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 Equinix Fabric Connections

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

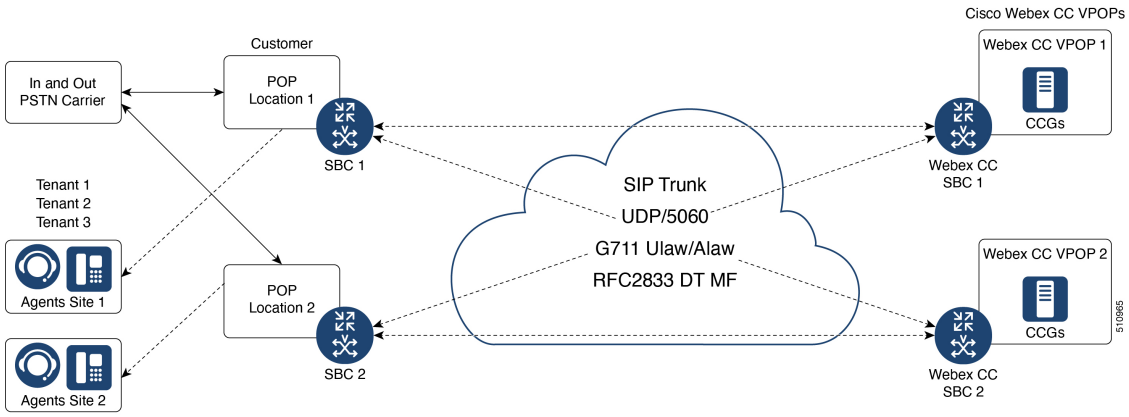
Public Internet

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
• Fastest to deploy • Inexpensive	• Best effort • May not meet security requirements

Figure 1: 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
• Secured connection • No additional costs	• Takes time to implement

Voice Ports

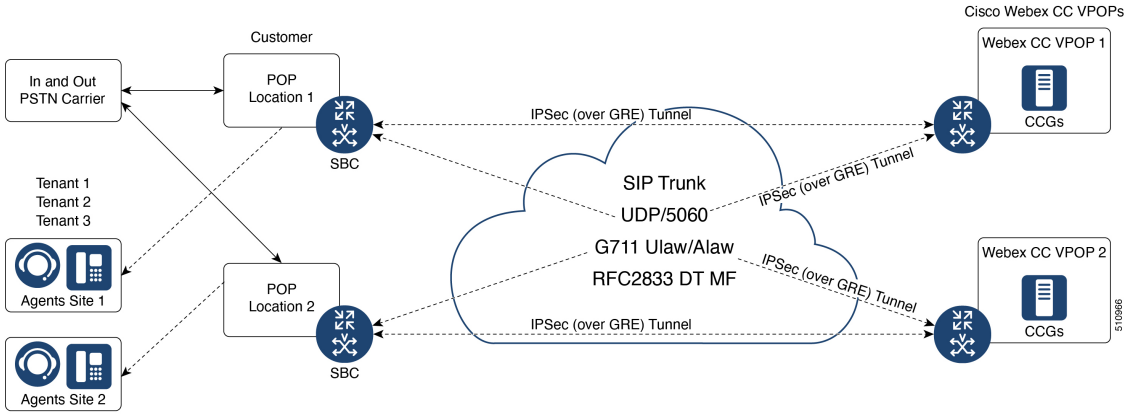
- RTP: 8000 - 48199
- SIP: UDP 5060

IPSec VPN or IPSec over GRE

The following options are available for VPN Connectivity:

- SBC to SBC connectivity
- GW to GW connectivity

Figure 2: Typical IPsec or IPSec over GRE Tunnel



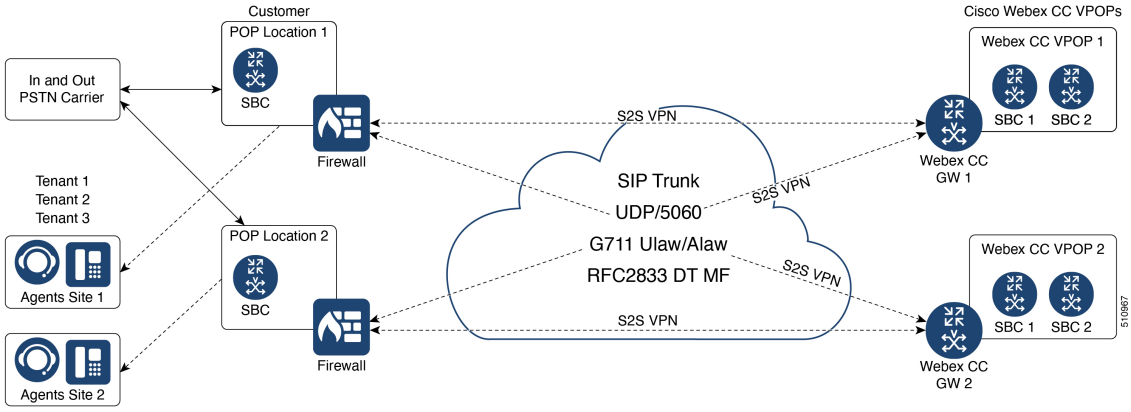
Webex Contact Center (IPSec or IPSec over GRE tunnel and Webex Contact Center S2S Connectivity) to use UDP/5060 instead of TCP/5060

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 (*Figure 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.

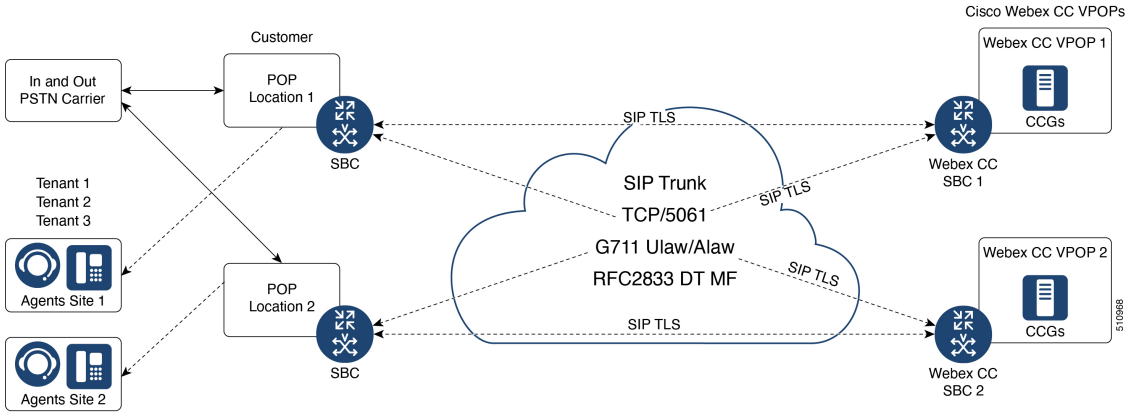
Figure 3: Typical Site-to-Site Connection



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 4: 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:

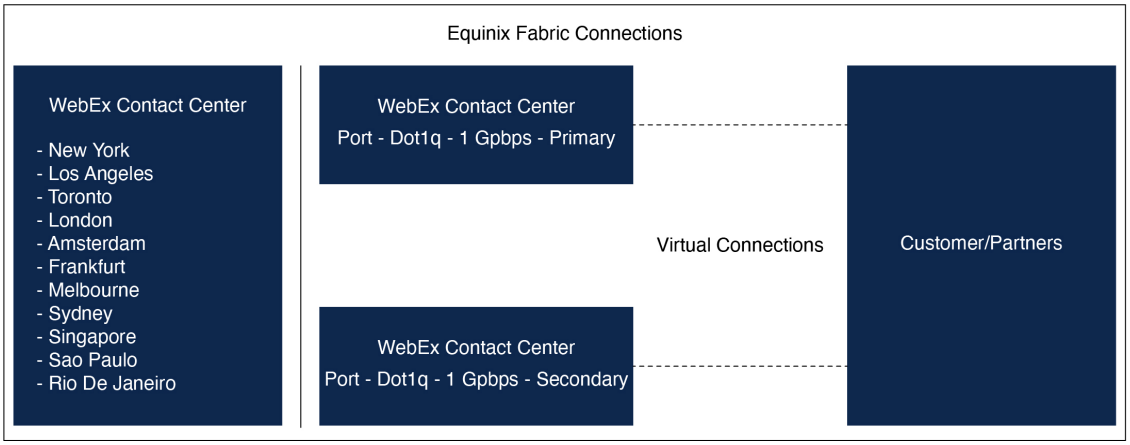
- Self-signed certificates are generated and exchanged between the customer and Webex Contact Center.
- Public CA – the following steps need to be completed to support Public CA:
  - Customer needs to share the root certificate which will be loaded into the Webex Contact Center SBC.
  - Customer needs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

Private Connectivity

Large enterprise providers often prefer a direct connection, because it 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. As the next step, a follow-up design meeting with the Webex Contact Center Voice Engineering team and the customer engineers has to be conducted. The customer has 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.

Cisco Webex Contact Center also offers Equinix Fabric connections for customers who have colocations with Equinix.

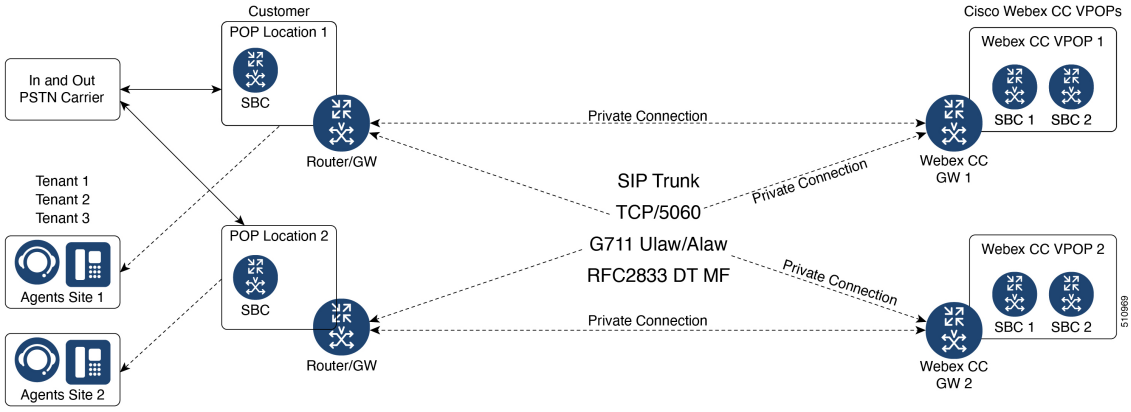
Figure 5: Equinix Fabric Connections



For more information on Equinix Fabric, see:

- *https://fabric.equinix.com/dashboard*
- *https://www.equinix.com/interconnection-services/equinix-fabric/provider-availability*

Figure 6: 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 in Webex Contact Center router/GW (gateway) and not in Webex Contact Center CUBEs.

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

Pros	Cons
• High reliability • Dedicated bandwidth	• A direct connection is the most expensive • Longest time to implement

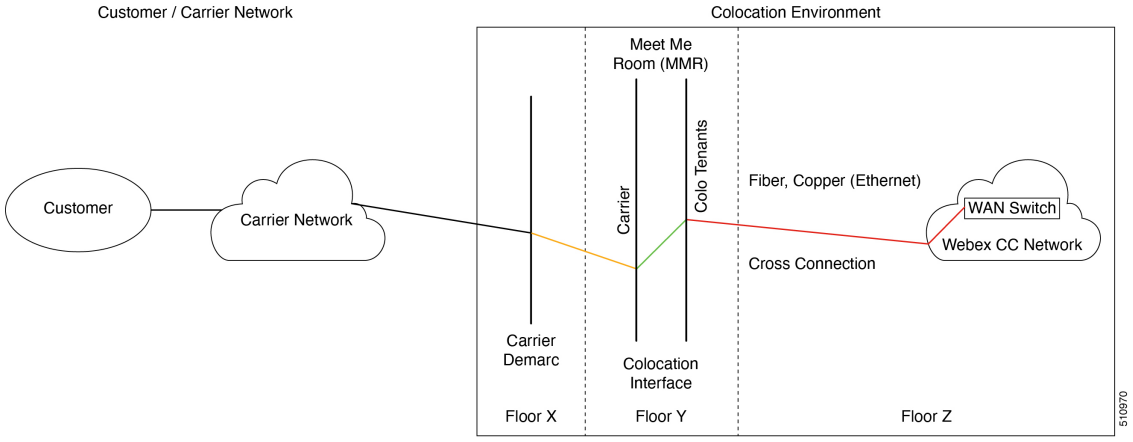
Note Equinix Fabric connections offer port redundancy, faster virtual connection ordering, and provisioning. We recommend using Equinix connection, rather than using other private connection methods.

Data Center Cross Connect

If a customer decides to use 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 *(Figure 6)*.

Note The *Cisco Webex Contact Center VPOP Circuit Order Guidelines* document will be provided to the customer directly during the onboarding process, if the customer opts for a private connection.

Figure 7: 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

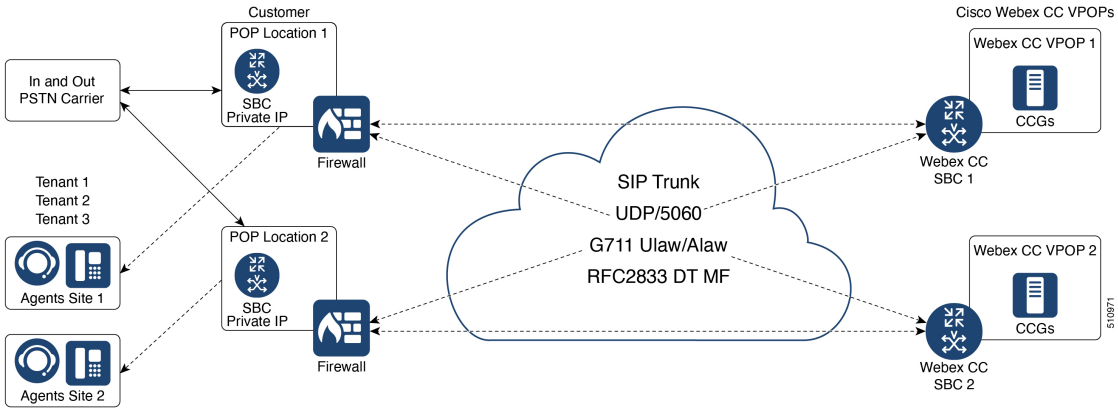
deployment. The proof of concept Gold Tenant often exceeds using open internet access for a SIP Trunk and would require one of the previously discussed connection types.

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 8: 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.