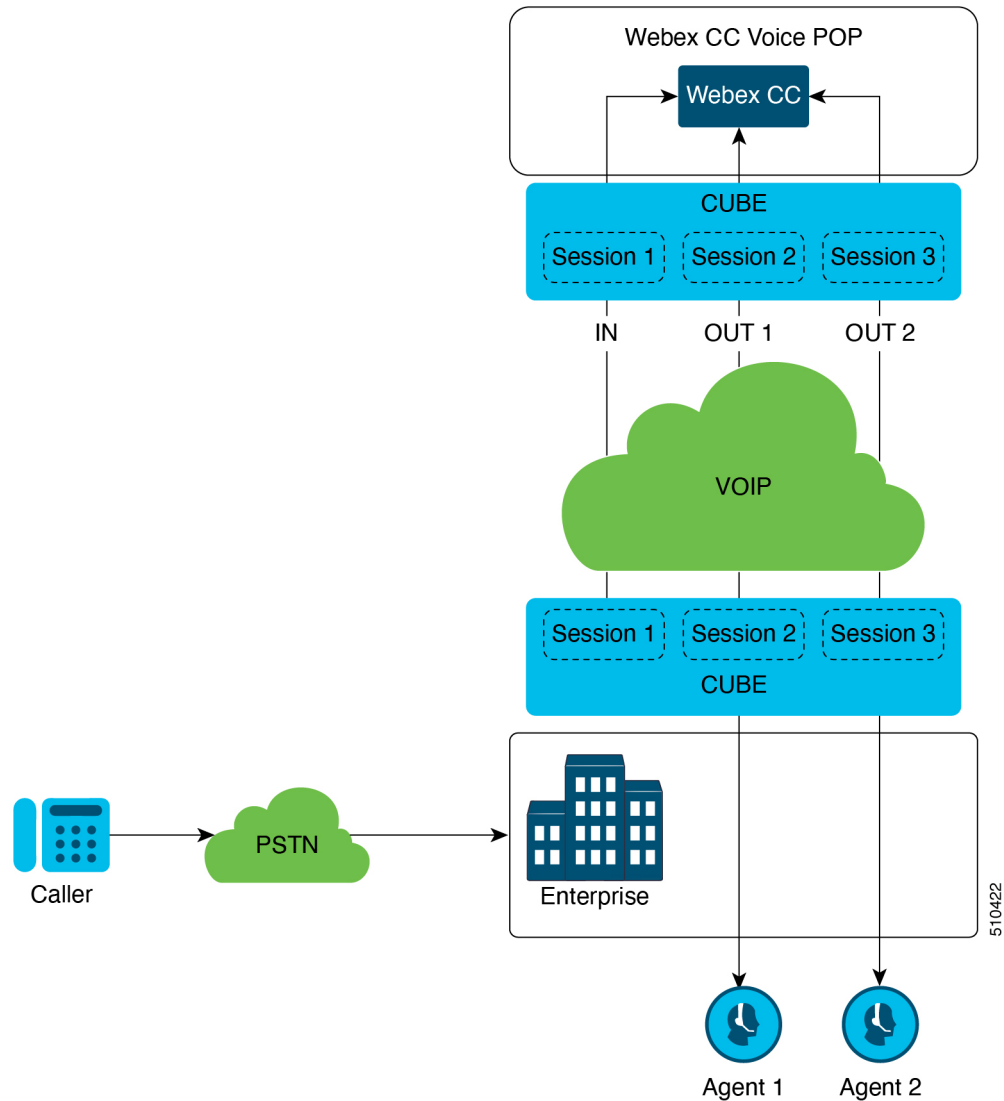
An inbound call to an agent adds an outbound session in the Webex Contact Center CUBE and a single session in the enterprise CUBE.

Figure 4: Inbound Call to an Agent

Conference and Consult Transfer

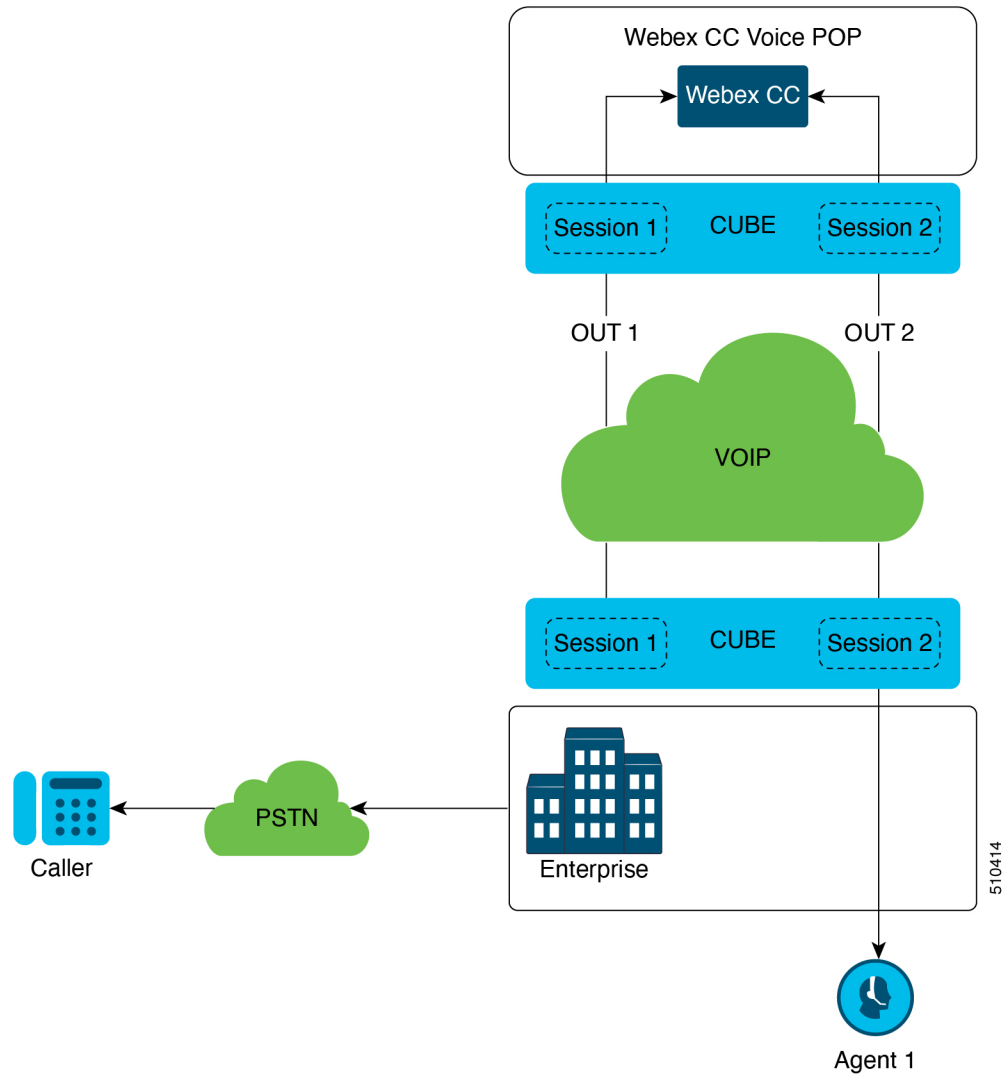
An agent to agent conference or consult transfer creates an additional outbound session in Webex Contact Center and enterprise CUBE.

Figure 5: Agent to Agent Conference



Callback or Outbound Call to PSTN

An outbound call creates two sessions, one from the Enterprise tenant to Webex Contact Center and another from Webex Contact Center to the Enterprise.

Figure 6: Outbound Call to PSTN



CHAPTER 3

CUBE License and Sizing Requirements

- [Cube Licensing, on page 11](#)
- [CUBE Session Sizing, on page 11](#)

Cube Licensing

Cisco Unified Border Element (CUBE) is licensed per session and requires a two-way session. For more information, see [Cisco Unified Border Element Data Sheet](#).

CUBE license sizing is the sum of the number of agent sessions and the number of calls at the Interactive Voice Response (IVR). Use the [CUBE Data Sheet](#) to determine the maximum number of sessions that your CUBE platform supports.

The number of licenses should be equal to the maximum capacity of the enterprise. Capacity is calculated as (number of agents X 2) + (number of active sessions in queue). For example:

- At peak time if you have 100 agents responding to customer calls, each call has two active sessions. The number of sessions is 200.
- The number of calls in queue in this instance is 100, which creates 100 sessions.
- Therefore, the total number of sessions equals 300 which is 300 licenses.

CUBE Session Sizing

A CUBE device can handle 1/3 of SIP sessions, if you have secured the calls using either TLS or SRTP. This is calculated as ((number of agents X 2) + (number of active sessions in queue)) X 3. Using the example of 100 calls in queue with 100 agents responding to calls, the number of sessions is ((100 X 2) + 100) X 3 = 900.

You can size the CUBE for 300 sessions if you have provisioned a private WAN for the SIP Trunk.

To help determine the maximum number of agents, assume that:

- 50% of calls are queued and use IVR ports, while the remaining 50% of calls are active with agents.
- 10% of calls use the consult and conference supplementary services.
- 100% of calls are secured using either TLS or SRTP.

Based on these assumptions, CUBE platforms can support one agent for every 9.3 sessions.



CHAPTER 4

Types of Connectivity

Webex Contact Center supports the following types of connectivity:

Connectivity	Types
Public Internet	Direct IPSec VPN or IPSec over GRE S2S SRTP/SIP TLS
Private Connectivity (Approval Required)	MPLS P2P VPLS SD-WAN Private WAN Data Center Cross-Connect



Note IOS Version for CUBE/vCUBE should support TLS 1.2.

- [Public Internet, on page 13](#)
- [Private Connectivity, on page 16](#)
- [Non-Standard Deployments, on page 18](#)

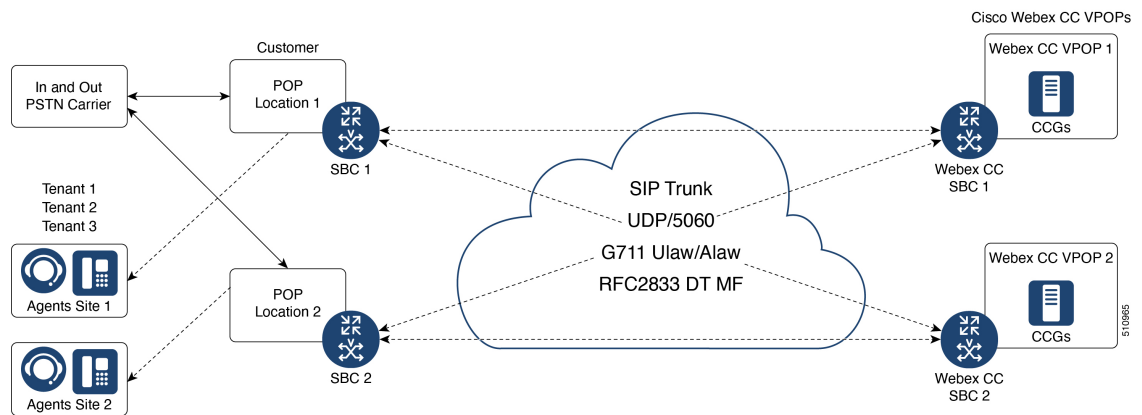
Public Internet

Direct SIP Trunk (Over the Top)

The customer's CUBE or SBC should be placed on a public IP. This is our recommended standard deployment model.

Pros	Cons
<ul style="list-style-type: none"> • Fastest to deploy • Inexpensive 	<ul style="list-style-type: none"> • Best effort • May not meet security requirements

Figure 7: Typical Direct Connection



As this is the most simplistic approach, it is also the least flexible. The benefits of a simplified topology are ease of management and troubleshooting. Network diagrams are completed by the customer and submitted to the Voice team, and dial-peers are created. Placing the CUBE in a DMZ alleviates the complexities of dealing with NAT. The CUBE itself is a firewall, and most medium/large providers place their CUBE in a public IP and use its security capabilities.

VPNs

A VPN is another type of connection that uses public internet. VPNs are often needed when a customer requires a secure connection for SIP and RTP. A VPN might also be required if the customer cannot place the CUBE in a public IP space. A provisioning meeting with Voice Engineering is required for VPN connections.

Pros	Cons
<ul style="list-style-type: none"> • Secured connection • No additional costs 	<ul style="list-style-type: none"> • Takes time to implement

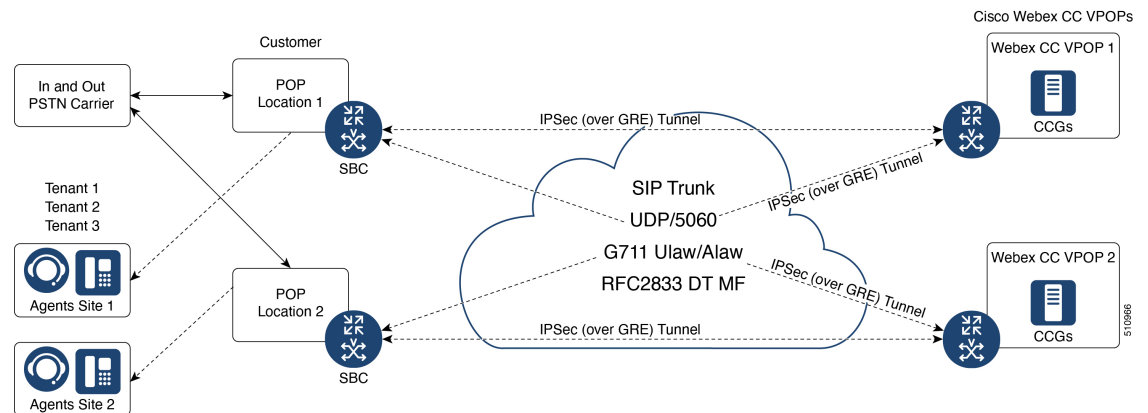
Voice Ports

- RTP: 8000 - 48199
- SIP: UDP 5060

IPSec VPN or IPSec over GRE

The following options are available for VPN Connectivity:

- SBC to SBC connectivity
- GW to GW connectivity

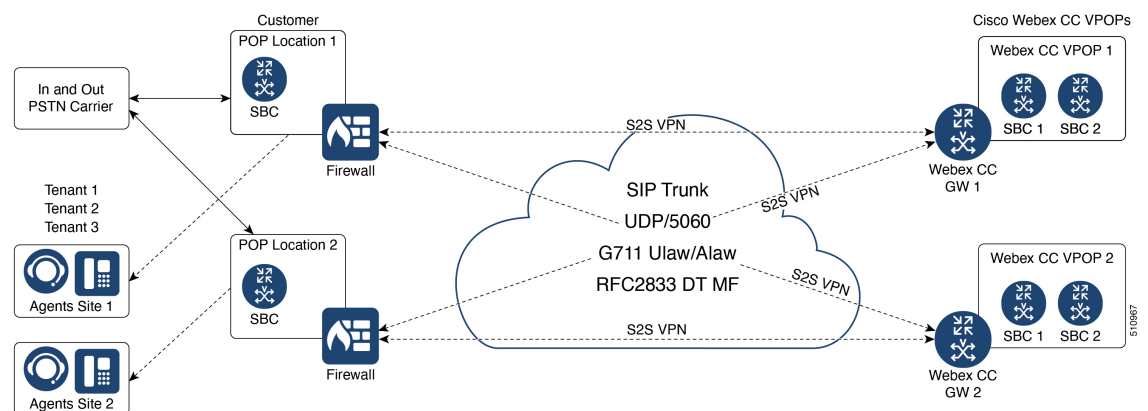
Figure 8: Typical IPsec or IPsec over GRE Tunnel

Webex Contact Center (IPsec or IPsec over GRE tunnel and Webex Contact Center S2S Connectivity) to use UDP/5060 instead of TCP/5060

An IPsec VPN or IPsec over GRE is a good option for a secure SIP Trunk when the CUBE is on a public IP. This is an SBC to SBC connection. (Fig 2) with VPN tunnels private IP address schemes must also be considered to avoid any overlap between customers. For GRE connections IP subnets are: 10.x.248.x and 10.x.249.x.

Site-to-Site (S2S)

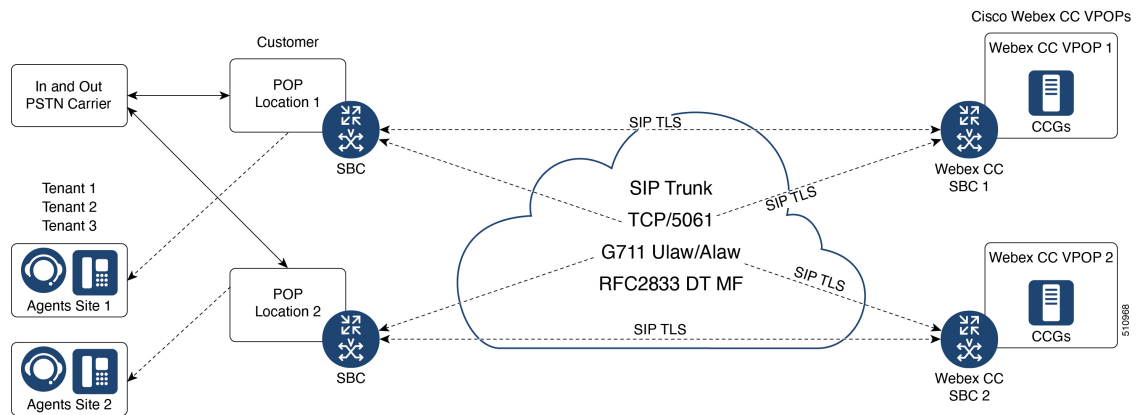
A S2S connection can be deployed if the customer needs a secure connection or cannot place the CUBE in a public IP. This is a gateway to gateway connection. There are no subnets specifically designated for S2S VPN connections as routing is based on interesting traffic without the involvement of a logical interface.

Figure 9: Typical Site-to-Site Connection

SIP TLS and SRTP

Using SRTP/SIP TLS is another option when the CUBE is on a public IP address. However, there is a performance hit for using SRTP/SIP TLS. A CUBE device can handle one-third of the SIP sessions if you have secured the calls using either TLS or SRTP. This is a SBC to SBC connection.

Figure 10: Typical SIP TLS and SRTP Connection



Public and Self-Signed Certificates

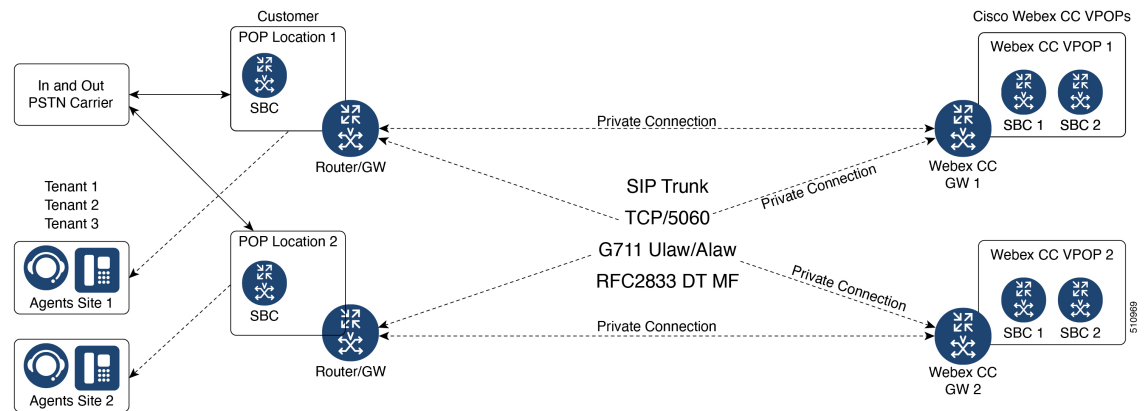
In order to establish a SIP TLS connection, it is necessary to exchange certificates. The following options are available:

- Self-signed certificates are generated and exchanged between the customer and Webex Contact Center.
- Public CA – the following steps need to be completed to support Public CA:
 - Customer needs to share the root certificate which will be loaded into the Webex Contact Center SBC.
 - Customer needs to update the DNS to include the IPs of the Webex Contact Center SBCs.

Private Connectivity

Often the connection choice of large enterprise providers, a direct connection provides a dedicated and secure circuit. If the customer needs a direct connection, the customer can be provided with the *Cisco Webex Contact Center VPOP Circuit Order Guidelines* document as the initial step, and a follow-up design meeting with the Webex Contact Center Voice Engineering team and the customer engineers needs to be conducted as the next step. The customer needs to provide a detailed network diagram of the customer's voice network including PSTN carrier interconnects for the meeting. Cisco will not host any customer equipment.

Figure 11: Typical Private connection



Irrespective of whether the customer chooses MPLS, P2P, VPLS, or SD-WAN, the topology will look similar and all circuits will terminate to Webex Contact Center router/GW and not to Webex Contact Center CUBEs.

The bandwidth requirements for a direct connect is based on the G.711 codec (~100kbps per call leg), allowing for two call legs per session.

Pros	Cons
<ul style="list-style-type: none"> • High reliability • Dedicated bandwidth 	<ul style="list-style-type: none"> • A direct connection is the most expensive • Longest time to implement

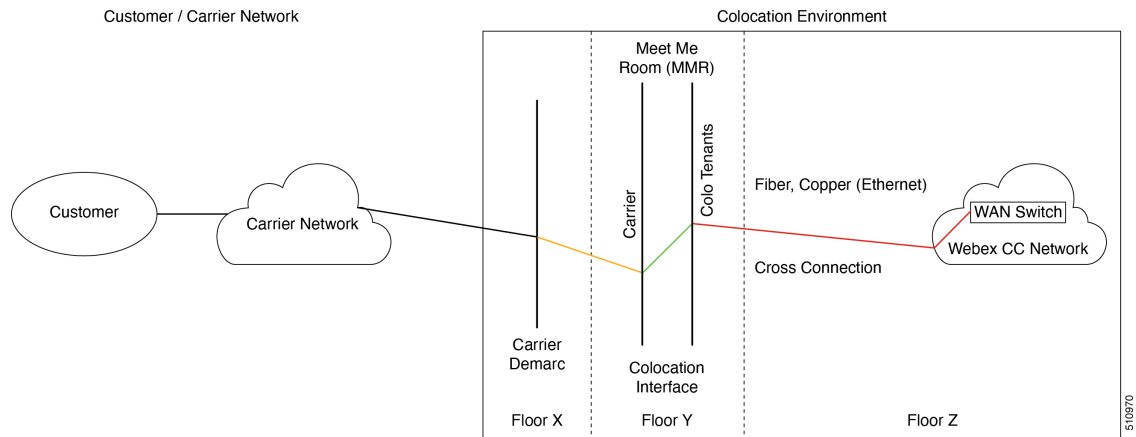
Data Center Cross Connect

If a customer decides on a private connection, it will be necessary to order data center cross connects as described in the *Cisco Webex Contact Center VPOP Circuit Order Guidelines* document. The customer will be responsible for the cost incurred and for getting the customer's circuit to the designated drop. (Fig 6.)



Note

The *Cisco Webex Contact Center VPOP Circuit Order Guidelines* document will be provided to the customer directly during the on-boarding process in case this connectivity option is preferred.

Figure 12: Typical Data Center Cross Connect

Non-Standard Deployments

Non-Standard Deployments

If the recommended topologies do not meet all the requirements of the customer's network, a design meeting must be scheduled with the Cisco Voice Engineering team via the customer's Cisco account team for a special approval process. The following are examples of non-standard deployments and deployments that are not recommended:

A2Q Exceptions

PSTN Provider terminating the circuit directly to Webex Contact Center VPOP.

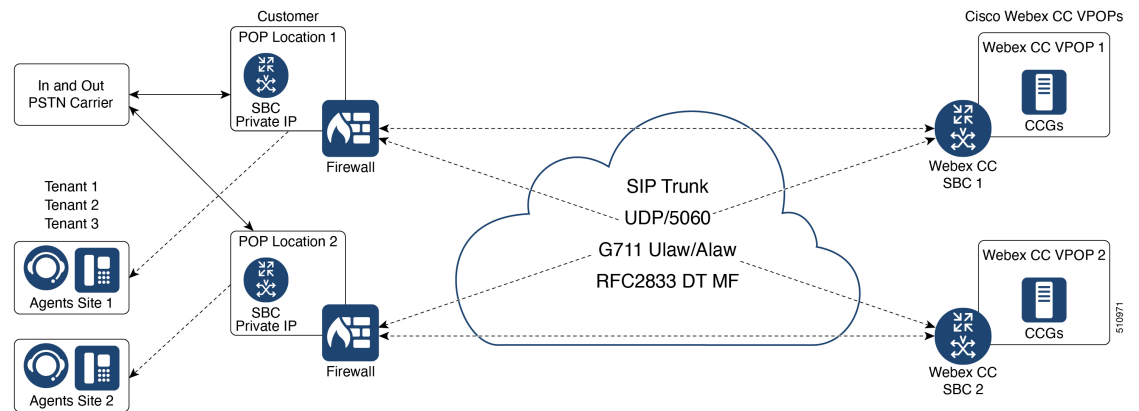
Gold Tenant Exceptions

We strongly recommend a direct SIP Trunk for Gold Tenant customers. This is the over-the-top topology of placing the CUBE in a public IP space. The need for a Gold Tenant often exists with larger providers; however, the provider requires the Gold Tenant to be a proof of concept for the provider's intended production deployment. The proof of concept Gold Tenant often exceeds using open internet access for a SIP Trunk and would require one of the previously discussed connection types.

Gold Tenant customers will not be monitored.

Public Internet – CUBE Behind Firewall

Placing a CUBE on a private IP address behind a NAT firewall is another deployment option. The security requirements from the customer's IT department can stipulate to have the voice application behind a firewall. This option has a few known drawbacks. Even though this may not cause issues in the network layer, it may result in issues in the SIP application layer. The private IP address is used within the SIP messages, which causes call processing failures. Firewall capacity is another factor to be considered for this type of deployment. Firewalls must be sized appropriately to handle VoIP traffic; the firewall may otherwise become a bottleneck and can impact call quality and call processing.

Figure 13: Typical Cube Behind Firewall

The following are the disadvantages of this deployment:

- Possible CUBE configuration and setup issues at the beginning.
- Increased load on firewall that could impact voice quality.
- The customer is responsible for CUBE setup and firewall sizing.
- Not a recommended topology due to impact on SLAs.



Note

This topology is not recommended due to the complexities of dealing with SIP and NAT. A meeting with the Cisco Voice Engineering team and the customer is required for approval of this type of deployment.



CHAPTER 5

Component Redundancy

Component redundancy allows Webex Contact Center to provide resilience when there is a service outage. You can configure both Webex Contact Center cloud and enterprise CUBE to be redundant:

- Within a geographic region—You can set up more than one POP within an enterprise.
- Across enterprise data centers within a geographic region.
- Within enterprise networks—You can also set up CUBE in high availability (HA) mode. HA mode preserves oth signaling and media.

All signaling and media are sourced to and from the virtual IP address.

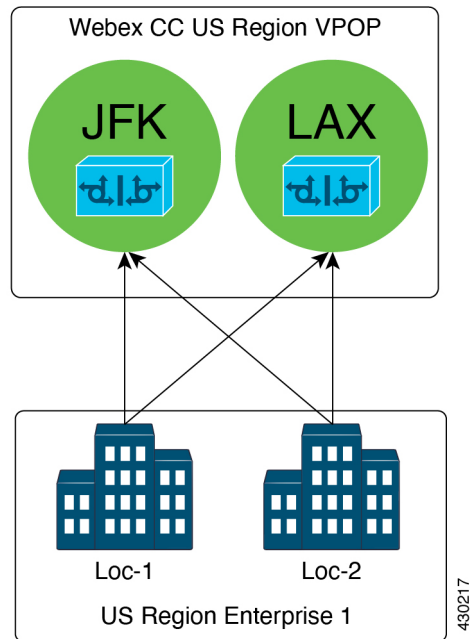
Webex Contact Center uses two VPOPs to ensure high availability. For optimal performance, the service provider should also set up two POPs. This ensures that the hunting between the Webex Contact Center VPOPs is an even round robin.

- [Redundancy Across Enterprise Data Centers Within a Geographic Region, on page 21](#)

Redundancy Across Enterprise Data Centers Within a Geographic Region

Configure two data centers within the enterprise to connect to the same Webex Contact Center VPOPs, within the same geographic region.

Figure 14: Redundancy Across Enterprise Data Centers Within a Geographic Region





CHAPTER 6

Enterprise CUBE to Webex Contact Center Configuration Example

This configuration example applies to the Cisco IOS Voice Gateway and the Cisco UBE Voice gateway. For complete CUBE configuration instructions, see the [Cisco Unified Border Element Configuration Guide](#). All configurations in this example use global configuration mode. To enter global configuration mode:

1. Enter `enable` to enter privileged EXEC mode.
2. Enter `configuration terminal` to enter global configuration mode.

- [Basic Configuration, on page 23](#)
- [Common Configuration, on page 24](#)

Basic Configuration

SIP Timers (MIN-SE has been set to 3600 across all VPOPs in Webex Contact Center. This can either be updated globally or modified in the Invite towards Weber Contact Center):

```
voice service voip
```

```
Sip
```

```
Min-se 3600
```

Configure Voice Codec Class

```
voice class codec 100
```

```
codec preference 1 g711alaw
```

```
codec preference 2 g711ulaw
```

Inbound dial-peer for calls from Weber Contact Center

```
dial-peer voice 200 voip
```

```
session protocol sipv2
```

```
voice-class codec 100
```

```
dtmf-relay rtp-nte
```

```
no vad
```

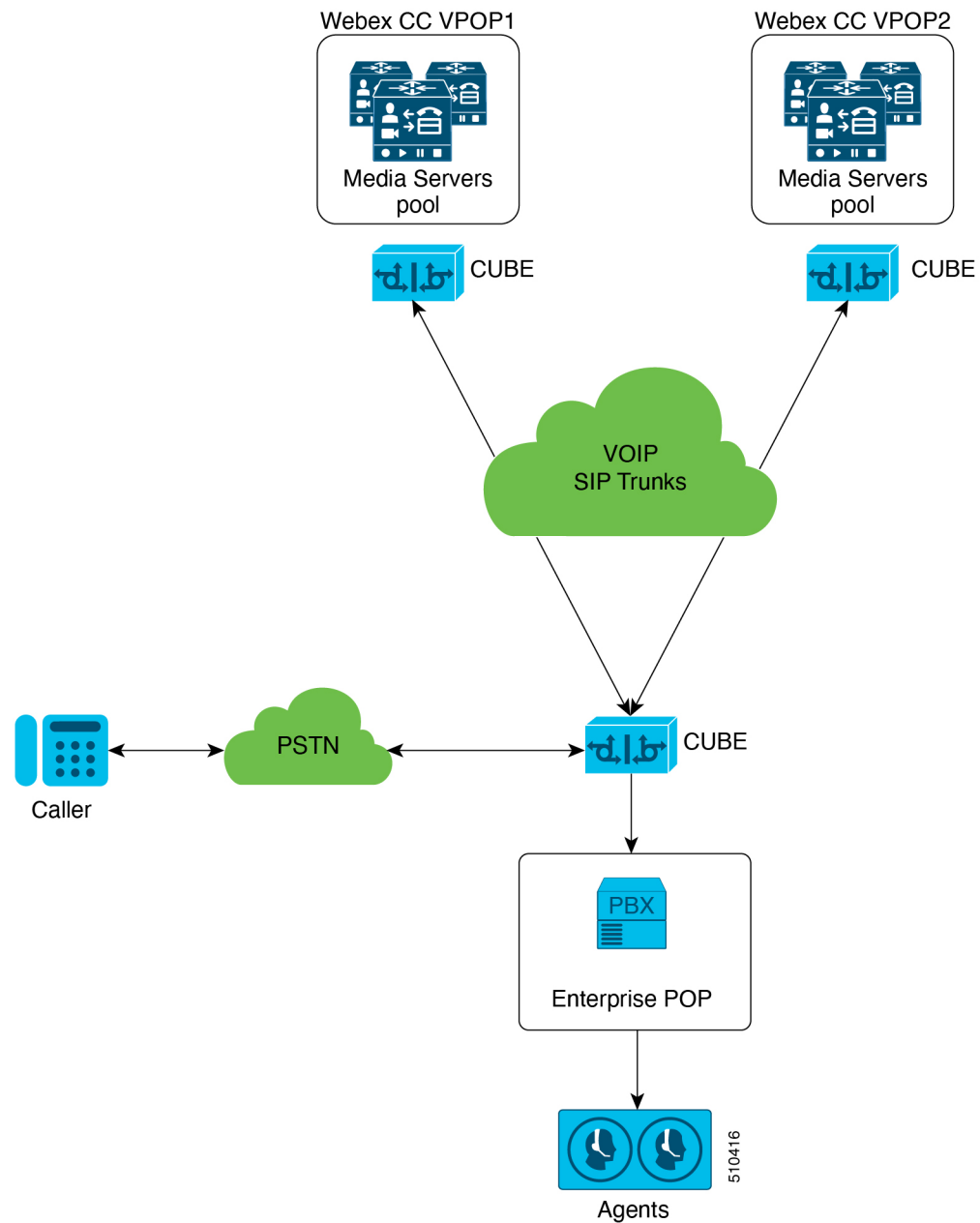
Outbound dial-peer for calls to Webex CC

```
dial-peer voice 100 voip
destination-pattern <Pattern towards Webex CC>
session protocol sipv2
session target ipv4:<Webex CC SBC IPs>
voice-class codec 100
voice-class sip options-keepalive
dtmf-relay rtp-nte
no vad
```

Common Configuration

This example shows Webex Contact Center trunk provisioning in USA with this topology:

Figure 15: Trunk Provisioning for Webex Contact Center



Setup details:

- Configure SIP Keepalive Options
- New dial peers with target destination IP address Webex CC LAX and JFK CUBEs.
- Dial-peer preference can be either setup to round robin or primary and secondary
- Codec is setup for G711ulaw and G711alaw (connections outside US). DTMF is RFC2833.

- SIP Communication is over UDP port 5060 and RTP port 8000 - 48199.
- Dial plan where the destination pattern matches Webex Contact Center to agents through PBX and PSTN.
- More than one POP for high availability.
- MIN SE timer on Webex CC is 3600; session timers should either be updated to this value or should allow SIP negotiation to this value during a call setup.

**Note**

If you are using CUBE/vCUBE, it is recommended to use an IOS version which supports TLS 1.2.



CHAPTER 7

Secure SIP Trunk Between CUBE and Webex Contact Center

This example demonstrates how to configure a SIP Transport Layer Security (TLS) connection between Cisco Unified Border Element (CUBE) and Webex Contact Center.

- [Example Configure SIP TLS, on page 27](#)

Example Configure SIP TLS

Before you Begin

Ensure that:

- The endpoints have the same date and time. You can synchronize endpoints by using a Network Time Protocol (NTP) server.
- You have TCP connectivity.
- The CUBE has the security and UCK9 licenses installed.

1. Create a trustpoint to hold the self-signed certificate of the CUBE:

```
crypto pki trustpoint CUBEtest(can be any name)
enrollment self-signed
serial-number none
fqdn none i
p-address none
subject-name cn= ISR4451-B.cisco.lab !(match the hostname of the router)
revocation-check none
rsakeypair ISR4451-B.cisco.lab !(match the hostname of the router)
```

2. Generate a self-signed certificate:

```
crypto pki enroll CUBEtest

% The fully-qualified domain name will not be included in the certificate

Generate Self Signed Router Certificate? [yes/no]: yes
```

3. Export the certificate:

```
crypto pki export CUBEtest pem terminal
```

4. Copy the self-signed certificate that you exported and save it as a text file with the `.pem` file extension.
5. Upload the self-signed CUBE certificate to Webex Contact Center:
6. Copy the certificate from Webex Contact Center:
7. Upload the Webex Contact Center certificate to CUBE:

```
crypto pki trustpoint HOSTNAME  
enrollment terminal  
revocation-check none  
crypto pku authenticate HOSTNAME
```

(PASTE THE CJP CERT HERE AND THEN PRESS ENTER TWICE)

Enter `yes` when you are prompted to accept the certificate.

8. Configure SIP to use the self-signed certificate trustpoint that you created in step 1:

```
crypto signaling default trustpoint CUBEtest
```

9. Configure the dial peers with transport layer security:

```
voice class sip-options-keepalive 100  
transport tcp tls  
dial-peer voice 9999 voip  
answer-address 35..  
destination-pattern 9999  
session protocol sipv2  
session target ipv4:<Webex CC SBC IPs>  
session transport tcp tls  
voice-class sip options-keepalive profile 100  
srtp
```



CHAPTER 8

Configure SIP Trunk for Your Tenant

- [Before you Configure, on page 29](#)
- [Provision Your Tenant, on page 29](#)
- [Webex Contact Center Regions, on page 29](#)

Before you Configure

- Ensure that you have the Gold partner tenant and access to the Service Provider Portal.
- Configure the enterprise session border controller. For more information, see the [Cisco Unified Border Element Configuration Guide](#).
- Obtain a destination address for your SIP Trunk. For more information, see the [SIP Binding for CUBE](#).

Provision Your Tenant

Cisco uses the provisioning information that you provide to configure the Webex Contact Center session border controller for your tenant. Make sure that the information you provide matches your order, and is accurate. For instructions to provision your tenant, see the [Cisco Webex Contact Center Management Portal User Guide](#) or the [Cisco Customer Journey Platform Service Provider Portal User Guide](#).

- Configure a SIP trunk that connects your customer's IP address to the configured border controller. Make sure that you select **CUBE** as your SIP Trunk Type. Configure a SIP trunk for each CUBE that you deploy.
- Create and provision a tenant.
- Assign SIP trunk to the tenant, add dial numbers, and provision your new tenant.

Once the tenant is provisioned and the Webex Contact Center CUBE is configured, you will receive an email that the tenant is ready for use.

Webex Contact Center Regions

VPOP is currently available by region for tenant connection as follows:

- US: Los Angeles and New York

- Europe: London, Amsterdam, Frankfurt
- Canada: Toronto and Vancouver
- Australia: Sydney and Melbourne
- Japan: Tokyo and Osaka