# Let's go

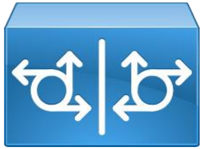
The bridge to possible

# High-Capacity Premises-based PSTN Option for Webex Calling

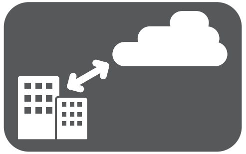
Hussain Ali, Technical Marketing Engineer
linkedin.com/in/hussaincube

# Additional sessions on IOS-XE UC (CUBE, Local Gateway, Survivability Gateway)

- BROCOL-2314 CUBE v14 Updates
- Session Room A4 – Tuesday 1:45PM – 2:45PM



- BRKCOL-2312 High-Capacity Premises-based PSTN Option for Webex Calling
    - Session Room A1 – Wednesday 2:30PM – 3:30PM
- Walk-in-Lab: LABCOL-2417 Local Gateway for Webex Calling



- BRKCOL-2993 Enabling Site Survivability for Webex Calling
    - Session Room A9 – Thursday 10:30AM – 11:30AM
- Walk-in-Lab: LABCOL-2416 Site Survivability for Webex Calling

# Agenda

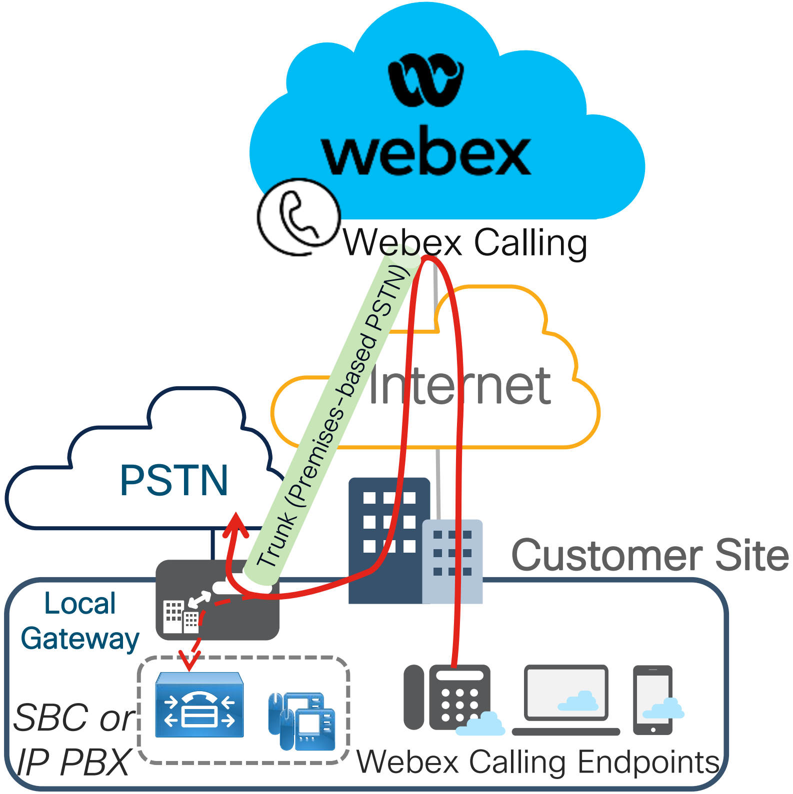
- Local Gateway (LGW) overview and sizing
- Multiple Registration-based LGWs on a single CUBE
- Validate Registration-based LGW Configuration through Control Hub
- Introducing Certificate-based Local Gateway
- Configuring a Certificate-based Local Gateway
- 3rd Party SBC as a Local Gateway
- Resources

# Local Gateway (LGW)

## Overview and Sizing

# Webex Calling Trunk - Local Gateway

## (Premises-based PSTN) Deployment




- Provides connectivity to a customer-owned premises-based PSTN service
- May also provide connectivity to an on-premises IP PBX or dedicated SBC/PSTN GW
- Enables on-prem to Webex Calling transition
- **Endpoint registration is NOT proxied through Local Gateway, unlike CUBE Lineside.** Endpoints directly register to Webex Calling over the Internet.

# IOS-XE Software Release Mapping

| CUBE Version | Initial IOS-XE Release for this CUBE version and Release date | | Subsequent IOS-XE Release for this CUBE version |
|---|---|---|---|
| 14.1 | 17.3.2* | Oct 2020 | 17.3.8a |
| 14.2 | 17.4.1a | Nov 2020 | 17.4.2 |
| 14.3 | 17.5.1 | March 2021 | 17.5.1a |
| 14.4 | 17.6.1a | July 2021 | 17.6.6a |
| 14.4 | 17.7.1a | Nov 2021 | 17.7.2 |
| 14.5 | 17.8.1a | March 2022 | |
| 14.6 | 17.9.1a | July 2022 | 17.9.4a |
| 14.6 | 17.10.1a | Nov 2022 | |
| 14.6 | 17.11.1a | March 2023 | |
| 14.7 | 17.12.1a | July 2023 | 17.12.2 |
| 14.8 | 17.13.1a | Nov 2023 | |
| 14.9 | 17.14.1a | March 2024 | |

Last release for ISR4K except ISR4461

# Local Gateway Trunking models

# Local Gateway Trunking Models

- There are two types of Local Gateway trunking models:
  - Registration-based trunks
  - Certificate-based trunks
- Both models provide similar functionality, but they differ in scale and device support

# Comparing Local Gateway trunking models

| Functionality | Registration-based | Certificate-based |
|---|---|---|
| Concurrent Calls | Concurrent calls of up to 250 per trunk (OTT Internet) | Greater than 250 concurrent calls per trunk |
| Device Type | Supports only CUBE (except ASR1000 series) | Supports all CUBE and 3rd party SBCs |
| Authentication model | Digest-based authentication model, which relies on a shared username and password used to authenticate registration and calls. | Certificate-based authentication model |
| Public DNS service requirements | None | Domain claims required.<br><br>A DNS A or SRV record must be configured in public DNS server |

# Network, firewall, and NAT requirements

| Registration-based | Certificate-based |
|---|---|
| Any NAT or Public IP is supported.<br>• Dynamic NAT is preferred since it’s easier for setup and requires less firewall configs<br><br>For ingress traffic, inbound pinholes(from WxC to LGW) are opened by the firewall based on outbound registration messages<br><br>Pinhole opening is recommended for all Webex Calling IP address and ports. | Public internet-facing network including a public IP or Static NAT. |

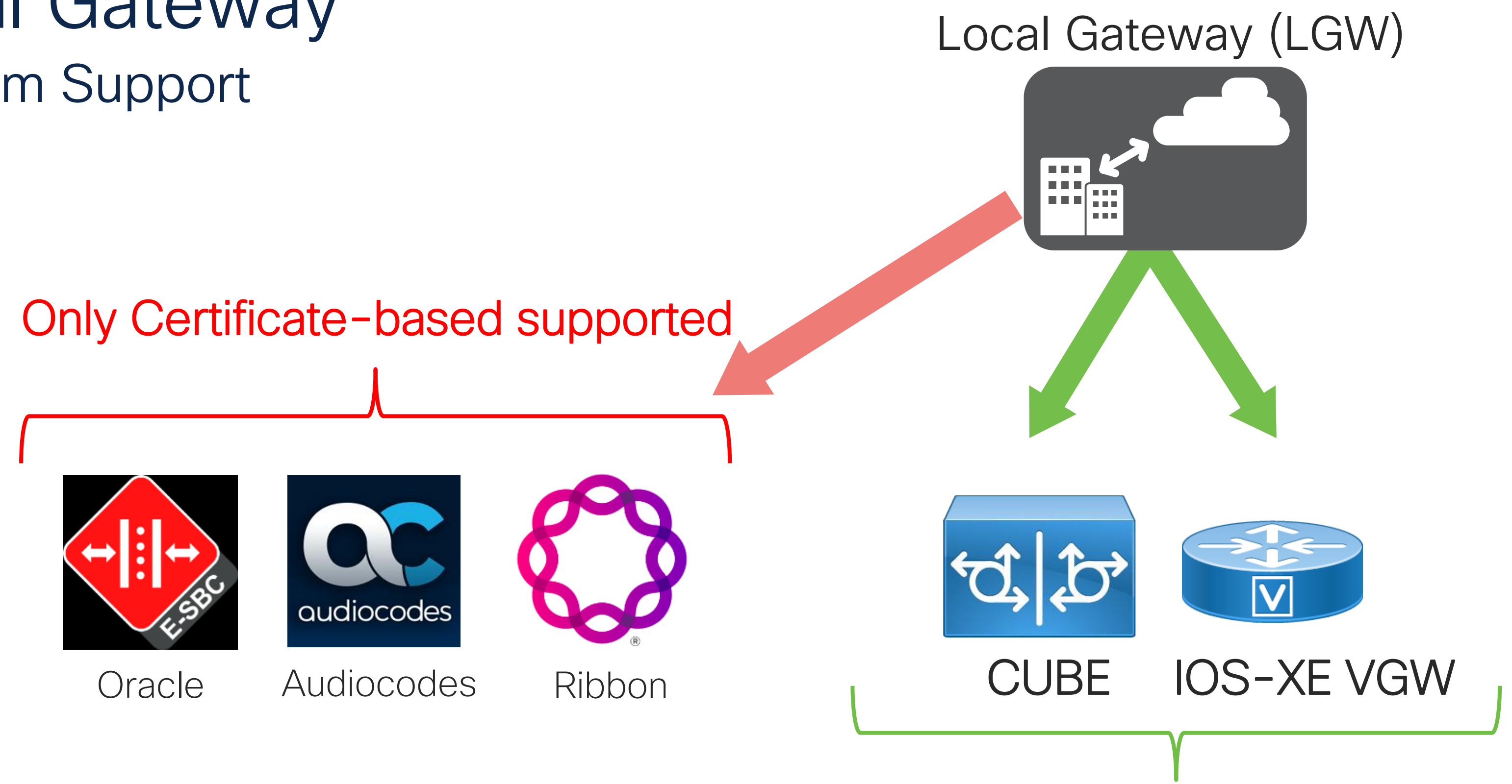
Both requires firewall to allow both ingress and egress traffic (Webex calling to Local Gateway and vice versa).

# CA and certificate requirements

| Registration-based | Certificate-based |
| --- | --- |
| | Local gateway must have a signed certificate using one of the certificate authorities listed in Root Certificate Authorities.<br><br>• Wild-card certificates are not supported<br>• Certificates must be signed per guidelines as mentioned in Configure Trunks, Route Groups, and Dial Plans for Webex Calling |

CA bundle that signed the Webex service's certificate has to be uploaded to the Local Gateway.

# Local Gateway
## Platform Support

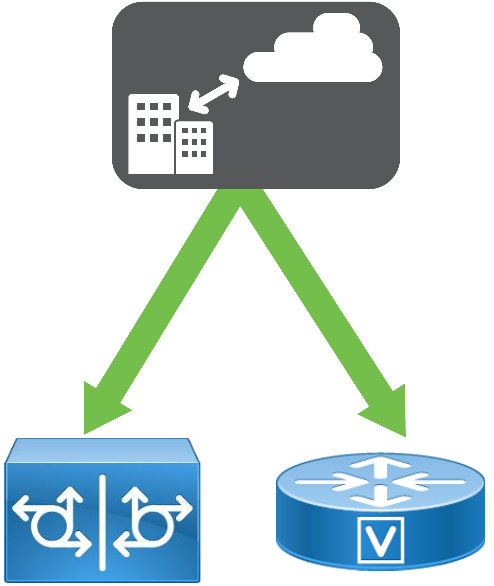



- AnyNode and Netmatch SBCs coming soon

# CUBE as Local Gateway

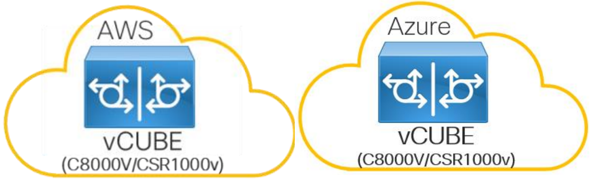
## Platform Support

Local Gateway (LGW)



CUBE IOS-XE voice GW

- **Cisco CUBE** (for IP-based connectivity) or Cisco IOS Gateway (for TDM-based connectivity)
- Hardware and software requirements:
  - ISR 4321, 4331, 4351, 4431, 4451, 4461 (IOS-XE 17.9.4a / 17.12.2)
  - vCUBE in AWS, Azure




  - Catalyst 8200/8300 series (IOS-XE 17.9.4a / 17.12.2)
  - CSR 1000v (vCUBE) (IOS-XE 17.3.8a)
  - Catalyst 8000v Edge (vCUBE) (IOS-XE 17.9.4a / 17.12.2)
    - C8000v/CSR 1000v licenses are not included in Webex Calling Flex and need to be purchased separately
    - Estimate 200 kbps total data throughput for every audio call
  - ISR 1100 (IOS-XE 17.9.4a / 17.12.2)

# Calling Capacity requirements

- Registration-based and Certificated-based trunking models have different concurrent call capacities as shown below

| Concurrent calls per local gateway / trunk | Trunk type Preference | Minimum Link Quality |
|---|---|---|
| ~ 2000-6500 | Certificate-based | Interconnect |
| 250 to ~ 2000 | Certificate-based | Over the top Internet (OTT) |
| up to 250 | Registration-based | OTT |

# Connection qualifications

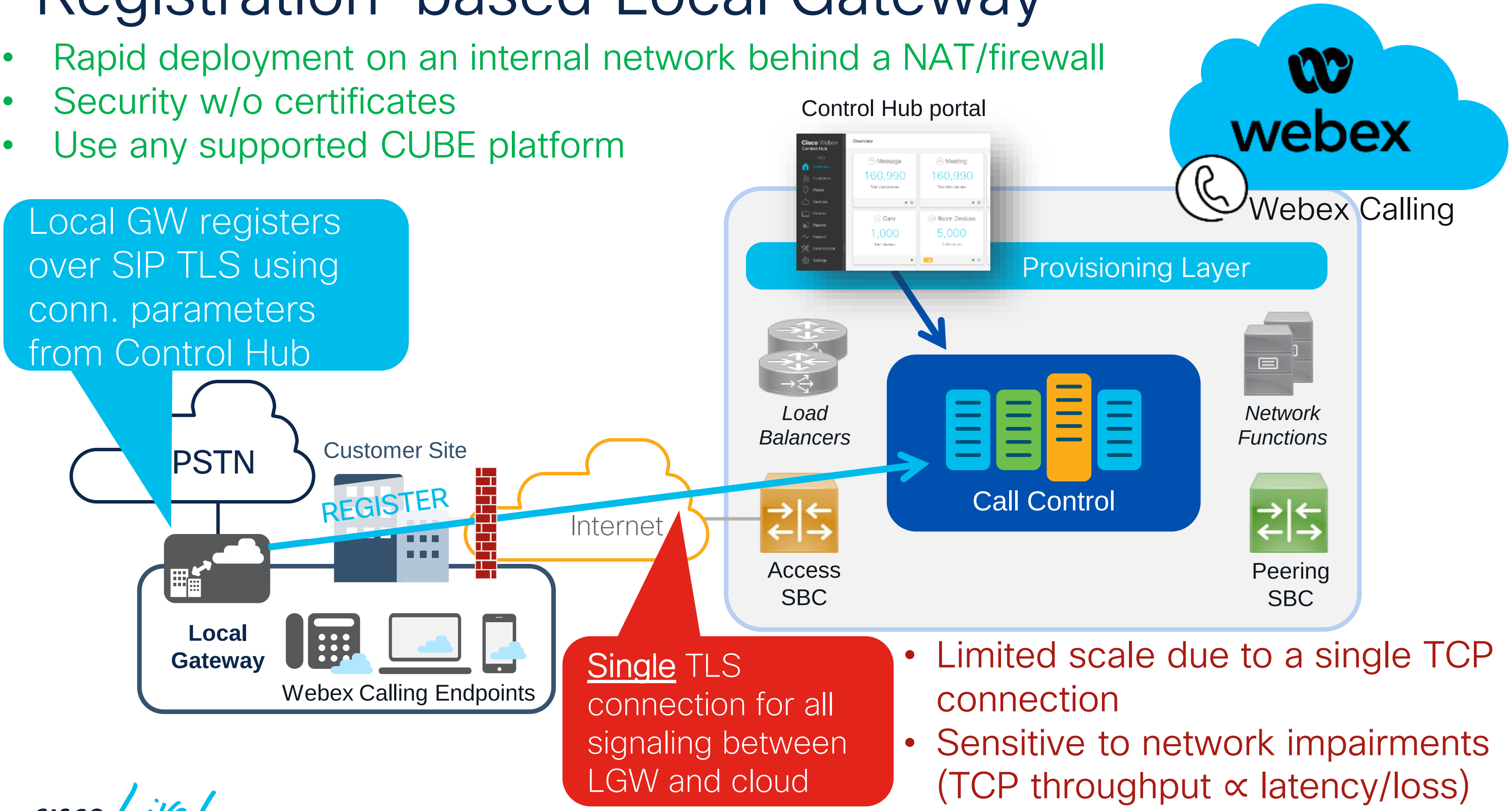
- Over the top (OTT) Internet and interconnect (e.g. Webex Edge Connect) must meet the following link quality conditions

| Connection Type | Latency | Jitter | Packet loss |
|---|---|---|---|
| OTT | 100 ms (max) | 100 ms (max) | 0.2% |
| Interconnect | 30 ms | 5 ms | Zero packet loss |

# Multiple Registration-based LGWs on a single CUBE

# Registration-based Local Gateway

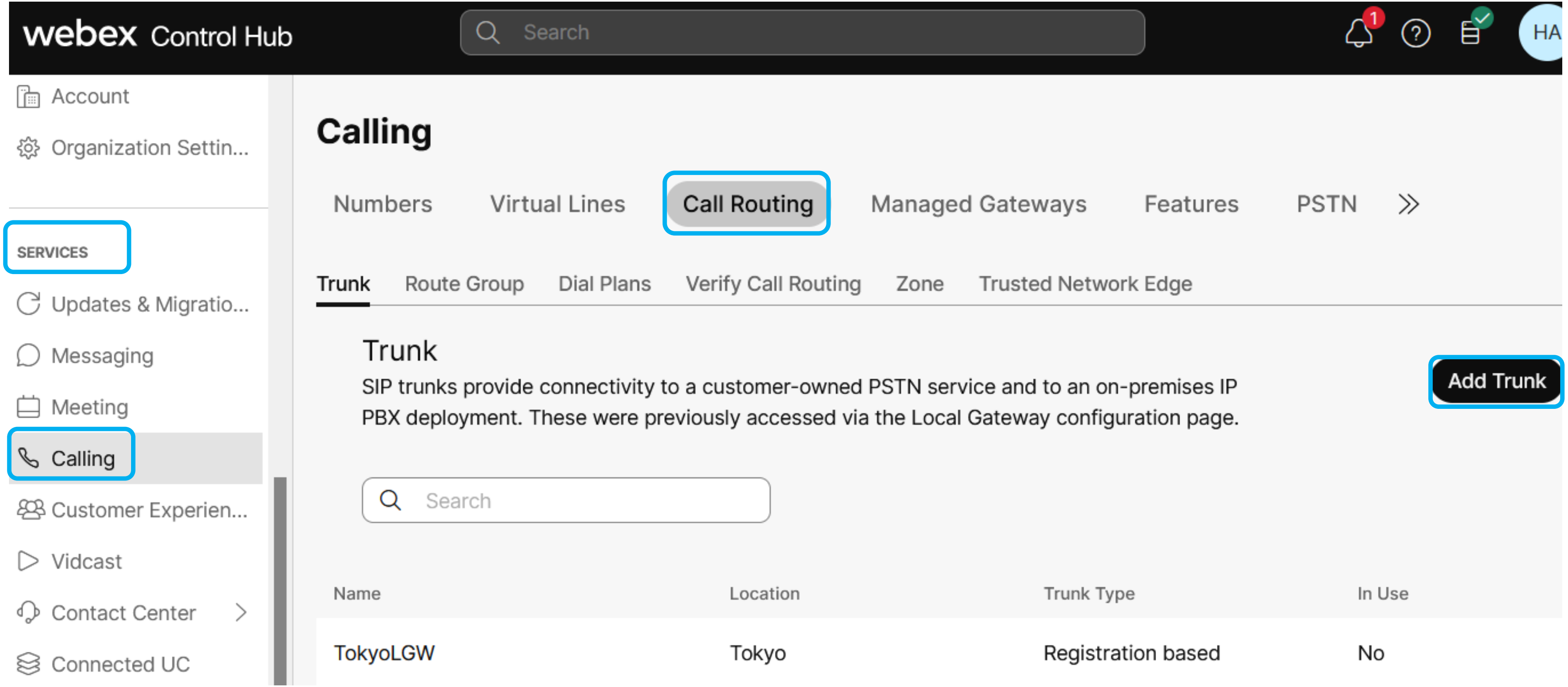
- Rapid deployment on an internal network behind a NAT/firewall
- Security w/o certificates
- Use any supported CUBE platform



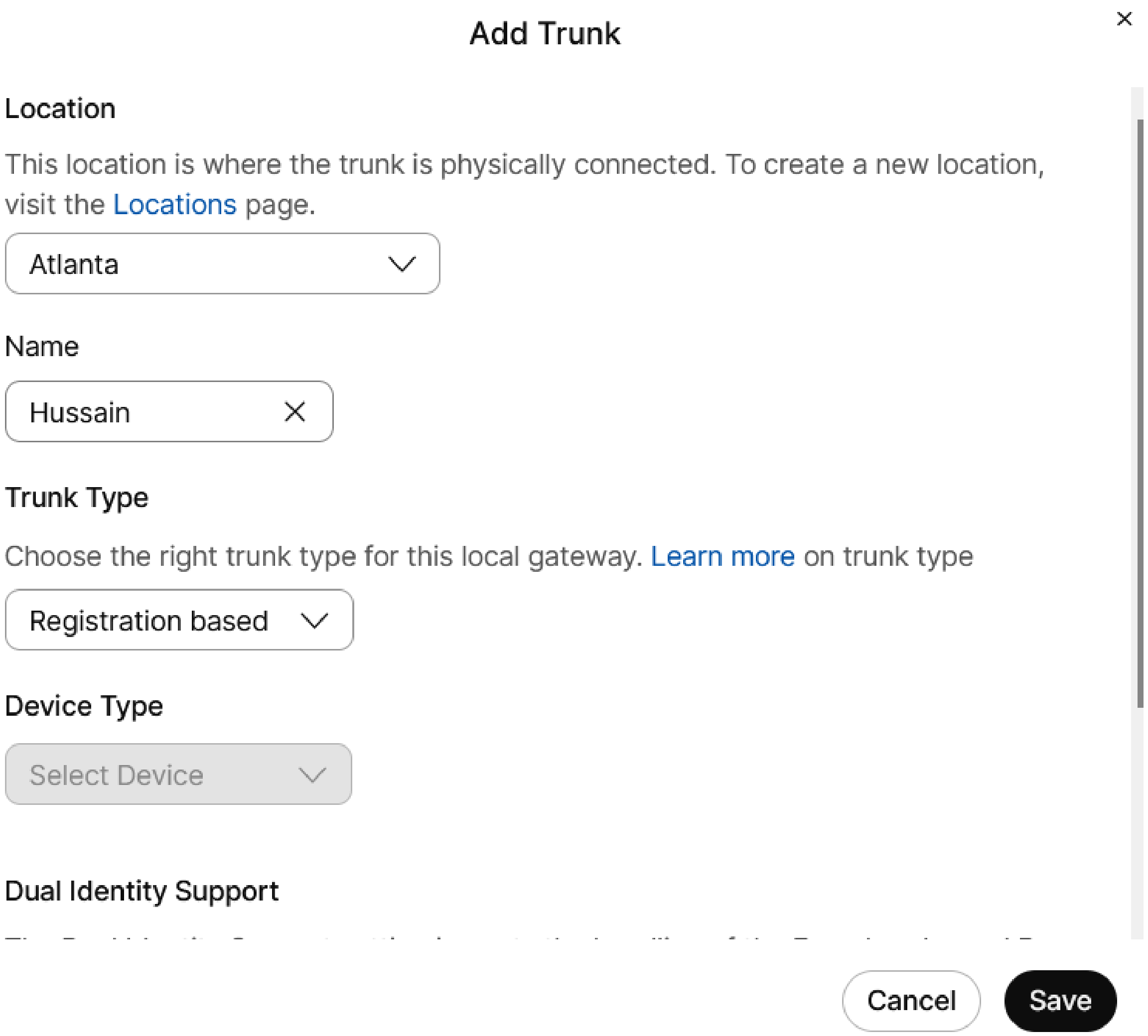

- Limited scale due to a single TCP connection
- Sensitive to network impairments (TCP throughput ∝ latency/loss)

# Onboarding Process
# Webex Calling Trunk

# Log in to Control Hub. Navigate to Services – Click Calling and then go to the Call Routing Tab. Click Add Trunk.



# Add a new Trunk for the desired Location




- Trunk name is limited to 24 characters

# Save the Trunk parameters to build the CUBE CLI for LGW

Parameters on this display required for building LGW CLI

## Add Trunk

Hussain Successfully Created.

Visit Route Group page to add trunk(s) to a route group.

Visit Locations page to configure PSTN connection to individual locations.

Visit Dial Plans page to use this trunk as the routing choice for a dial plan.

### Trunk Info

**Status**

unknown

**Trunk Group OTG/DTG**

hussain2572_lgu

**Outbound Proxy Address**

la01.sipconnect-us10.cisco-bcld.com

**Registrar Domain**

40462196.cisco-bcld.com

**Line/Port**

Hussain6346_LGU@40462196.cisco-bcld.com

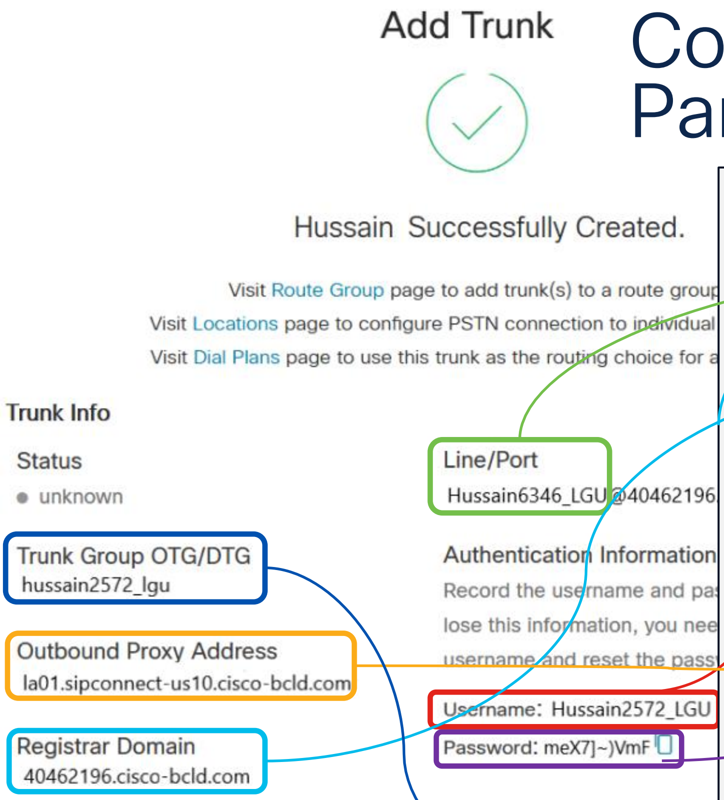
**Authentication Information**

Record the username and password below. If you lose this information, you need to retrieve the username and reset the password.

Username: Hussain2572_LGU

Password: meX7]~)VmF

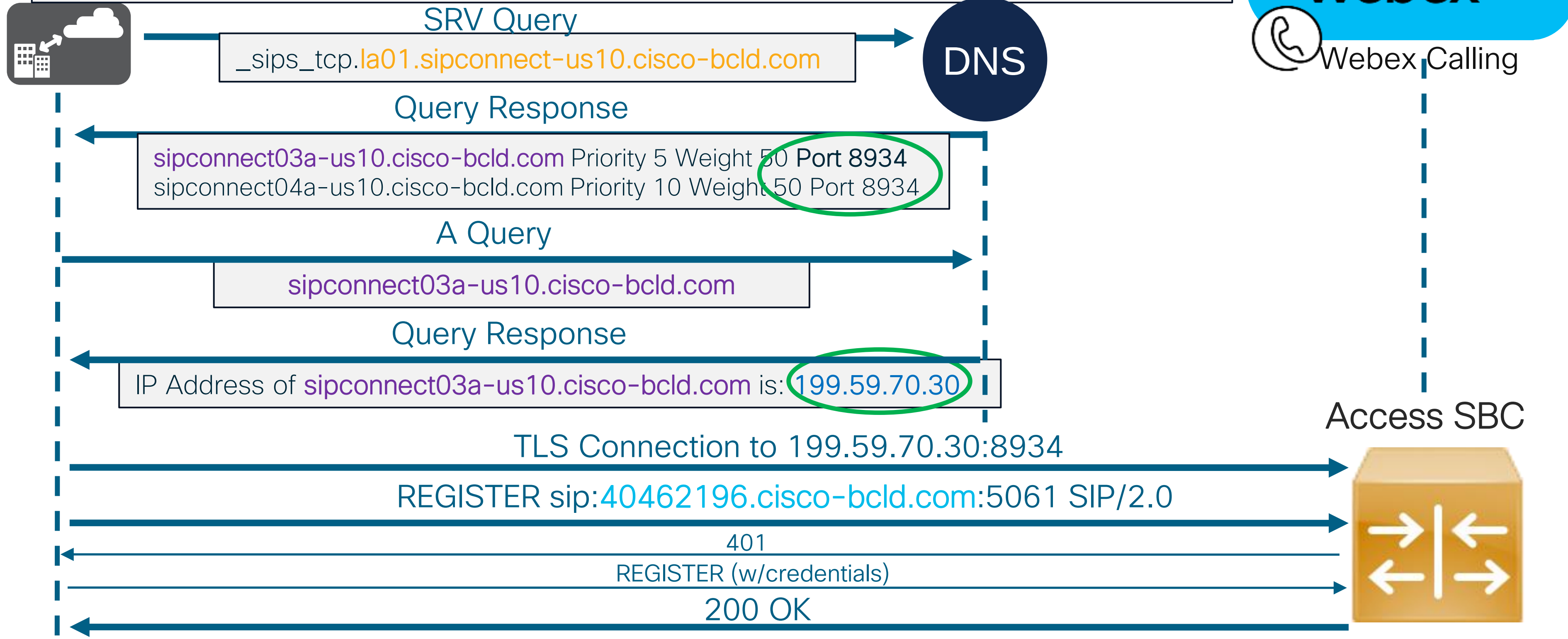
# Control Hub Trunk Info Connection Parameters → LGW CLI Config




```
voice class tenant 200
  registrar dns:40462196.cisco-bcld.com scheme sips expires 240 refresh-ratio 50 tcp tls
  credentials number Hussain6346_LGU username Hussain2572_LGU password 0 meX7]~)VmF realm BroadWorks
  authentication username Hussain2572_LGU password 0 meX7]~)VmF realm BroadWorks
  authentication username Hussain2572_LGU password 0 meX7]~)VmF realm 40462196.cisco-bcld.com
  sip-server dns:40462196.cisco-bcld.com
  connection-reuse
  srtp-crypto 200
  session transport tcp tls
  url sips
  error-passthru
  bind control source-interface GigabitEthernet0/0/1
  bind media source-interface GigabitEthernet0/0/1
  no pass-thru content custom-sdp
  sip-profiles 200
  outbound-proxy dns:la01.sipconnect-us10.cisco-bcld.com
...
voice class sip-profiles 200
 rule 1 request ANY sip-header SIP-Req-URI modify "sips:" "sip:"
 rule 10 request ANY sip-header To modify "<sips:" "<sip:"
 rule 11 request ANY sip-header From modify "<sips:" "<sip:"
 rule 12 request ANY sip-header Contact modify "<sips:(.*)>" "<sip:\1;transport=tls>"
 rule 13 response ANY sip-header To modify "<sips:" "<sip:"
 rule 14 response ANY sip-header From modify "<sips:" "<sip:"
 rule 15 response ANY sip-header Contact modify "<sips:" "<sip:"
 rule 16 request ANY sip-header From modify ">" ";otg=hussain2572_lgu>"
 rule 17 request ANY sip-header P-Asserted-Identity modify "<sips:" "<sip:"
```

# Establishing Secure Connectivity b/w LGW and Webex Calling

```
voice class tenant 200
  registrar dns:40462196.cisco-bcld.com scheme sips expires 240 refresh-ratio 50 tcp tls
  session transport tcp tls
  url sips
  outbound-proxy dns:la01.sipconnect-us10.cisco-bcld.com
```



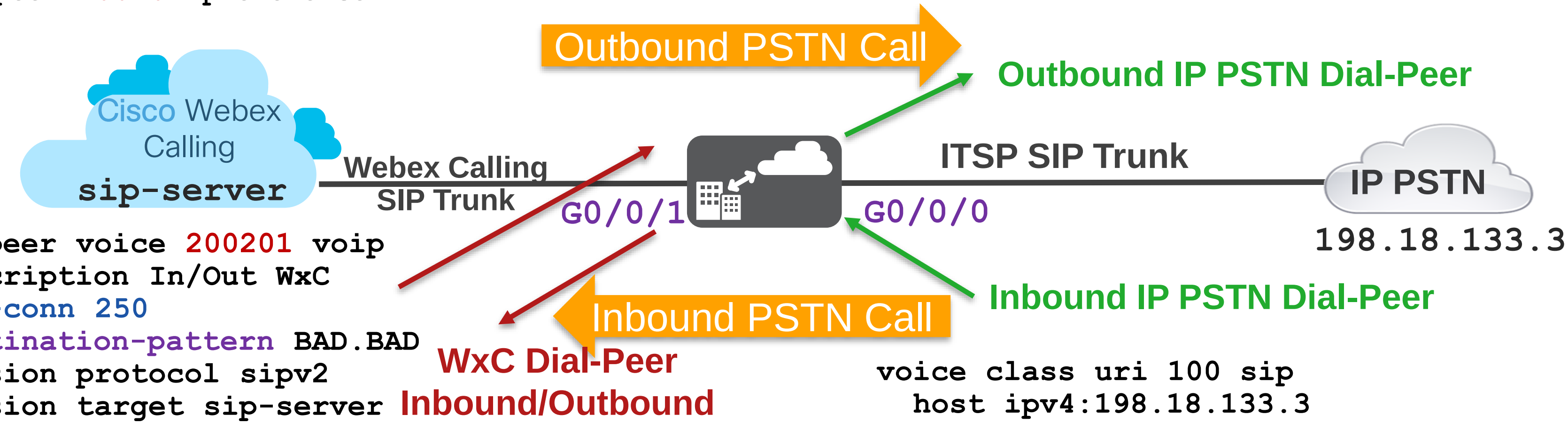
# Dial-peer structure

```
voice class uri 200 sip
  pattern dtg=hussain2572_lgu

voice class dpg 100
 description Incoming WxC(DP200201) to IP PSTN(DP101)
 dial-peer 101 preference 1

voice class dpg 200
 description Incoming IP PSTN(DP100) to WxC(DP200201)
 dial-peer 200201 preference 1
```

```
dial-peer voice 101 voip
 description Outgoing dial-peer to IP PSTN
 destination-pattern BAD.BAD
 session protocol sipv2
 session target ipv4:198.18.133.3
 voice-class codec 99
 voice-class sip tenant 100
 dtmf-relay rtp-nte
 no vad
```

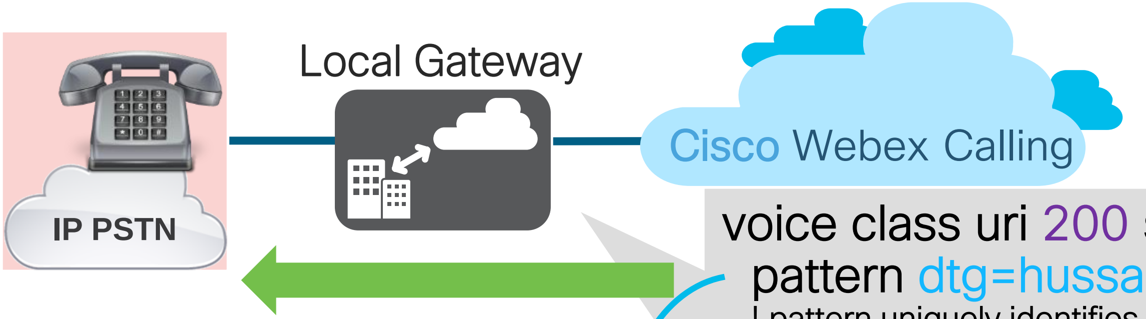



```
dial-peer voice 200201 voip
  description In/Out WxC
  max-conn 250
  destination-pattern BAD.BAD
  session protocol sipv2
  session target sip-server
  destination dpg 100
  incoming uri request 200
  voice-class codec 99
  voice-class stun-usage 200
  no voice-class sip localhost
  voice-class sip tenant 200
  dtmf-relay rtp-nte
  srtp
  no vad
```

```
voice class uri 100 sip
  host ipv4:198.18.133.3

dial-peer voice 100 voip
  description Incoming dial-peer from IP PSTN
  incoming uri via 100
  session protocol sipv2
  destination dpg 200
  voice-class codec 99
  voice-class sip tenant 300
  dtmf-relay rtp-nte
  no vad
```

# Local Gateway call routing based on Trunk Group ID




```
voice class uri 200 sip
  pattern dtg=hussain2572_lgu
  ! pattern uniquely identifies a Local gateway site
  ! within an Enterprise, Trunk Group OTG/DTG from
  ! Control Hub

dial-peer voice 200201 voip
 description Webex Calling
  incoming uri request 200
  destination dpg 100
```

INVITE Received by Local Gateway from Webex Calling

Received:
INVITE sip:+16785551234@198.18.1.226:5061;transport=tls;dtg=hussain2572_lgu SIP/2.0
Via: SIP/2.0/TLS 199.59.70.30:8934;branch=z9hG4bK2hokad30fg14d0358060.1

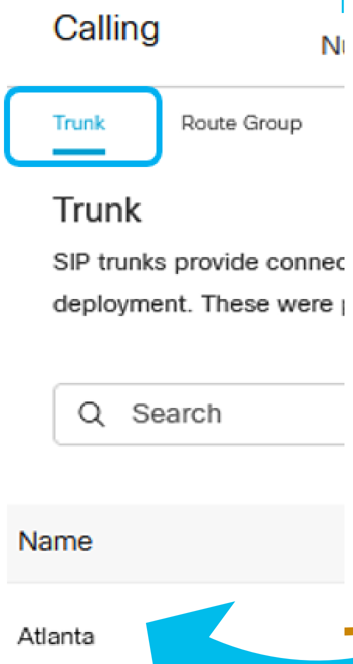
# What constitutes a Registration-based LGW within a CUBE platform?

```
voice class sip-profiles 200
  rule 20 request ANY sip-header From modify ">" ";otg= hussain2572_lgu >"

voice class tenant 200
  registrar dns:XXXXXX scheme sips expires 240 refresh-ratio 50 tcp tls
  credentials number XXXXXX username XXXXXX password 0 XXXXXX realm BroadWorks
  authentication username XXXXXX password 0 XXXXXX realm BroadWorks
  authentication username XXXXXX password 0 XXXXXX realm XXXXXX
  sip-server dns:XXXXXX
  session transport tcp tls
  url sips
  bind control source-interface GigabitEthernet1
  bind media source-interface GigabitEthernet1
  sip-profiles 200
  outbound-proxy dns:XXXXXX

voice class uri 200 sip
  pattern dtg=hussain2572_lgu

dial-peer voice 200201 voip
  description In/Out WxC
  max-conn 250
  destination-pattern BAD.BAD
  session protocol sipv2
  session target sip-server
  destination dpg 100
  incoming uri request 200
  voice-class sip tenant 200
```



# Single CUBE platform with two LGWs

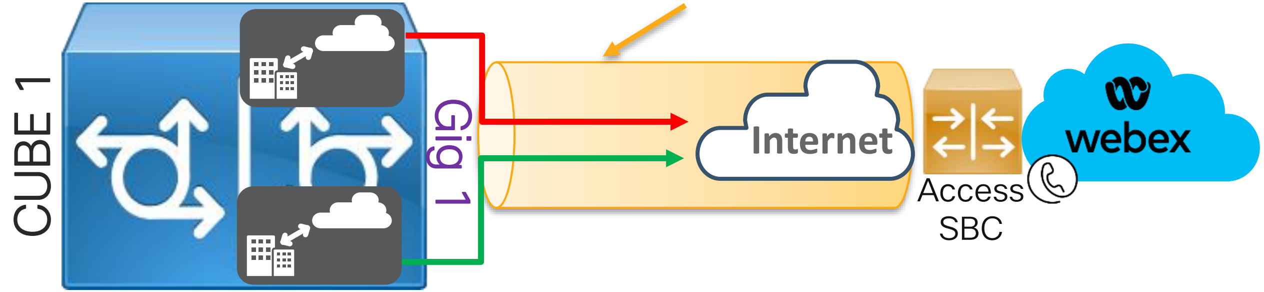
## 1 TLS Connection to Access SBC = 250 max calls

```
voice class uri 200 sip

Inbound dial-peer 200201
 voice class tenant 200
  bind interface Gig 1
   voice class sip-profiles 200
 destination dpg 200
```

LGW1

Single TLS Connection between CUBE and Access SBC.

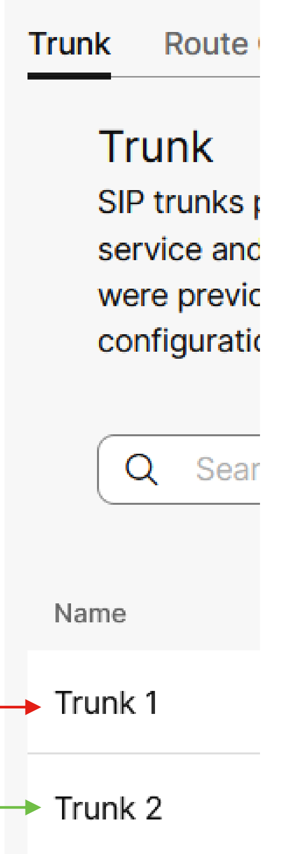



**250** max calls per CUBE

```
voice class uri 300 sip

Inbound dial-peer 300301
 voice class tenant 300
  bind interface Gig 1
   voice class sip-profiles 300
 destination dpg 300
```

LGW2



# Single CUBE platform with two LGWs

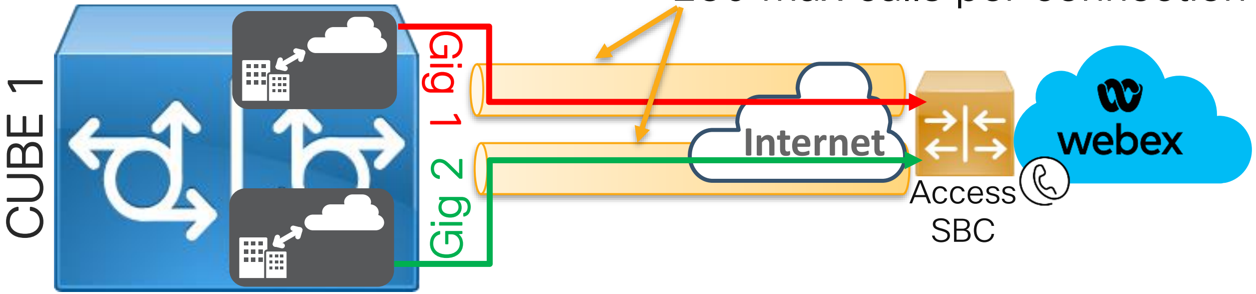
## 2 TLS Connections to Access SBC = 500 max calls

```
voice class uri 200 sip

Inbound dial-peer 200201
 voice class tenant 200
  bind interface Gig 1
  voice class sip-profiles 200
 destination dpg 200
```

LGW1

Each LGW with its own TLS connection = 250 max calls per connection

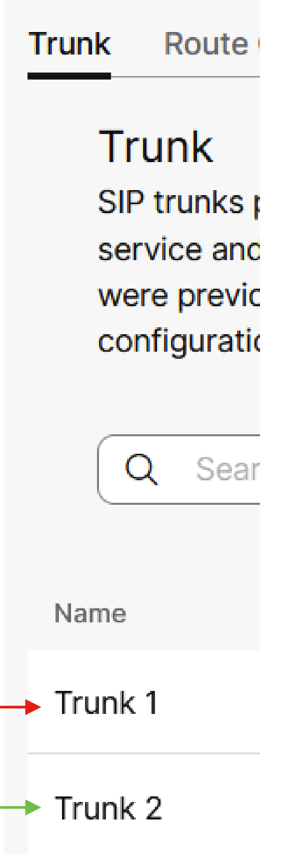



**500** max calls per CUBE

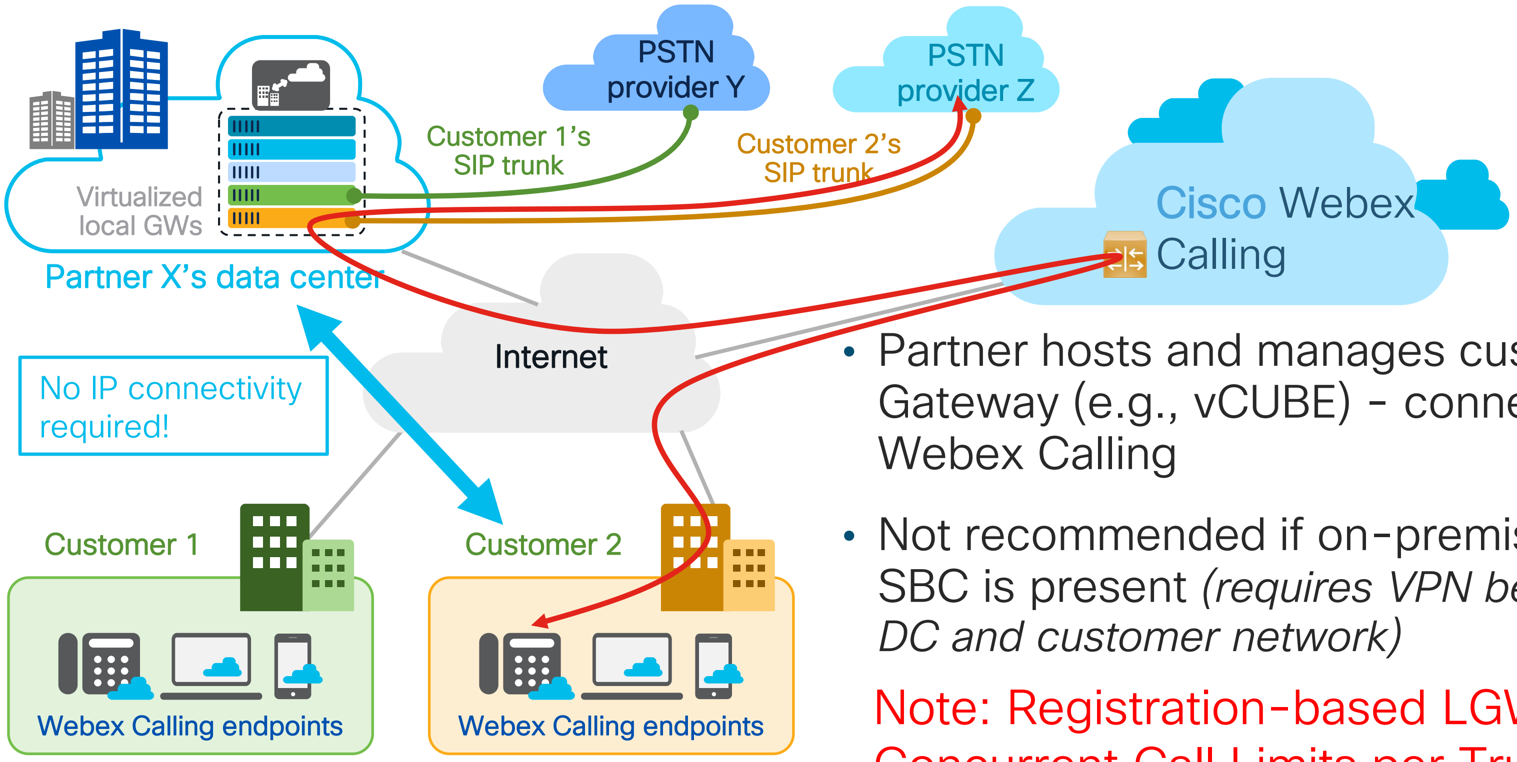
```
voice class uri 300 sip

Inbound dial-peer 300301
 voice class tenant 300
  bind interface Gig 2
  voice class sip-profiles 300
 destination dpg 300
```

LGW2



# Partner hosted Local Gateway (Multi-tenant)




- Partner hosts and manages customer's Local Gateway (e.g., vCUBE) - connected OTT to Webex Calling
- Not recommended if on-premises PBX or SBC is present *(requires VPN between Partner DC and customer network)*

Note: Registration-based LGW Concurrent Call Limits per Trunk and per TLS connection Apply

# Single vCUBE instance with two LGWs – Total 500 calls

IOS-XE 17.8.1a or later

Trunk1 - LGW1=250 calls

```
dial-peer voice 200201 voip
 description In/Out WxC
 max-conn 250
 destination-pattern BAD.BAD
 session protocol sipv2
 session target sip-server
 destination dpg 100
 incoming uri request 200
 voice-class sip tenant 200

voice class tenant 200
 bind control source-interface GigabitEthernet1
 bind media source-interface GigabitEthernet1
  listen-port secure 5062
  tls-profile 2

voice class tls-profile 2
 trustpoint CUBE-TLS
```

Trunk 2 - LGW2=250 calls

```
dial-peer voice 300301 voip
 description In/Out WxC
 max-conn 250
 destination-pattern BAD.BAD
 session protocol sipv2
 session target sip-server
 destination dpg 300
 incoming uri request 300
 voice-class sip tenant 300

voice class tenant 300
 bind control source-interface GigabitEthernet1
 bind media source-interface GigabitEthernet1
  listen-port secure 5070
  tls-profile 3

voice class tls-profile 3
 trustpoint CUBE-TLS
```

BRKCOL-2314

# CUBE Encrypted Audio Call Capacity

| Platform<br>[1]CSR1Kv - Based on tests using Cisco UCS ® C240 host with Intel ® Xeon ® 6132 2.60GHz processors running VMware ESXi 6.0. | Audio IP Telephony calls<br>RTP(G711)-RTP(G711) | Encrypted Audio (SHA1_80) calls<br>sRTP(G711)-RTP(G711) | CPS |
|---|---|---|---|
| 1100 series (Default DRAM) | 500 | 300 | 2 |
| 4321 (4 GB) | 500 | 300 | 1 |
| 4331 (4 GB) | 1000 | 600 | 3 |
| 4351 (4 GB) | 2000 | 750 | 4 |
| 4431 (8 GB) | 3000 | 750 | 4 |
| 4451 (8 GB) | 6000 | 2100 (16.12.2) | 11 |
| 4461 (8 GB) | 10000 (17.2.1r) | 9900 (17.6.4) | 30 |
| C8200L-1N-4T (4 GB) | 1500 (17.5.1) | 400 (17.5.1) | 3 |
| C8200-1N-4T (8 GB) | 2500 (17.4.1) | 650 (17.4.1) | 4 |
| C8300-1N1S-6T (8 GB) | 7000 (17.3.2) | 1600 (17.3.2) | 9 |
| C8300-2N2S-6T (8 GB) | 7500 (17.3.2) | 1800 (17.3.2) | 10 |
| C8300-1N1S-4T2X (8 GB) | 8000 (17.3.2) | 3500 (17.12+) | 15 |
| C8300-2N2S-4T2X (16 GB) | 10000 (17.3.2) | 4300 (17.3.2) | 24 |
| C8000V-S/CSR1Kv – 1 vCPU[1] (4 GB) | 1000 | 300 | 1 |
| C8000V-M/CSR1Kv - 2 vCPU[1] (4 GB) | 3000 | 1000 | 6 |
| C8000V-L/CSR1Kv - 4 vCPU[1] (8 GB) | 6000 | 1080 | 6 |

# Validate Registration-based LGW Configuration through Control Hub

# Managed Gateway now **Online**

## Calling

Numbers | Locations | Call Routing | **Managed Gateways** | Features | PSTN | Service Settings | Client Settings

Search | All Gateways | 10 Gateway(s) | Events History | Add Gateway

| Gateway Name | Version | Connector Sta... | Service | Assigned to | Actions |
|---|---|---|---|---|---|
| Amsterdam SGW | 17.9.3 | Online | Survivability Gateway | Location: Amsterdam Office | ... |
| Hussain-Cat8kv | 17.9.20221... | Online | - | - | ... |
| Lisbon SGW | 17.9.3 | Online | Survivability Gateway | Location: Lisbon Office | ... |
| London SGW | 17.9.3 | Offline | Survivability Gateway | Location: London Branch Office | ... |
| Madrid SGW | 17.9.3 | Online | Survivability Gateway | Location: Madrid Office | ... |
| Munich SGW | 17.9.3 | Online | Survivability Gateway | Location: Munich Office | ... |
| Paris SGW | 17.9.3 | Online | Survivability Gateway | Location: Paris Office | ... |

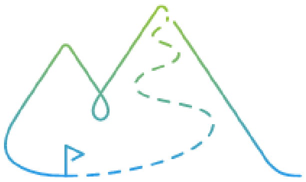
# Assign a Service to the Managed Gateway

< Managed Gateways

## Hussain-Cat8kv

Actions

● Connector Online • Version 17.9.20221213

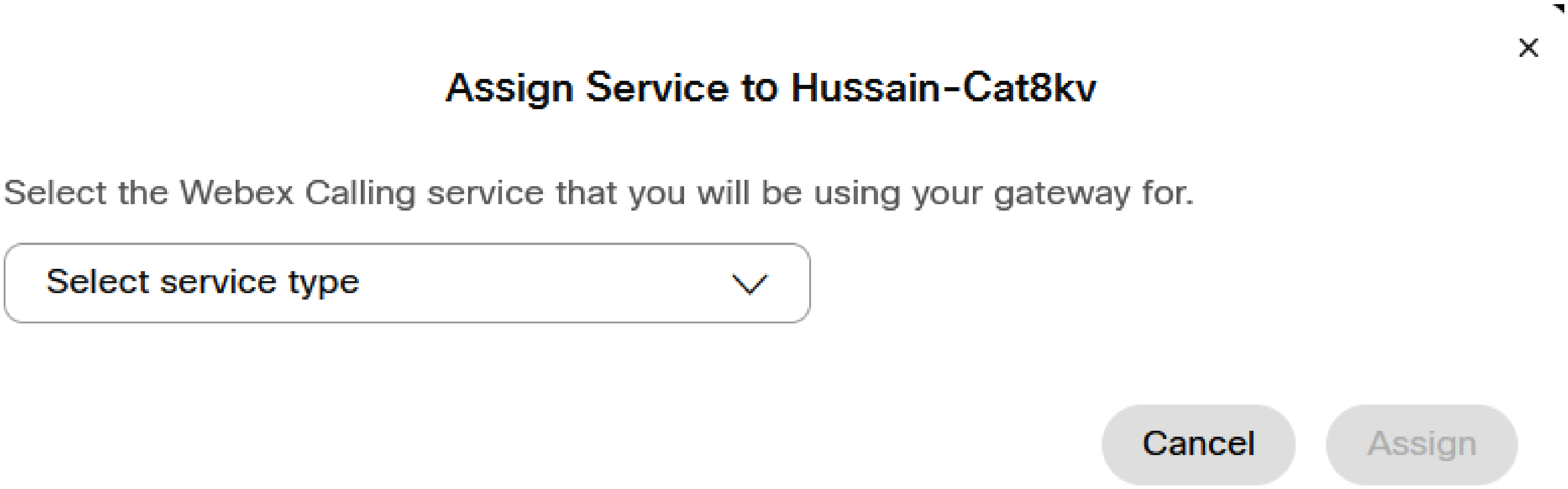


### Assign Service

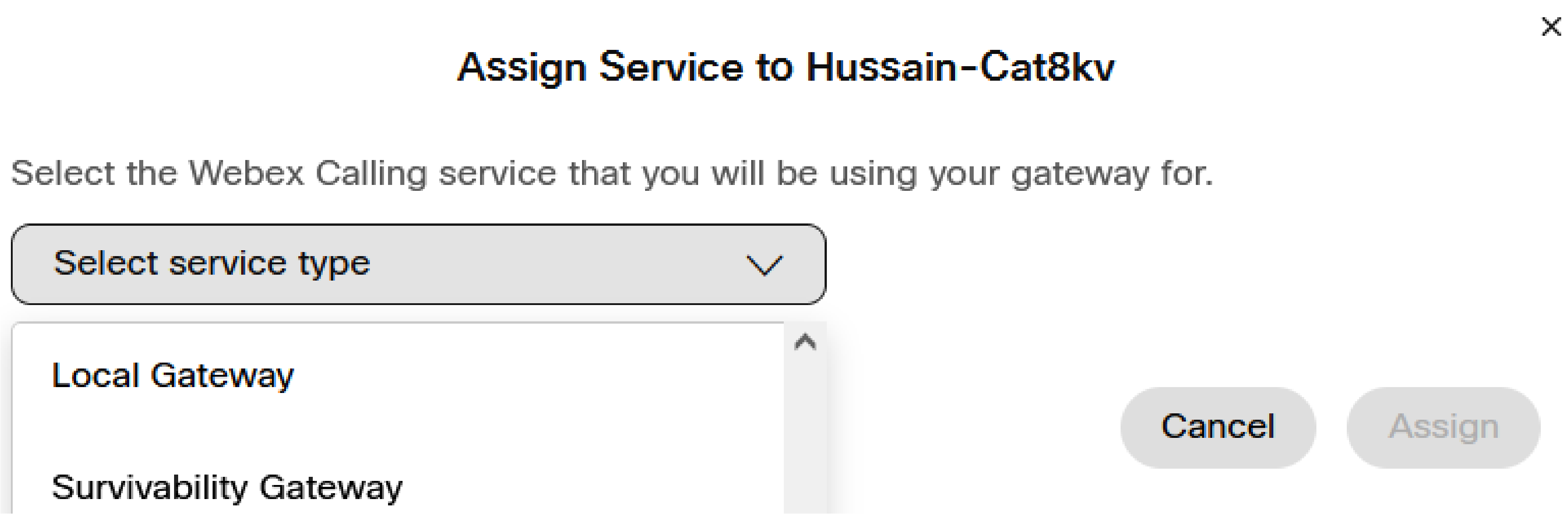
Assign the Webex Calling service that you will be using your gateway for.

Assign Service

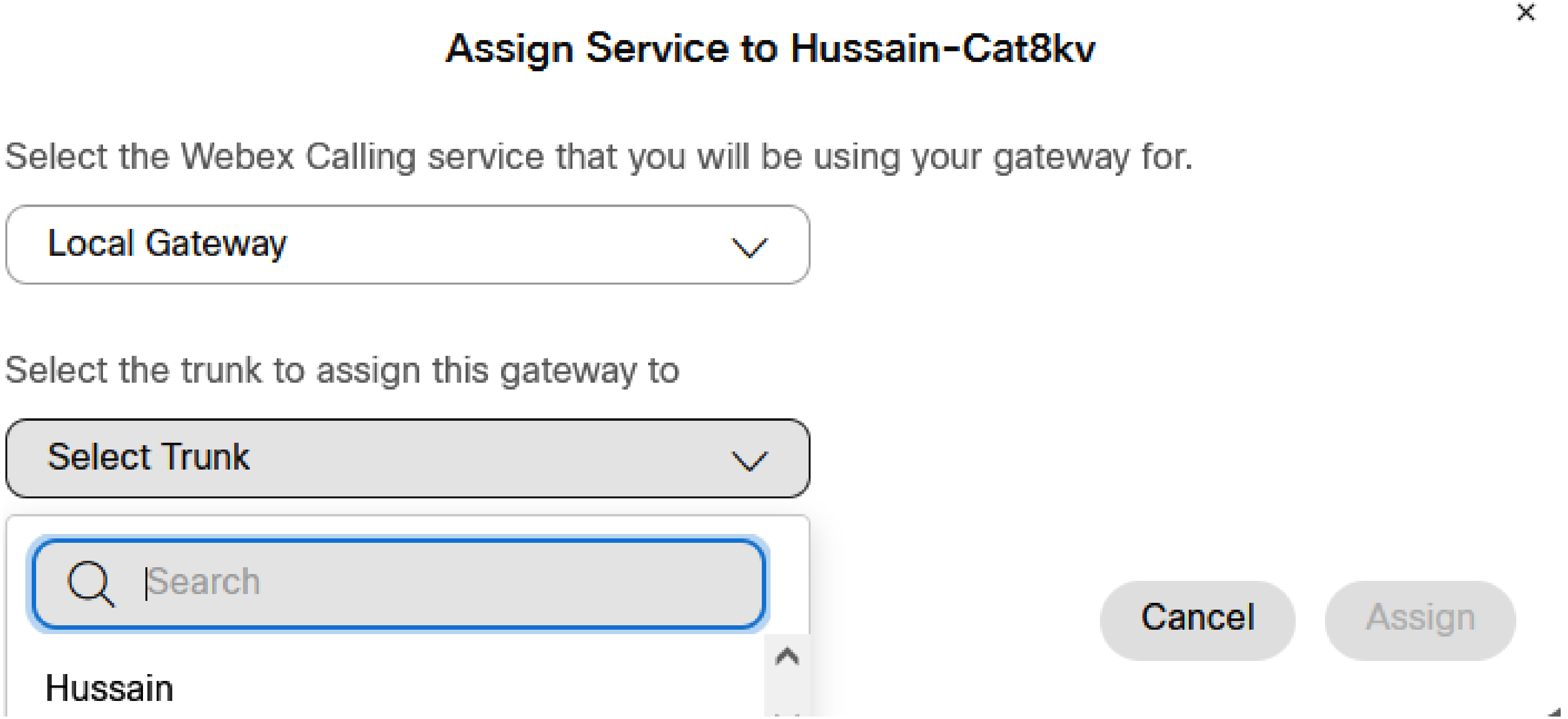
# Select a Service Type



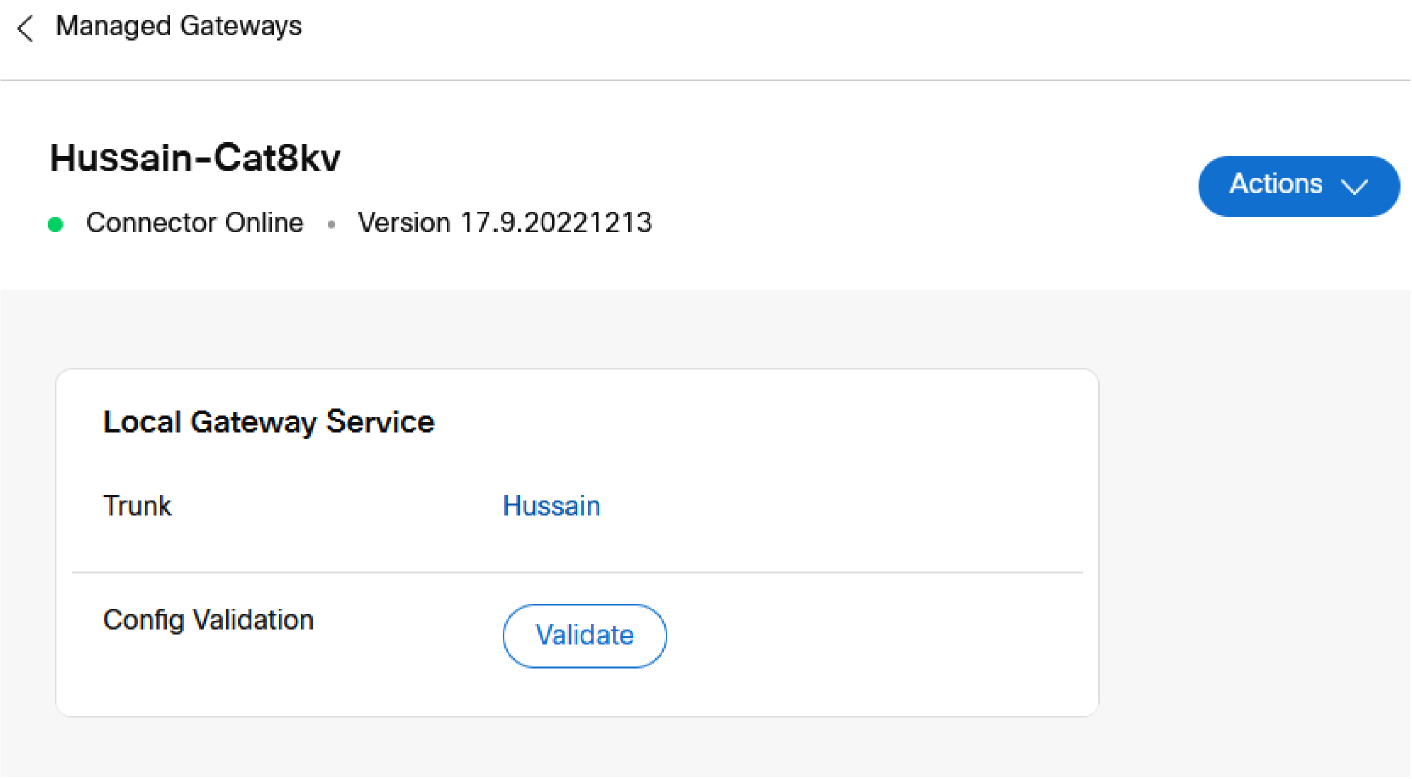
# Service Type: LGW or SGW



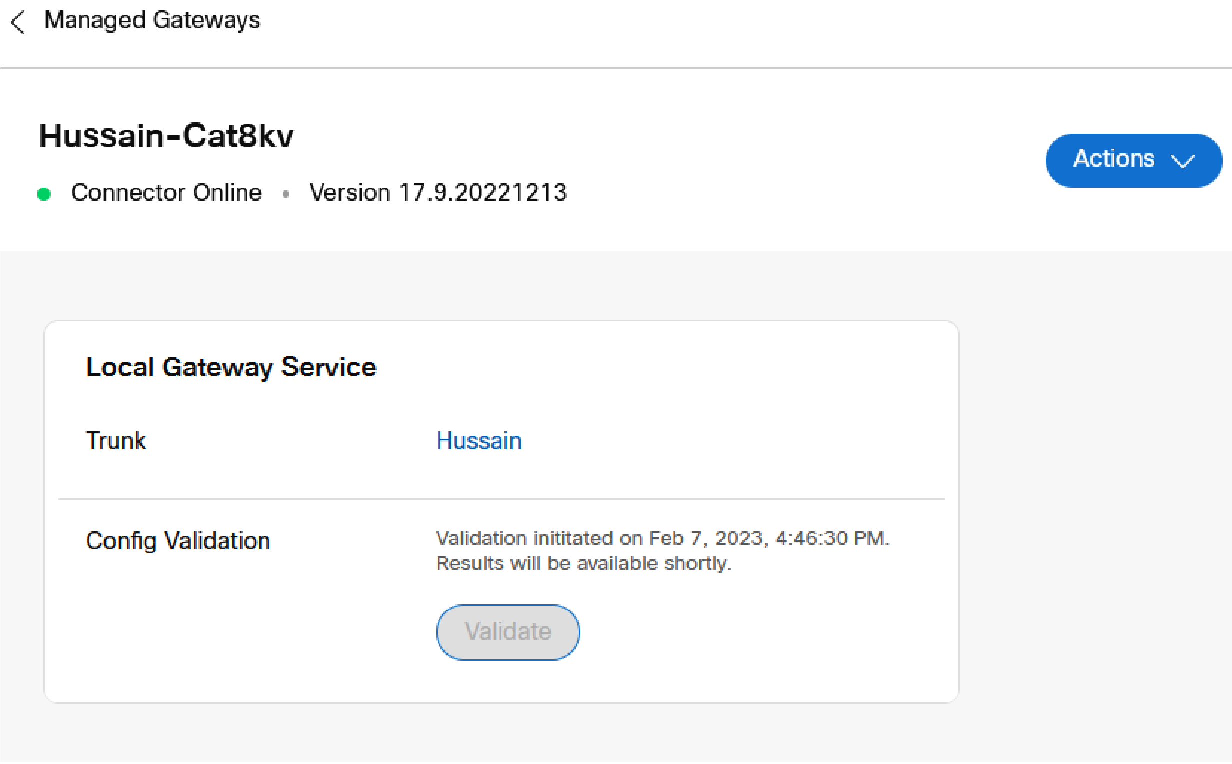
# For Service Type Local Gateway, specify the **Trunk**



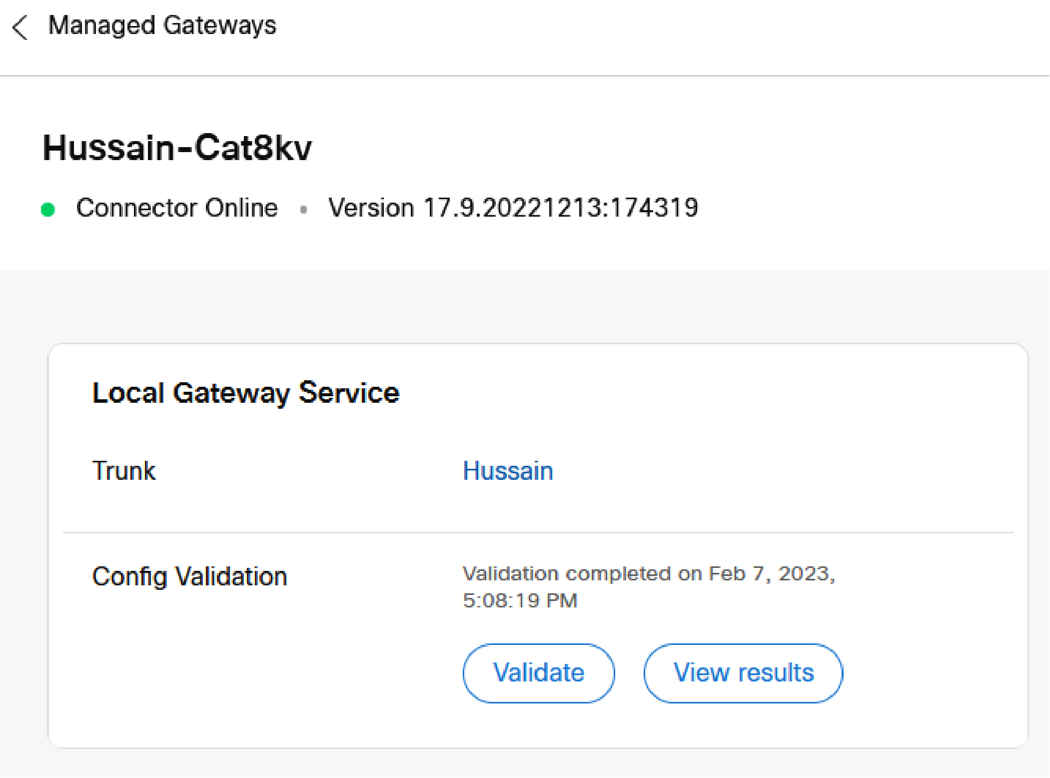
# Validate Registration-based LGW Configuration



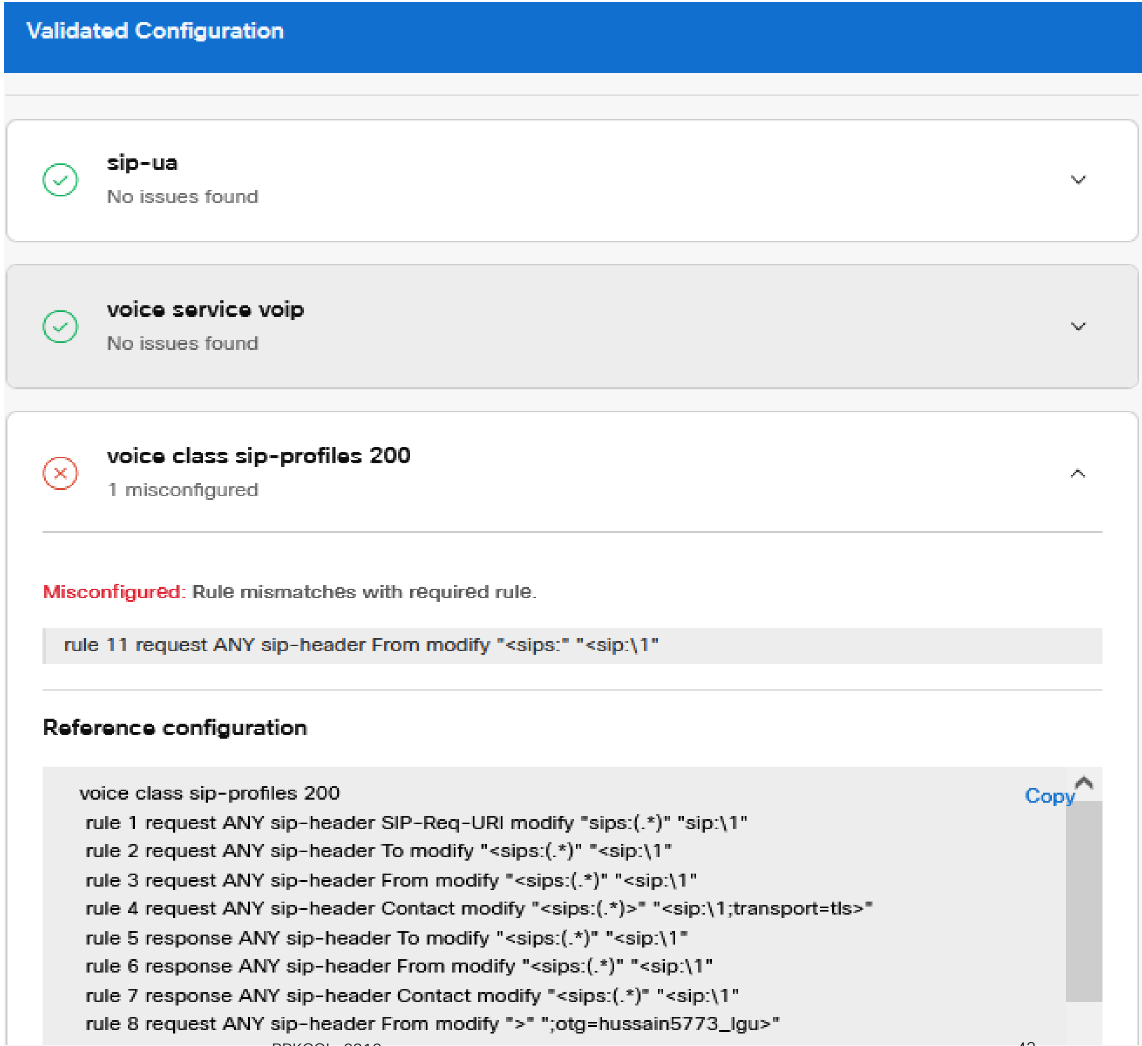
# Validation takes a few minutes



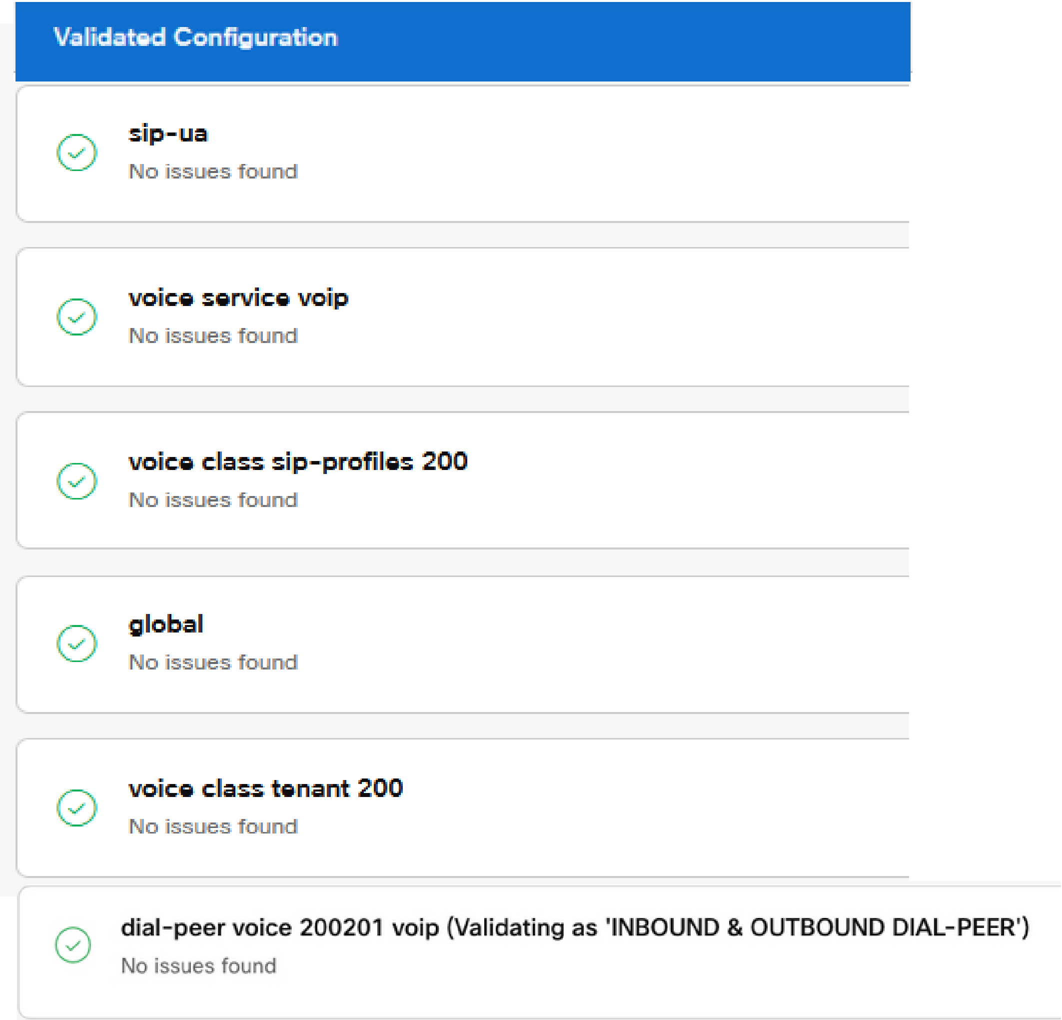
# View Validation results



# In the Validated Configuration page, verify if there are any misconfigurations



# Fix misconfigurations within the Local Gateway and run validation again



# Introducing Certificate-based Local Gateway

# Webex Calling Trunk - Local Gateway (Certificate-based)

Webex Calling edge proxy address (FQDN)

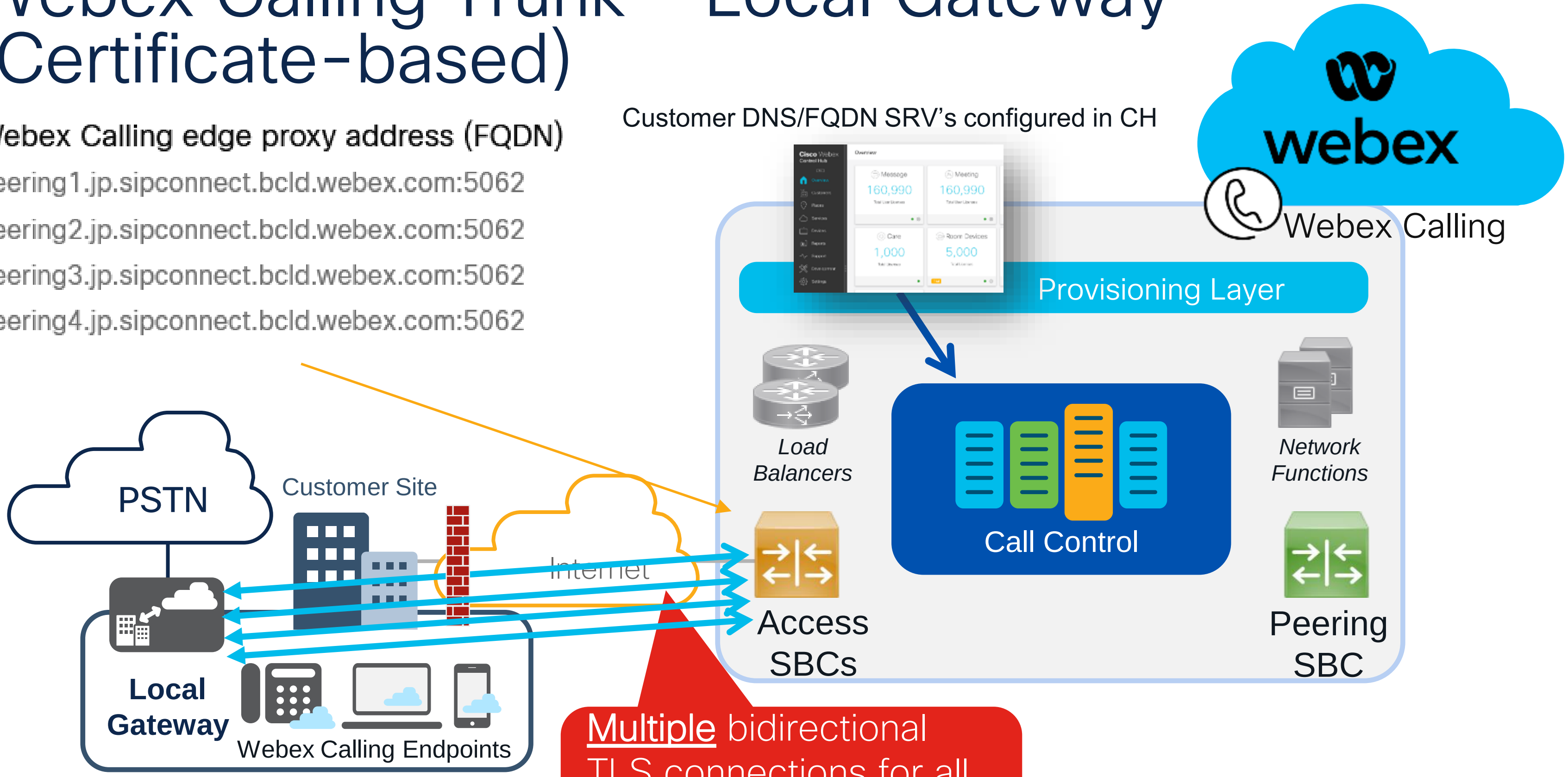
peering1.jp.sipconnect.bcld.webex.com:5062

peering2.jp.sipconnect.bcld.webex.com:5062

peering3.jp.sipconnect.bcld.webex.com:5062

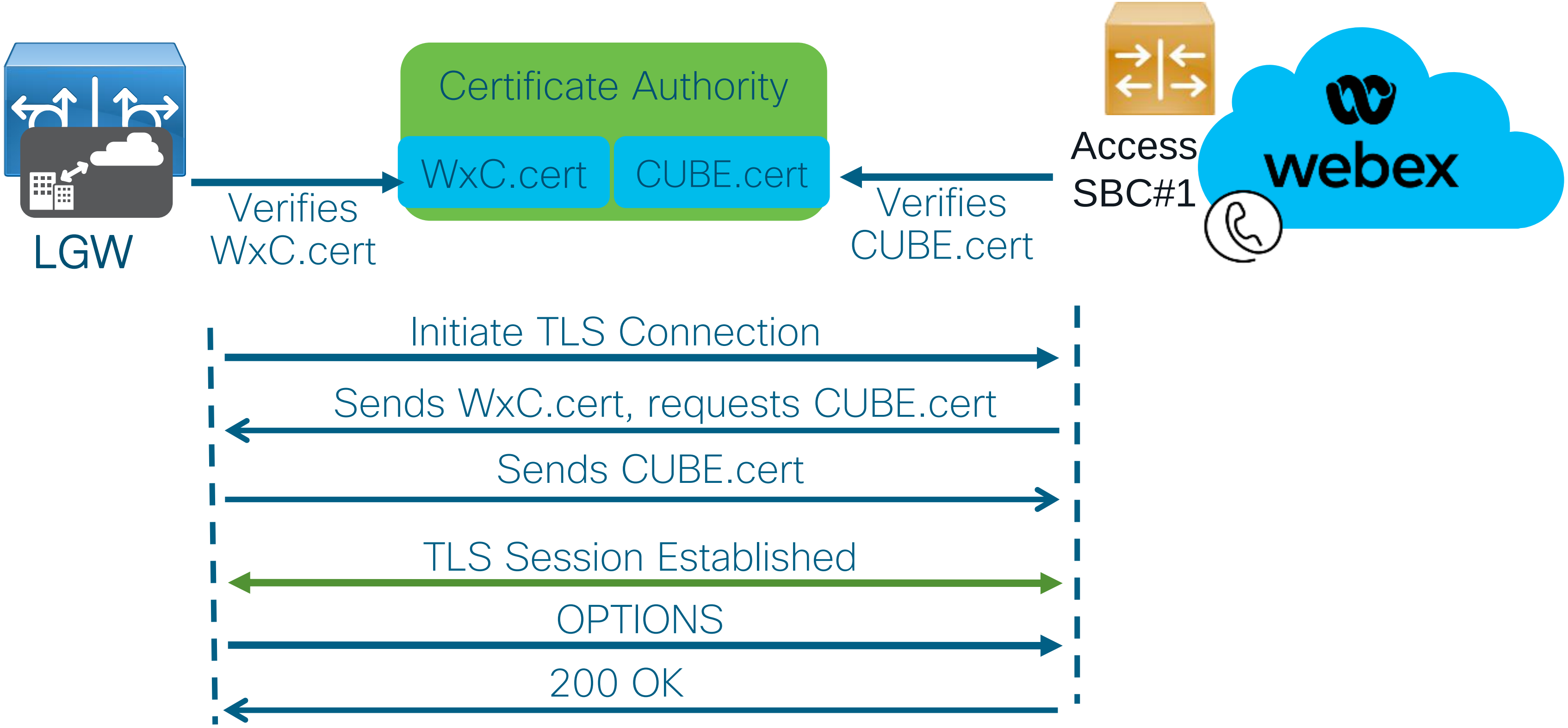
peering4.jp.sipconnect.bcld.webex.com:5062

Customer DNS/FQDN SRV's configured in CH

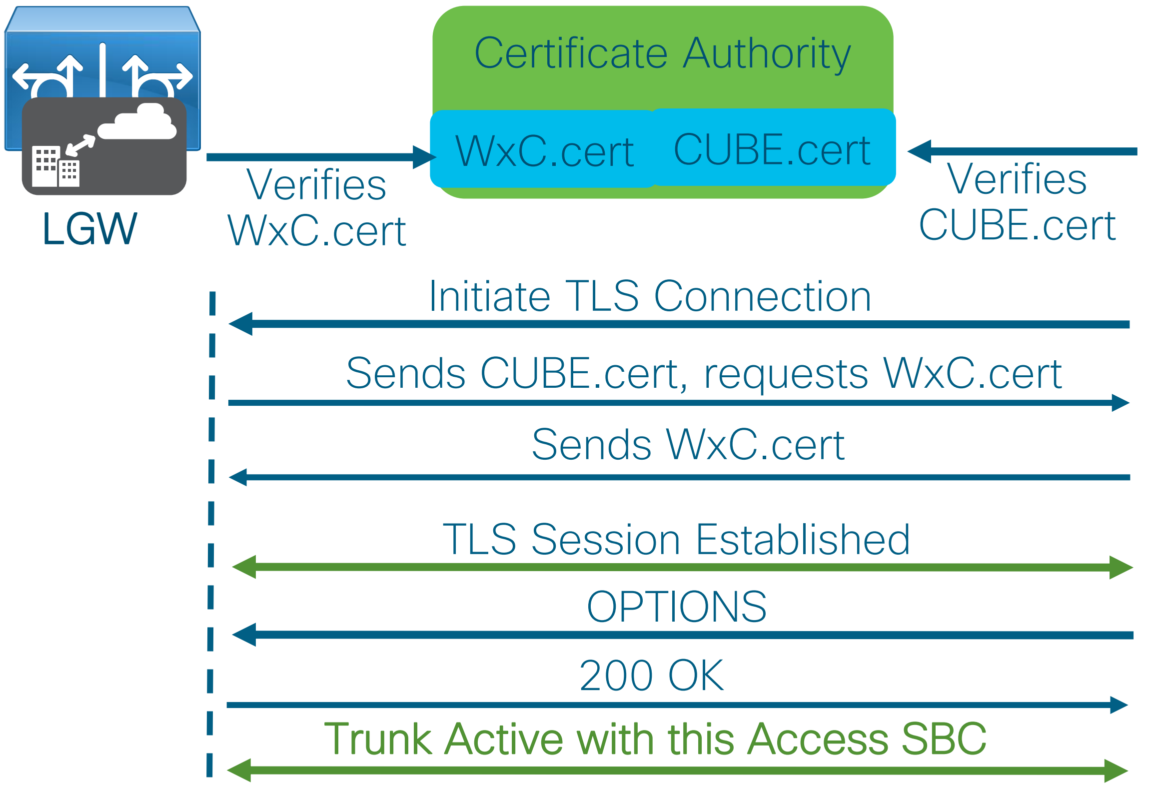


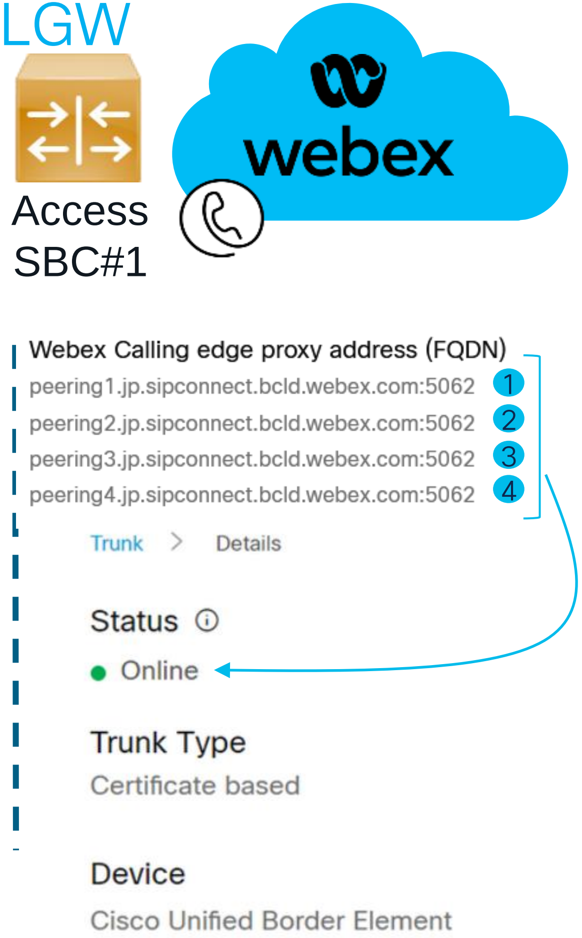

<u>Multiple</u> bidirectional TLS connections for all signaling between LGW and cloud

# Certificate-based Local Gateway (Trunk Establishment) – 1st WxC Access SBC - Outbound from LGW to WxC



# Certificate-based Local Gateway (Trunk Establishment) – 1st WxC Access SBC - Inbound from WxC to LGW



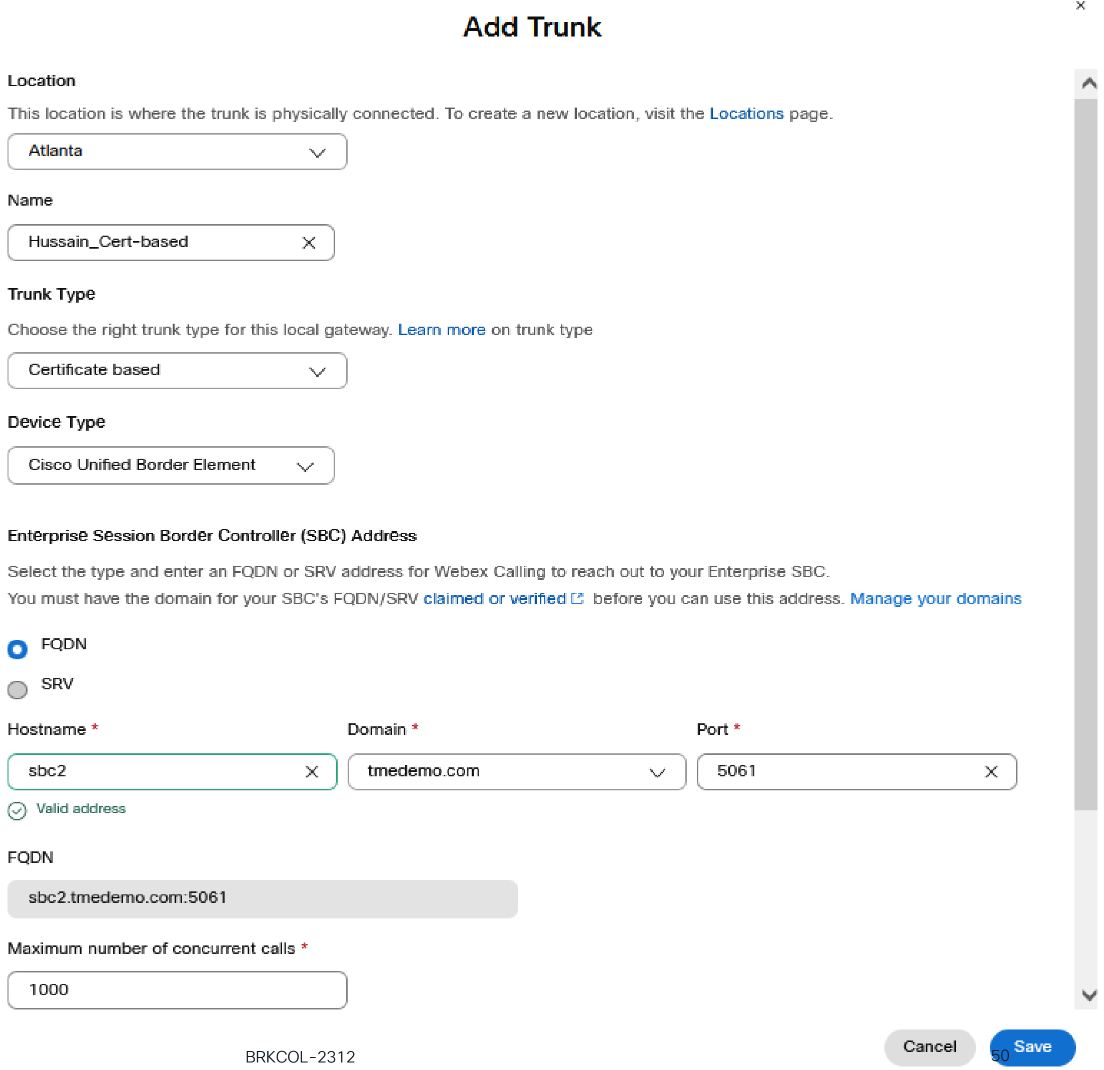




Now repeat the process with the 2nd, the 3rd, and the 4th WxC Access SBC

# Configuring a Certificate-based LGW

# Adding a Certificate-based Trunk in Control Hub

# Add a Certificate-based Trunk to a Location



# Adding a Trunk

## Add Trunk

**Location**

This location is where the trunk is physically connected. To create a new location, visit the Locations page.

Atlanta

**Name**

Hussain_Cert-based

**Trunk Type**

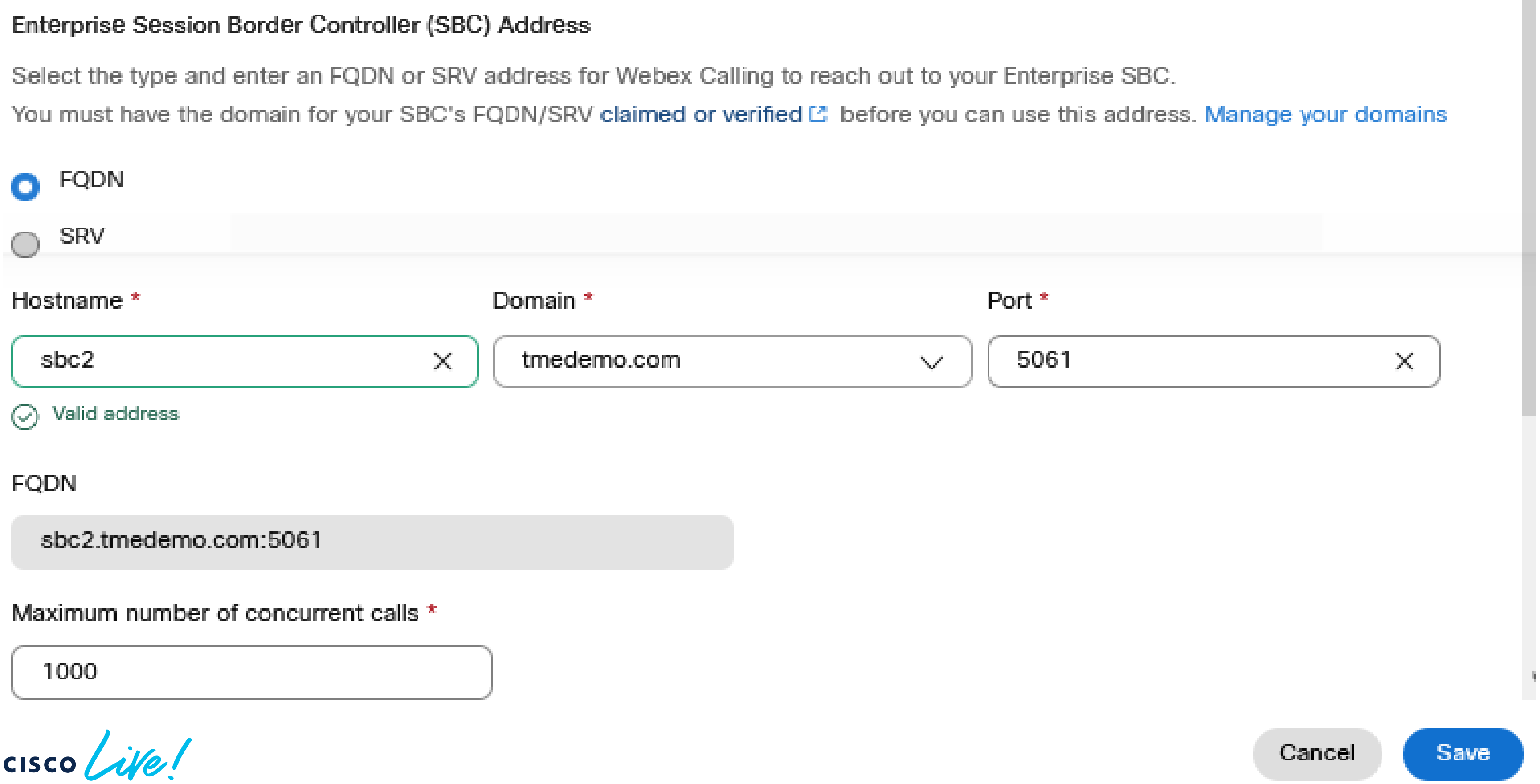
Choose the right trunk type for this local gateway. Learn more on trunk type

Certificate based

**Device Type**

Cisco Unified Border Element

# Define the LGW hostname and select to resolve the LGW through an FQDN or an SRV



# Save the Webex Calling Edge Addresses displayed

## Add Trunk

Hussain_Cert-based Successfully Created.

Visit Route Group page to add trunk(s) to a route group.
Visit Locations page to configure PSTN connection to individual locations.
Visit Dial Plans page to use this trunk as the routing choice for a dial plan.

IOS-XE 17.6+

**Trunk Info**

Status

● Unknown

Webex Calling edge proxy address (FQDN)

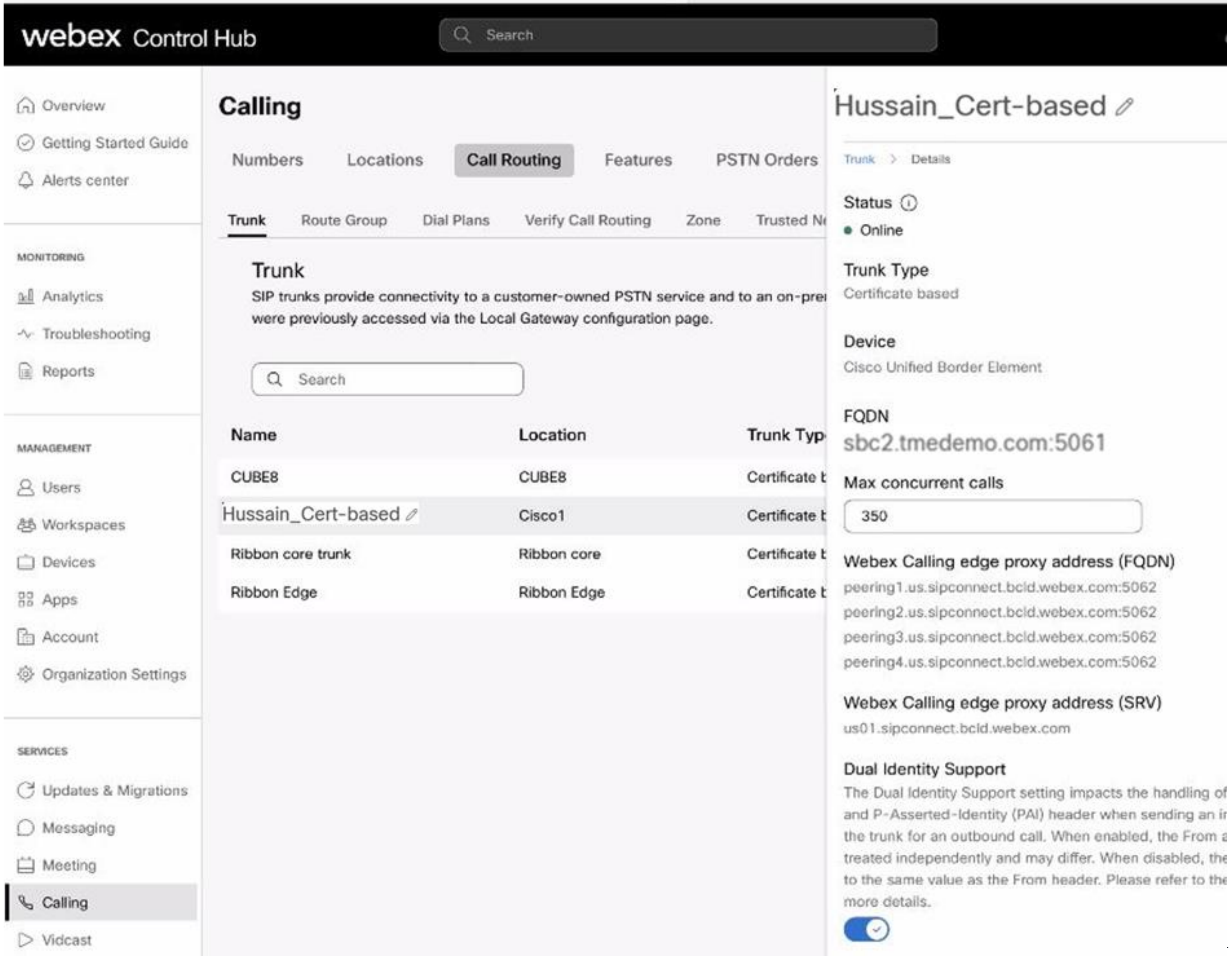
peering1.us.sipconnect.bcld.webex.com:5062
peering2.us.sipconnect.bcld.webex.com:5062
peering3.us.sipconnect.bcld.webex.com:5062
peering4.us.sipconnect.bcld.webex.com:5062

IOS-XE 17.9+

Webex Calling edge proxy address (SRV)

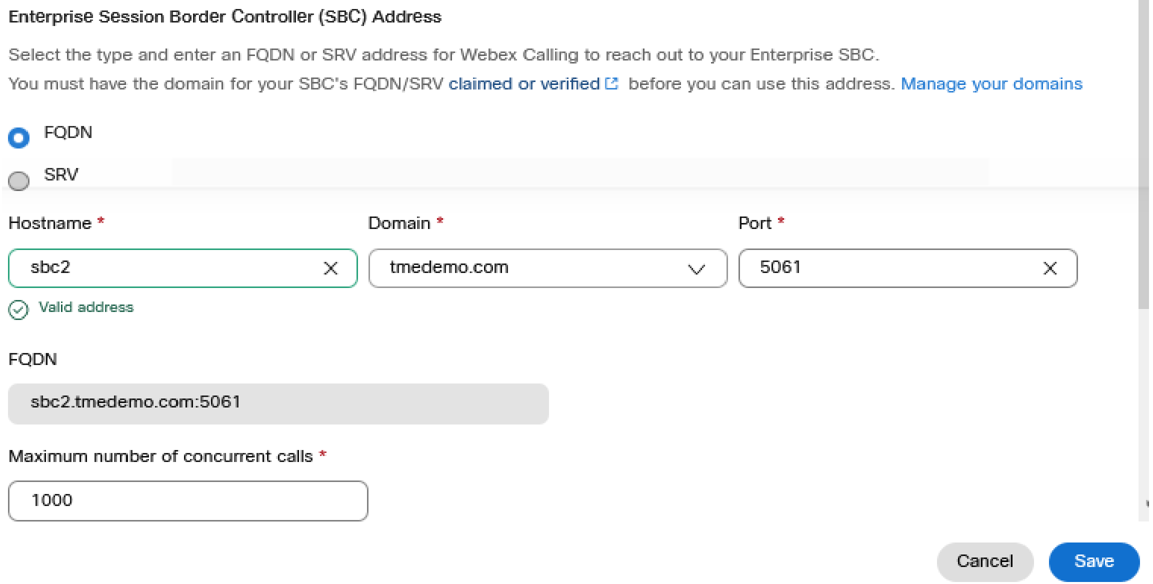
us01.sipconnect.bcld.webex.com

# View your trunk



# References in this presentation

| | |
|---|---|
| Top level Domain | tmedemo.com |
| SBC/CUBE's FQDN (should be publicly reachable) | sbc2.tmedemo.com |
| Static Public IP associated with the CUBE FQDN | 198.135.2.118 |



# Configuring CUBE as a Certificate-based LGW

# Step by Step CUBE config: Common Global Configuration

## Step 1 :
## Base Platform configuration and Certificates

# CUBE Reference platform configuration

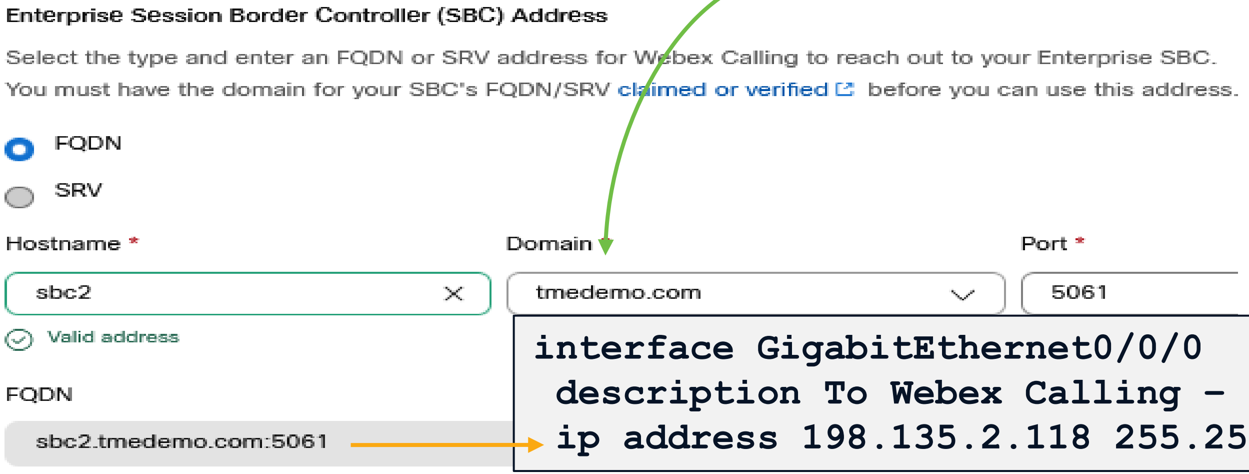
- Before proceeding with CUBE configuration, ensure baseline platform configuration such as NTPs, ACLs, enable passwords, IP routing, IP Addresses, etc. are configured according to your organization's policies and procedures
- All SIP and media ports on the external interface (Webex Calling facing) of the Local Gateway MUST be accessible to Webex Calling service and vice versa.
- Public IPv4 address(es) must be reachable from the outside and should resolve through a public DNS service
- FQDN for the LGW configured within Control Hub should resolve to this interface IP (Static NAT supported)
- IOS-XE 17.6+ is required.

```
interface GigabitEthernet 1
 description To Webex Calling - Public IPv4
 ip address 198.135.2.118 255.255.255.0
```

# Configure IP Name Server to enable DNS lookup, Domain-name, NTP

```
CUBE#config terminal
CUBE(config)#hostname sbc2
sbc2(config)#ip domain-name tmedemo.com
sbc2(config)#ip name-server 208.67.222.222
sbc2(config)#ntp server 0.us.pool.ntp.org
```

- DNS Servers: ensure the ip name-server is reachable by successfully pinging it. Local Gateway must resolve Webex Calling proxy addresses using this DNS
- Set the same domain name for the platform as defined in Control Hub




```
interface GigabitEthernet0/0/0
 description To Webex Calling - Public IPv4
 ip address 198.135.2.118 255.255.255.0
```

# Certificates

# Trust between Webex Calling and Local Gateway

- A signed certificate is required for a successful authorization and authentication of calls from the trunk. The certificate must meet the following requirements:
  - The certificate MUST be signed by a CA mentioned in What Root Certificate Authorities are Supported for Calls to Cisco Webex Audio and Video Platforms?
  - The trust bundle mentioned in What Root Certificate Authorities are Supported for Calls to Cisco Webex Audio and Video Platforms? should be uploaded on to the Local Gateway (CUBE).

# Import Cisco CA bundle for Webex Calling Certificate authentication

```
crypto pki trustpool import clean url
http://www.cisco.com/security/pki/trs/ios_core.p7b

Reading file from
http://www.cisco.com/security/pki/trs/ios_core.p7b
Loading http://www.cisco.com/security/pki/trs/ios_core.p7b
% PEM files import succeeded.
```

# Generate an RSA key pair - `sbc2-key`

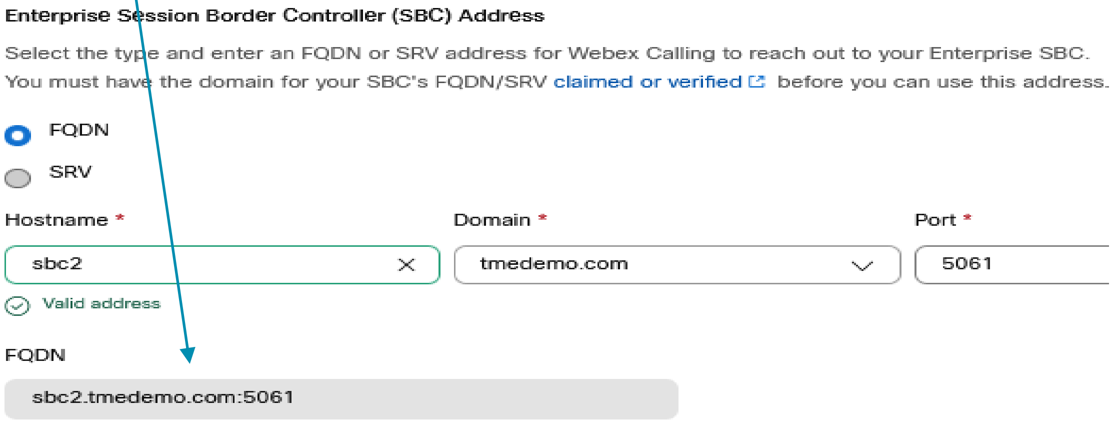
```
crypto key generate rsa general-keys label sbc2-key
modulus 4096 exportable
```

- Create an RSA key matching the certificate length of the root certificate with the above command
- Most CAs require private key size to be at least 2048 bit

# Create a PKI trustpoint to hold the CA-signed CUBE certificate using the RSA key

```
crypto pki trustpoint CUBE_CA_CERT
 enrollment terminal pem
 serial-number none
 subject-name CN=sbc2.tmedemo.com ! (must match platform's DNS hostname through which it is reachable)
 subject-alt-name sbc2.tmedemo.com
 revocation-check none
 rsakeypair sbc2-key ! Created previously
```

- CUBE_CA_CERT – Trustpoint name can be anything
- Certificates MUST contain the Fully Qualified Domain Name (FQDN) as a common name or subject alternate name in the certificate with the FQDN chosen in the Control Hub



# Generate a CSR on CUBE

```
crypto pki enroll CUBE_CA_CERT

% Start certificate enrollment..

% The subject name in the certificate will include: cn=sbc2.tmedemo.com
% The subject name in the certificate will include: sbc2.tmedemo.com
Display Certificate Request to terminal? [yes/no]: yes
```

- Input certificate details, make sure the LGW FQDN defined in Control Hub is present in the SAN [https://www.sslshopper.com/csr-decoder.html](https://www.sslshopper.com/csr-decoder.html)
- Copy and save the CSR
- Send the CSR to your CA, who will send back a certificate for the host and also the root/intermediate CAs
- You may need to add the LGW FQDN (`sbc2.tmedemo.com`) record to your public DNS before your CA will issue you the cert

**Paste Certificate Signing Request (CSR)**


-----BEGIN CERTIFICATE REQUEST-----
MIICpDCCAYwCAQAwPjEaMBgGA1UEAxMRc2JjMi5jdWJlLXRtZS5jb
hkiG9w0BCQIWEXNiYzIuY3ViZS10bWUuY29tMIIBIjANBgkqhkiG9w
AQ8AMIIBCgKCAQEAjBuVXcBKtrPeAHQM1ips3MxaDYlZT6e9N1h
EtIQPvVnFDjSXS2LTMx9FHnmdpEgYkGOzxVjdd0G+aVcsrG/JqtJeS
yJT86Yre9M5uvswEWiwYy/uq3nz3CDFd5NpyUa3sHYqsdnY5/nAo
2T12i3jMpIMqjoDAnP2izd/zPqJBouRPAkx5LVVGATYm1mjfcggAW
KbuoE0Hqaot89mkJxVYKdTHFKZGt1xtQy8QXNMzyiXAe/ElqTbTi5
vCOzcA3ecOWrjrTsbd5hinLq654cyF1c2YVSTQIDAQABoCEwHwYJ
MRIwEDAOBgNVHQ8BAf8EBAMCBaAwDQYJKoZIhvcNAQEFBQAD
DTCNQTOpzsCjqI6f5l1z6/DGISwy2Lvm5j9SdTZZ7M7NZndEcFubq
c8az2Ss6i0fWP5+JxF1ptbWy1ValsA4fxSgeSHNS2nvLriy9el3F7u8H
B1J5hdtqRzanCLR1IJgTKRFWqOM/NHqgTWX4LpDmePIq66XAsv+
2b3kCUGYL324Ys1+9VfuoUeSKUj4lccwNaZmRImCGF0ItgUnCUPk
JeuxjTJFdu1MZtXYMfXFCV99axLEgAuGl6Acp6LtpQfvE0rgWgKv+2
Ke9XS3t4KYM=
-----END CERTIFICATE REQUEST-----


**CSR Information:**

✅ **Common Name:** sbc2.cube-tme.com

# Create a PKI trustpoint to hold the Root Certificate from the Certificate Authority

```
crypto pki trustpoint Root_CA_CERT
 enrollment terminal
 revocation-check none
!
crypto pki authenticate Root_CA_CERT
<paste root CA X.64 based certificate here>
-----BEGIN CERTIFICATE-----
… ! Paste this in Root_CA_CERT
-----END CERTIFICATE-----
```

# Create a PKI trustpoint to hold the Intermediate Certificate, **if** the root certificate has an intermediate CA

```
crypto pki trustpoint Intermediate_CA
 enrollment terminal
 chain-validation continue Root_CA_CERT
 revocation-check none
!
crypto pki authenticate Intermediate_CA
<paste Intermediate CA X.64 based certificate here>
-----BEGIN CERTIFICATE-----
… ! Paste this in Intermediate_CA
-----END CERTIFICATE-----
```

# Authenticate and import the CA signed CUBE cert as shown below (Intermediate CA present)

```
! If the root certificate has an intermediate CA, then proceed as
! shown below. Paste in the top-level intermediate cert only that
! can authenticate the host (CUBE) cert
crypto pki authenticate CUBE_CA_CERT
<paste Intermediate CA X.64 based certificate here>
-----BEGIN CERTIFICATE-----
… ! Paste this in Intermediate_CA
-----END CERTIFICATE-----

! Import the host(CUBE) certificate as shown below
crypto pki import CUBE_CA_CERT certificate
<paste CUBE CA X.64 based certificate here>
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
… ! Paste this in CUBE_CA_CERT
-----END CERTIFICATE-----
```

- CUBE_CA_CERT – Trustpoint label to associate certificate

# Authenticate and import the CA signed CUBE cert as shown below (Intermediate CA **NOT** present)

```
! If the root certificate does not have an intermediate CA, then
! proceed as shown below. Paste in the top-level root cert only
! that can authenticate the host (CUBE) cert

crypto pki authenticate CUBE_CA_CERT
<paste root CA X.64 based certificate here>
------BEGIN CERTIFICATE-----
… ! Paste this in Root_CA_CERT
------END CERTIFICATE-----

! Import the host(CUBE) certificate as shown below
crypto pki import CUBE_CA_CERT certificate
<paste CUBE CA X.64 based certificate here>
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
------BEGIN CERTIFICATE-----
… ! Paste this in CUBE_CA_CERT
------END CERTIFICATE-----
```

- CUBE_CA_CERT – Trustpoint label to associate certificate

# Specify the default trustpoint and TLS version under SIP-UA

```
sip-ua
 transport tcp tls v1.2
 crypto signaling default trustpoint CUBE_CA_CERT
```

- `transport tcp tls v1.2` – Default TLS version to be 1.2

# Step by Step CUBE config:
## Common Global Configuration

### Step 2:
### Trunk Enablement

# Configure Global CUBE settings
(voice service voip)

```
voice service voip
 ip address trusted list
  ipv4 X.X.X.X Y.Y.Y.Y  ! Check Webex Calling Port Reference Guide
 allow-connections sip to sip
 no supplementary-service sip refer
 no supplementary-service sip handle-replaces
 fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none
 sip
  early-offer forced
```

# Codec Lists

```
voice class codec 100
 codec preference 1 opus
 codec preference 2 g711ulaw
 codec preference 3 g711alaw
```

# Configure STUN to enable ICE-Lite

```
voice class stun-usage 100
 stun usage ice lite
```

- Used to enable STUN with ICE-Lite
- Will be applied to all Webex Calling facing dial-peers

# Enable SRTP Crypto and SIP Profiles

```
voice class sip-profiles 100
 rule 10 request ANY sip-header Contact modify "198.135.2.118" "sbc2.tmedemo.com"
 rule 20 response ANY sip-header Contact modify "198.135.2.118" "sbc2.tmedemo.com"
!
voice class srtp-crypto 100
 crypto 1 AES_CM_128_HMAC_SHA1_80
```

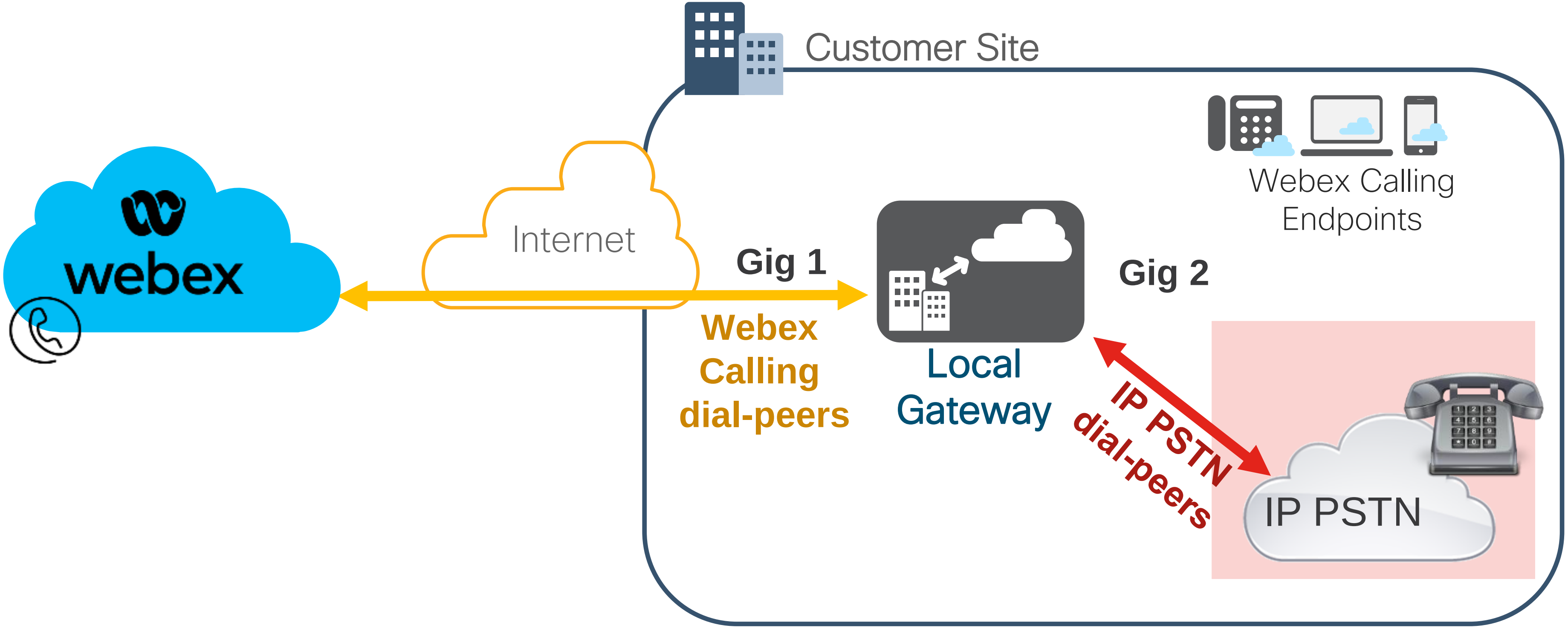
- Above SIP Profile applied to all Webex Calling facing dial-peers:
  - 198.135.2.118 is the IP address of the Local Gateway interface facing Webex Calling and sbc2.tmedemo.com is the FQDN of the enterprise SBC (Local Gateway) defined within Control Hub
  - Rules 10 and 20 ensure that the Local Gateway IP address is replaced with the FQDN in the Contact header of SIP request and response messages. This is a requirement for authentication of Certificate-based Local Gateway to be used as a trunk in Webex Calling

- **`crypto 1 AES_CM_128_HMAC_SHA1_80` -** Used to set the crypto cipher for the Webex Calling trunk.

# Step by Step CUBE config:

## Step 3:
## Call Routing

# Call Routing components



# Outbound Dial-peers to Webex Calling peering proxies

- The following 4 dial peers are used for load balancing
  1. Dial-peer voice 201 voip
  2. Dial-peer voice 202 voip
  3. Dial-peer voice 203 voip
  4. Dial-peer voice 204 voip

| Webex Calling edge proxy address (FQDN) |
|---|
| peering1.jp.sipconnect.bcld.webex.com:5062 |
| peering2.jp.sipconnect.bcld.webex.com:5062 |
| peering3.jp.sipconnect.bcld.webex.com:5062 |
| peering4.jp.sipconnect.bcld.webex.com:5062 |

- IP PSTN Inbound dial-peer **100** invokes voice class dpg **200**

```
voice class dpg 200
 description Incoming IP PSTN(DP100) to WxC(DP201/202/203/204)
 dial-peer 201 preference 1
 dial-peer 202 preference 1
 dial-peer 203 preference 1
 dial-peer 204 preference 1
```

- This dial-peer structure ensures LGW is maintaining multiple active bidirectional connections with Webex Calling edge proxies

# Outbound Dial-peer 201 – Towards WxC Proxy 1

```
dial-peer voice 201 voip
 description Outbound dial-peer towards Webex Calling Proxy 1
 destination-pattern BAD.BAD
 session protocol sipv2
 session target dns:peering1.us.sipconnect.bcld.webex.com:5062
 session transport tcp tls
 voice-class sip rel1xx disable
 voice-class codec 100
 voice-class stun-usage 100
 voice-class sip profiles 100
 voice-class sip srtp-crypto 100
 voice-class sip options-keepalive
 voice-class sip bind control source-interface GigabitEthernet 1
 voice-class sip bind media source-interface GigabitEthernet 1
 dtmf-relay rtp-nte
 srtp
 no vad
```

# Outbound Dial-peer 202 – Towards WxC Proxy 2

```
dial-peer voice 202 voip
 description Outbound dial-peer towards Webex Calling Proxy 2
 destination-pattern BAD.BAD
 session protocol sipv2
 session target dns:peering2.us.sipconnect.bcld.webex.com:5062
 session transport tcp tls
 voice-class sip rel1xx disable
 voice-class codec 100
 voice-class stun-usage 100
 voice-class sip profiles 100
 voice-class sip srtp-crypto 100
 voice-class sip options-keepalive
 voice-class sip bind control source-interface GigabitEthernet 1
 voice-class sip bind media source-interface GigabitEthernet 1
 dtmf-relay rtp-nte
 srtp
 no vad
```

# Outbound Dial-peer 203 – Towards WxC Proxy 3

```
dial-peer voice 203 voip
 description Outbound dial-peer towards Webex Calling Proxy 3
 destination-pattern BAD.BAD
 session protocol sipv2
 session target dns:peering3.us.sipconnect.bcld.webex.com:5062
 session transport tcp tls
 voice-class sip rel1xx disable
 voice-class codec 100
 voice-class stun-usage 100
 voice-class sip profiles 100
 voice-class sip srtp-crypto 100
 voice-class sip options-keepalive
 voice-class sip bind control source-interface GigabitEthernet 1
 voice-class sip bind media source-interface GigabitEthernet 1
 dtmf-relay rtp-nte
 srtp
 no vad
```

# Outbound Dial-peer 204 – Towards WxC Proxy 4

```
dial-peer voice 204 voip
 description Outbound dial-peer towards Webex Calling Proxy 4
 destination-pattern BAD.BAD
 session protocol sipv2
 session target dns:peering4.us.sipconnect.bcld.webex.com:5062
 session transport tcp tls
 voice-class sip rel1xx disable
 voice-class codec 100
 voice-class stun-usage 100
 voice-class sip profiles 100
 voice-class sip srtp-crypto 100
 voice-class sip options-keepalive
 voice-class sip bind control source-interface GigabitEthernet 1
 voice-class sip bind media source-interface GigabitEthernet 1
 dtmf-relay rtp-nte
 srtp
 no vad
```

# Outbound WxC Dial-peer 2000 – Towards Webex Calling

## edge proxy SRV address from Control Hub

```
dial-peer voice 2000 voip
 description Outbound dial-peer towards WxC Edge Proxy SRV Address
 destination-pattern BAD.BAD
 session protocol sipv2
 session target dns:us01.sipconnect.bcld.webex.com
 session transport tcp tls
 voice-class sip rel1xx disable
 voice-class codec 100
 voice-class stun-usage 100
 voice-class sip profiles 100
 voice-class sip srtp-crypto 100
 voice-class sip options-keepalive
 voice-class sip bind control source-interface GigabitEthernet 1
 voice-class sip bind media source-interface GigabitEthernet 1
 dtmf-relay rtp-nte
 srtp
 no vad
```

IOS-XE 17.9+

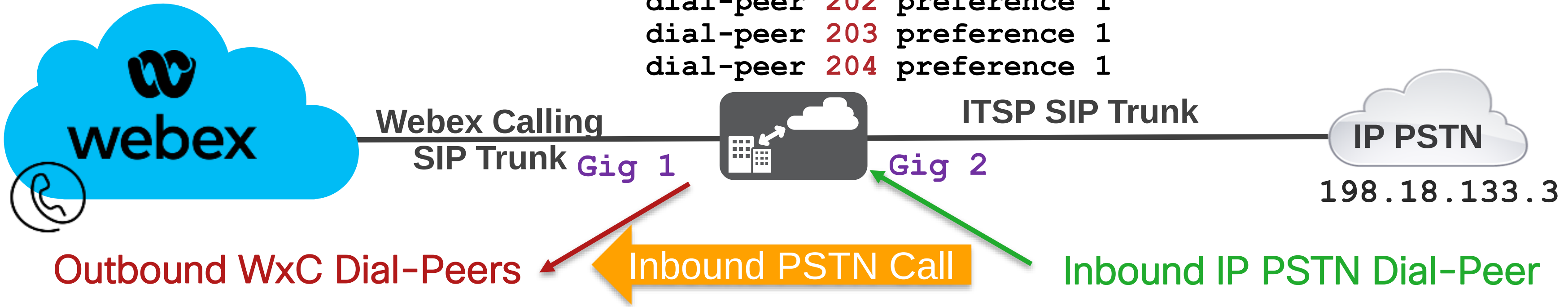
Webex Calling edge proxy address (SRV)

us01.sipconnect.bcld.webex.com

```
voice class dpg 200
 description Incoming IP PSTN(DP100) to WxC(DP2000)
 dial-peer 2000 preference 1
```

# Inbound PSTN Call

```
voice class dpg 200
 description Incoming IP PSTN(DP100) to WxC(DP201/202/203/204)
 dial-peer 201 preference 1
 dial-peer 202 preference 1
 dial-peer 203 preference 1
 dial-peer 204 preference 1
```




```
dial-peer voice 201 voip
 description Outbound dial-peer to Webex Calling Proxy 1
 session target dns:peering1.us.sipconnect.bcld.webex.com:5062

dial-peer voice 202 voip
 description Outbound dial-peer to Webex Calling Proxy 2
 session target dns:peering2.us.sipconnect.bcld.webex.com:5062

dial-peer voice 203 voip
 description Outbound dial-peer to Webex Calling Proxy 3
 session target dns:peering3.us.sipconnect.bcld.webex.com:5062

dial-peer voice 204 voip
 description Outbound dial-peer to Webex Calling Proxy 4
 session target dns:peering4.us.sipconnect.bcld.webex.com:5062
```

```
voice class uri 100 sip
  host ipv4:198.18.133.3

dial-peer voice 100 voip
  description Incoming dial-peer from IP PSTN
  incoming uri via 100
  session protocol sipv2
  destination dpg 200
  voice-class codec 100
  dtmf-relay rtp-nte
  no vad
```

# Inbound Dial-peer 200 – From Webex Calling

```
voice class uri 200 sip
 pattern sbc2.tmedemo.com  ← Local Gateway's FQDN
!
dial-peer voice 200 voip
 description inbound from Webex Calling
 session protocol sipv2
 session transport tcp tls
 incoming uri request 200
 destination dpg 100
 voice-class codec 100
 voice-class stun-usage 100
 voice-class sip profiles 100
 voice-class sip srtp-crypto 100
 voice-class sip bind control source-interface GigabitEthernet 1
 voice-class sip bind media source-interface GigabitEthernet 1
 dtmf-relay rtp-nte
 srtp
 no vad
```

FQDN

sbc2.tmedemo.com:5061

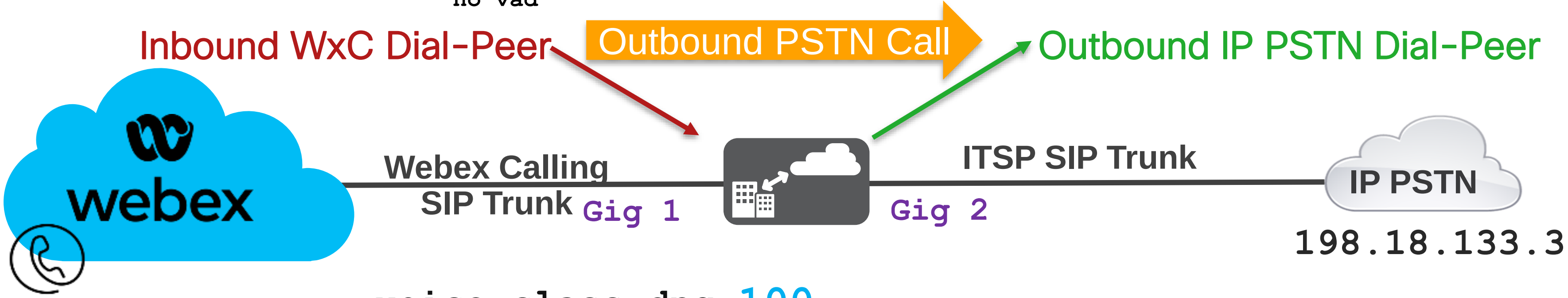
```
voice class dpg 100
 description Incoming WxC(DP200) to IP PSTN(DP101)
 dial-peer 101 preference 1
```

# Outbound PSTN Call

```
voice class uri 200 sip
  pattern sbc2.tmedemo.com

dial-peer voice 200 voip
 description inbound from Webex Calling
 session protocol sipv2
 session transport tcp tls
 destination dpg 100
 incoming uri request 200
 voice-class codec 100
 voice-class stun-usage 100
 voice-class sip profiles 100
 voice-class sip srtp-crypto 100
 voice-class sip bind control source-interface GigabitEthernet 1
 voice-class sip bind media source-interface GigabitEthernet 1
 dtmf-relay rtp-nte
 srtp
 no vad
```

```
dial-peer voice 101 voip
 description Outgoing dial-peer to IP PSTN
 destination-pattern BAD.BAD
 session protocol sipv2
 session target ipv4:198.18.133.3
 voice-class codec 100
 dtmf-relay rtp-nte
 no vad
```




```
voice class dpg 100
 description Incoming WxC(DP200) to IP PSTN(DP101)
 dial-peer 101 preference 1
```

# Registration-based Trunk
## Pros and Cons

### Pros:

- CUBE can sit on internal network behind a NAT/firewall
  - No need for the customer to expose CUBE’s external interface
  - No need for the customer to setup a DMZ
- Easier to deploy: achieves security without a need for certificates
- Recommended method
- Config Validation from the Control Hub

### Cons:

- Limited scale (single TCP/TLS connection)
  - Scales upto 250 calls (OTT), 500+ (Interconnect)
- Sensitive to network impairments (all calls affected when TCP/TLS connection is lost)

# Certificate-based Trunk
## Pros and Cons

### Pros:

- Higher scale, up to CUBE platform limits (multiple TCP/TLS connections)
- Better resilience (each call is independent)
  - Network drop does not impact new calls as the call could land on the new connection
- Both sides (Webex Calling Access SBC and CUBE) can create connections on demand

### Cons:

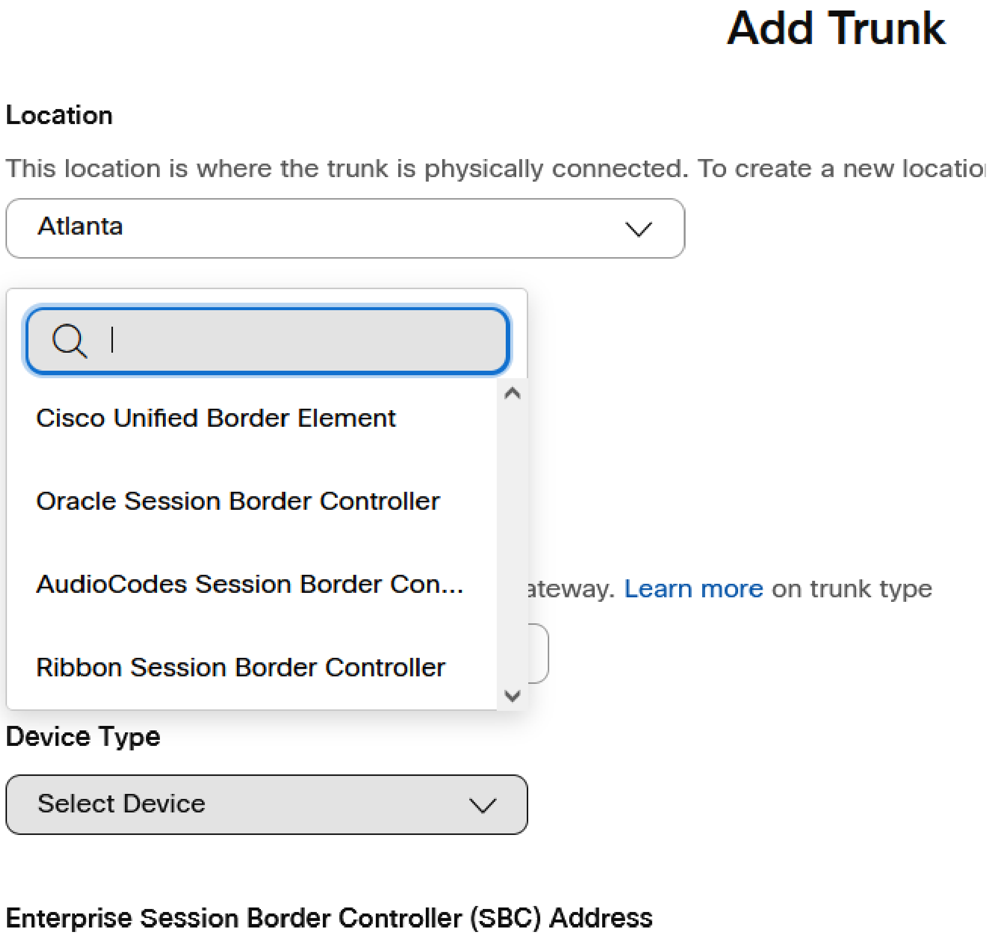
- CUBE must be reachable from the cloud (public IPv4 address on the external interface with inbound FW rules) [CUBE can be behind static NAT]
  - Customer will need to publish an FQDN (IOS-XE 17.6+ - current help.Webex documentation) or SRV (IOS-XE 17.9+) for WxC to reach the LGW
- Requires certificates signed by public CA on each CUBE and a DNS SRV

# 3rd Party SBC as a Local Gateway

# Oracle SBC is now
## Certificate-based only

Oracle conducted tests with SBC 9.0 software – this on any of the following products:

- AP 1100
- AP 3900
- AP 4600
- AP 6300
- AP 6350
- AP 3950 (Starting from SBC 9.0 version)
- AP 4900 (Starting from SBC 9.0 version)
- VME
- Oracle SBC on Public Cloud

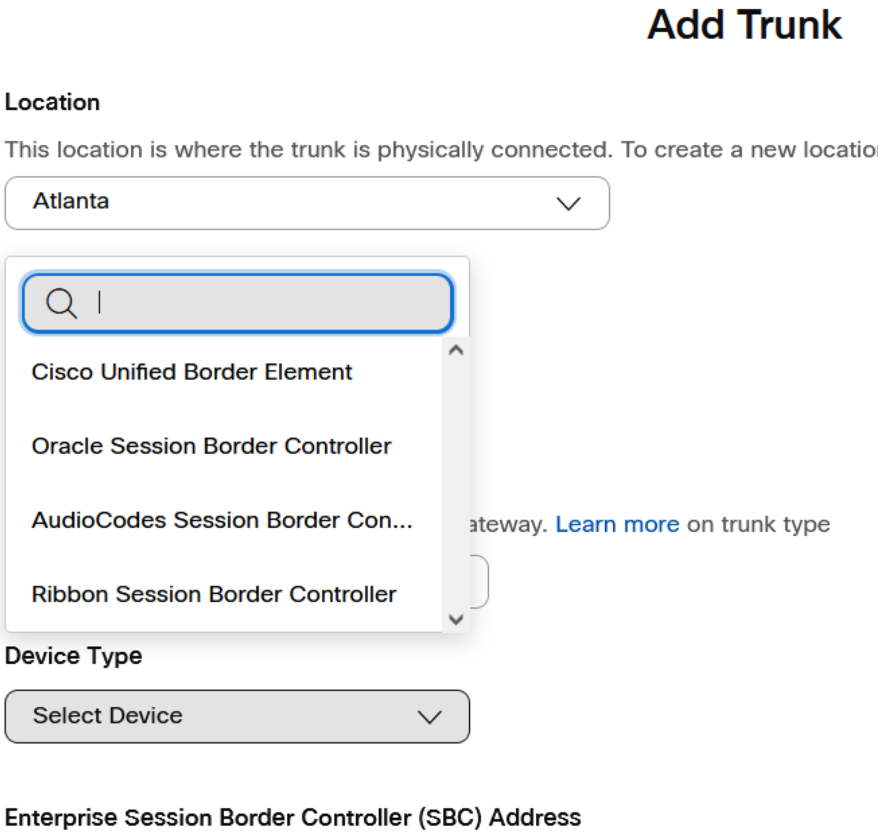



- [Configuration Guide]

# AudioCodes SBC is now supported as LGW

## Certificate-based only

| AudioCodes |
|---|
| Mediant 500 Gateway & E-SBC<br>Mediant 800B/C Gateway & E-SBC<br>Mediant 1000B Gateway & E-SBC<br>Mediant 2600 E-SBC<br>Mediant 4000/B SBC<br>Mediant 9000, 9030, 9080 SBC<br>Mediant Software SBC (VE/SE/CE) |
| 7.40A.250.440 or later |



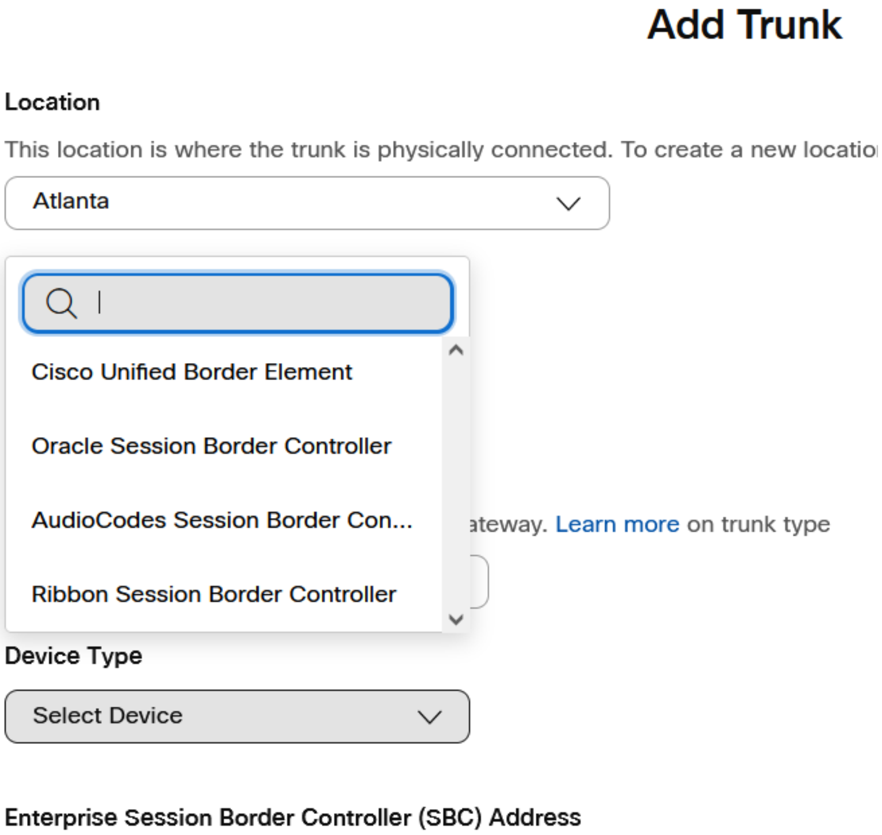

[Configuration Guide]

# Ribbon SBC is now supported as LGW

## Certificate-based only

| Ribbon Platform | Ribbon Code Version |
| --- | --- |
| SBC 5000 | 10.1.0 |
| SBC 7000 | |
| SBC SWe | |

[Configuration Guide]



# Resources

# Resources

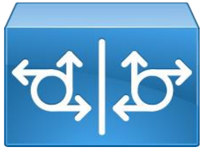
For more information take a look at the following resources:

- What's new in Webex Calling: https://help.webex.com/en-us/article/rdmb0/What's-new-in-Webex-Calling
- Trunk configuration guide: Webex Calling Trunks
- Configure Local Gateway on Cisco IOS XE for Webex Calling https://help.webex.com/en-us/article/jr1i3r/Configure-Local-Gateway-on-Cisco-IOS-XE-for-Webex-Calling
- https://help.webex.com/en-us/article/n0xb944/Configure-Trunks,-Route-Groups,-and-Dial-Plans-for-Webex-Calling

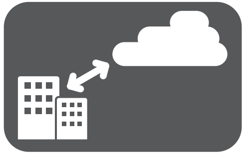
# Resources

- Enroll Cisco IOS Managed Gateways to Webex Cloud
- Assign Services to Managed Gateways
- Validate Cisco Local Gateway Configuration through Control Hub
- Webex Integrations: Webex Integrations > Oracle
- Oracle SBC integration with Cisco Webex Calling as 3rd party Local Gateway (LGW) https://www.oracle.com/a/otn/docs/oracle-sbc-integration-with-cisco-webex-calling-v1.0.pdf

# Additional sessions on IOS-XE UC
## (CUBE, Local Gateway, Survivability Gateway)



- BROCOL-2314 CUBE v14 Updates
- **Session Room A4 – Tuesday 1:45PM – 2:45PM**



- BRKCOL-2312 High-Capacity Premises-based PSTN Option for Webex Calling
  - **Session Room A1 – Wednesday 2:30PM – 3:30PM**
- Walk-in-Lab: LABCOL-2417 Local Gateway for Webex Calling

- BRKCOL-2993 Enabling Site Survivability for Webex Calling
  - **Session Room A9 – Thursday 10:30AM – 11:30AM**
- Walk-in-Lab: LABCOL-2416 Site Survivability for Webex Calling

# Thank you

# Let’s go