AWS Direct Connect for Amazon Chime SDK Voice Connector

AWS White Paper

First published January 10, 2023

Last updated January 10, 2023

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract and introduction 4

Abstract 4

Are you Well-Architected? 4

Introduction 4

Technical overview 6

Connecting 7

Physical cross-connect 7

Carrier interconnection 8

Data center interconnection 10

Virtual interfaces (VIF) 11

Network Requirements 12

Scope BGP communities 13

Set up your network 16

Amazon Chime SDK Voice Connector AWS Region selection considerations 17

Using Voice Connector Groups for resilience 17

Conclusion 17

Contributors 18

Further reading 18

Document revisions 18

Abstract and introduction

Abstract

Today, network engineers and voice application builders want to use Amazon Chime SDK Voice Connector (Voice Connector) in conjunction with AWS Direct Connect to provide secure and reliable Session Initial Protocol (SIP) trunking. This whitepaper provides guidance on the best practices, architectural considerations, and technical requirements for using these services together.

Are you Well-Architected?

The AWS Well-Architected Framework helps you understand the pros and cons of the decisions you make when building systems in the cloud. The six pillars of the Framework allow you to learn architectural best practices for designing and operating reliable, secure, efficient, cost-effective, and sustainable systems. Using the AWS Well-Architected Tool, available in the AWS Management Console, you can review your workloads against these best practices by answering a set of questions for each pillar.

For more expert guidance and best practices for your cloud architecture—reference architecture deployments, diagrams, and whitepapers—refer to the AWS Architecture Center.

Introduction

Amazon Chime SDK Voice Connector is a pay-as-you-go SIP trunking service. It is tested for interoperability with many common SIP-based Private Branch Exchanges (PBXs), call centers, and Session Border Controllers (SBCs). Voice Connector enables customers to connect on-premises phone systems to the public telephone network and/or Amazon artificial intelligence (AI), machine learning (ML) and business intelligence (BI) services, such as Amazon Transcribe and Amazon Comprehend. Access to Voice Connector is provided via the Internet or via AWS Direct Connect, with management via the AWS Management Console.

For some organizations the use of AWS Direct Connect is a prerequisite to using Voice Connector. Common examples behind this include:

- Public sector and regulated industries with elevated encryption requirements.
- Customers with a history of poor internet service that require service levels with providers to improve network conditions.

- Customers whose security protocols require minimization of traffic exposure to a public wide area network (WAN).
- Customers with requirements for resiliency over public and private links.

Public sector and regulated industries with elevated encryption requirements

Voice Connector can be configured to use Transport Layer Security (TLS) to encrypt signaling and messaging traffic, and Secure Real-time Transport Protocol (SRTP) to encrypt voice traffic. This is intended to help ensure that traffic is protected from interception and snooping. The use of TLS encryption is dependent upon the customer's remote SIP system being able to support this secure transport method.

For an additional layer of security, including when the use of TLS is not possible, and to help protect against man-in-the-middle attacks, you can use AWS Direct Connect. AWS Direct Connect supports MACsec encryption to further encrypt traffic between your network and AWS infrastructure.

Customers with a history of poor internet service that require service levels with providers to improve network conditions

While software as a service (SaaS) adoption over public internet is both widely used and reliable, there are circumstances where organizations may require a service level guarantee on throughput and latency that private links can provide. For these use cases, AWS Direct Connect lets you route traffic across dedicated links to the AWS Cloud. There are two key stages, outlined in more detail below, but summarized as:

1. Establishing a network circuit between your premise and an AWS Region. There are three options. Circuits are provided by third party suppliers and generally include a service level guarantee.
2. Create a virtual interface over the circuit to connect to the public IP addresses of the AWS services to be used. Each service will be covered by a service level agreement provided by AWS.

Customers whose security protocols require minimization of traffic exposure to public WAN

Similar to the previous use cases, customers may have security policies in place to prevent business critical information from traversing the public internet. These customers can use dedicated links to avoid routing traffic through the public internet.

Note that even though data is routed with public addresses, the public addresses are advertised through the Direct Connect service. Because of this, a more specific route is available, which causes the router to select the route over Direct Connect rather than the public Internet.

Customers with requirements for resiliency over public and private links

In some cases, meeting business-defined uptime requirements may require redundant or resilient connectivity links. There are cases when multiple internet service providers (ISPs) are unavailable at specific locations, or additional ISPs may utilize the same fiber links as the incumbent ISP. AWS Transit Gateway peering provides you with a simple and cost-effective way to share resources between AWS Regions or replicate data for geographic redundancy. For more information about Transit Gateway peering, refer to AWS Transit Gateway features. Additionally, AWS Direct Connect provides a number of resiliency recommendations.

Technical overview

This whitepaper outlines how Amazon Chime SDK Voice Connector can be implemented with AWS Direct Connect services to help provide secure and reliable SIP trunking. The white paper also provides details to ensure that the signaling, messaging, and voice payloads route correctly over the AWS Direct Connect service to the Voice Connector public IP addresses.

There are five simple steps to configure Direct Connect for operation with Voice Connector:

1. Establish a connection in an AWS Direct Connect location.
2. Set up a Direct Connect Public Virtual Interface.
3. Select the Border Gateway Protocol (BGP) community tags for region, continental, or global.
4. Set up and advertise an 802.1q virtual local area network (VLAN).
5. Route traffic to the advertised Voice Connector addresses.

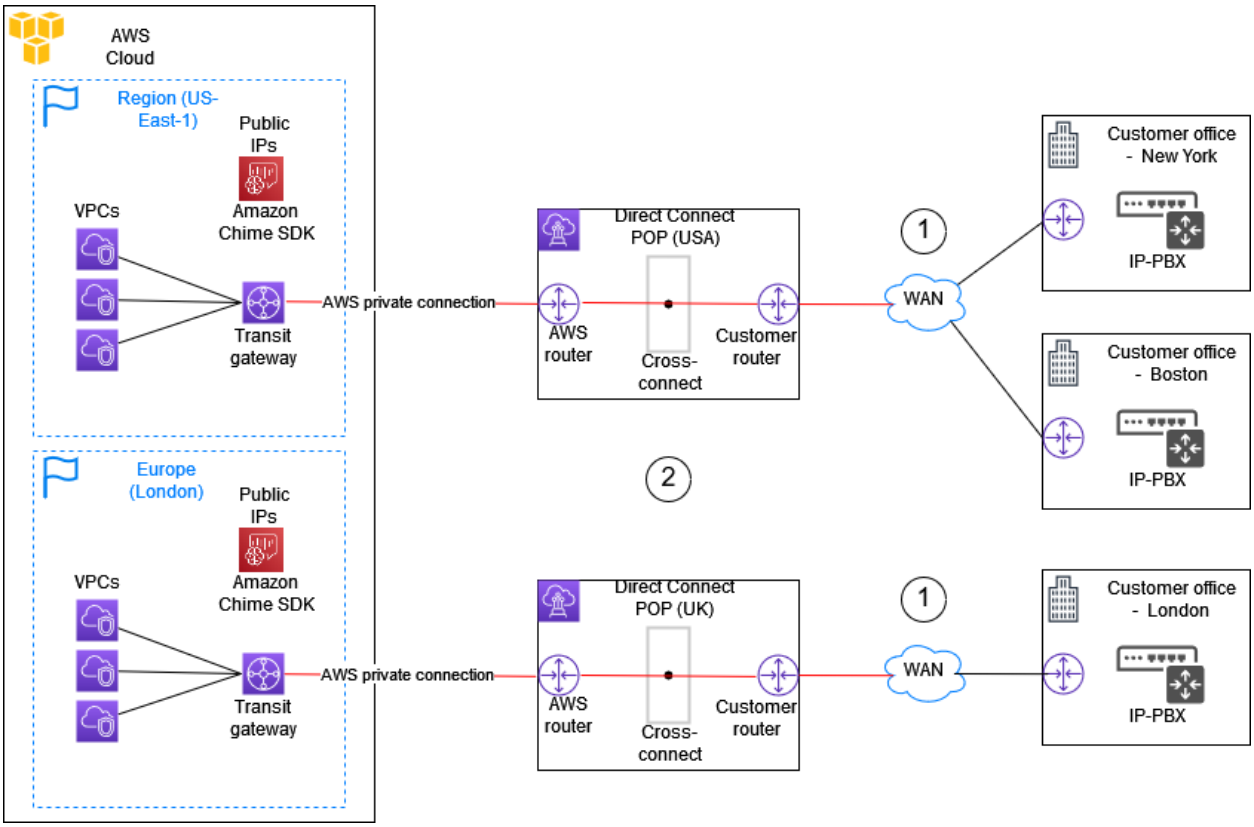
Connecting

There are three primary methods for connecting to AWS with Direct Connect:

- Physical cross-connect
- Carrier interconnection
- Data center interconnection

Physical cross-connect

First, we'll discuss using a physical cross-connect to establish a network connection from your premises to an AWS Region. This topology utilizes a partner in the AWS Direct Connect Partner Program to establish network circuits between an AWS Direct Connect point-of-presence (POP) and your data center, office, or colocation environment.



As indicated by the numbers on the diagram:

1. **Connections** – Create a connection in an AWS Direct Connect Point of Presence (POP) to establish a network connection from your premises to an AWS Region.
2. **AWS Direct Connect location (DX POP)** – Work with a partner in the AWS Direct Connect Partner Program to help you establish network circuits between an AWS Direct Connect POP and your data center, office, or colocation environment. The Partner can also help provide collocation space within the same facility as the POP location.

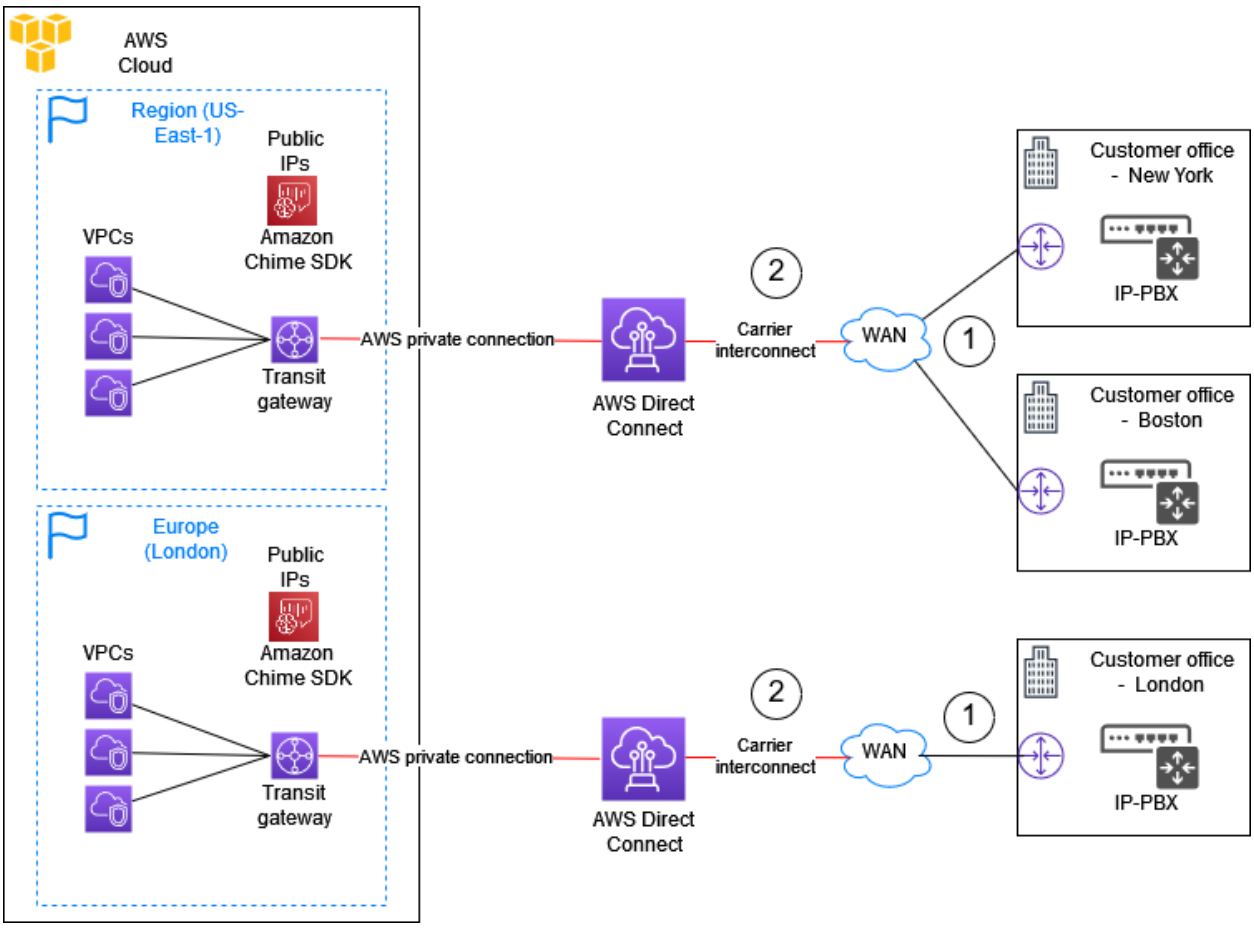
Note: **Port speed** – The possible values are one Gbps, 10 Gbps, and 100 Gbps. You cannot change the port speed after you create the connection request. To change the port speed, you must create and configure a new connection.

Customer router requirements

The interface must use single-mode fiber with a 1000BASE-LX (1310 nm) transceiver for 1 gigabit ethernet, a 10GBASE-LR (1310 nm) transceiver for 10 gigabits, or a 100GBASE-LR4 for 100 gigabit ethernet. Auto-negotiation for a port must be disabled for a connection with a port speed of more than one Gbps. However, depending on the AWS Direct Connect endpoint serving your connection, auto-negotiation might need to be enabled or disabled for one Gbps connections.

Carrier interconnection

Next, we'll discuss using carrier interconnection to establish a network connection from your premises to an AWS Region. This topology uses existing WAN services, such as Multiprotocol Label Switching, or MPLS, to provide the connection between your data center, office, or colocation environment to AWS.



As indicated by the numbers on the diagram:

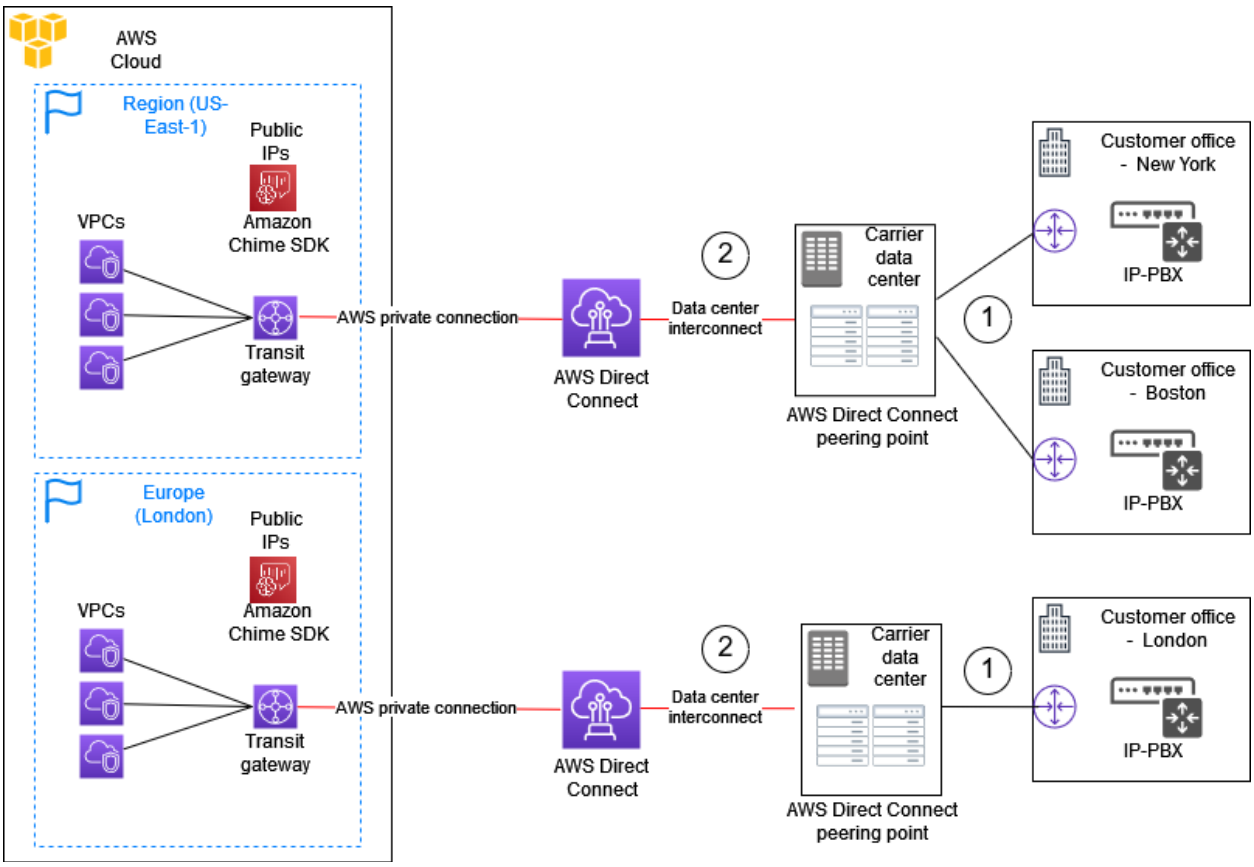
1. **Connections** – Create a connection with an independent service provider (carrier) to establish a network connection from your premises to an AWS Region. In this case, the carrier will provide a virtual network connection (VLAN) to AWS using the existing WAN service (such as Multiprotocol Label Switching, or MPLS). Customers choosing this method of connection will usually already have a carrier service that has the option for virtual onramp service to AWS.

   Examples of carriers that can provide this service are:
   - AT&T with Netbond
   - Verizon with Software Defined Interconnect
   - CenturyLink with Cloud Connect

2. **Port speed** – You will subscribe to a port speed from the carrier. Although AWS Direct Connect is fixed at 1 Gbps, 10 Gbps, or 100 Gbps, carriers can provide a variety of different speeds over the existing WAN connection.

Data center interconnection

Finally, we'll discuss using a data center interconnection to establish a network connection from your premises to an AWS Region. This topology utilizes a physical connection in a data center to a private network and virtual network connection, or VLAN, to AWS.



As indicated by the numbers on the diagram:

1. 1. **Connections** – Create a connection with an independent service provider (data center) to establish a network connection from your premises to an AWS Region. In this case, the data center will provide a physical connection to their private network and a virtual network connection (VLAN) to AWS. Customers choosing this method of connection generally will already have a presence in a data center that provides private onramp service to AWS.

   Examples of data centers that can provide this service are:
   - Equinix with Equinix Cloud Exchange
   - Switch with Switch Cloud Platform

2. **Port speed** – You will subscribe to a port speed from the data center. Although AWS Direct Connect is fixed at 1 Gbps, 10 Gbps, or 100 Gbps, data centers can provide a variety of different speeds over their private network connections.

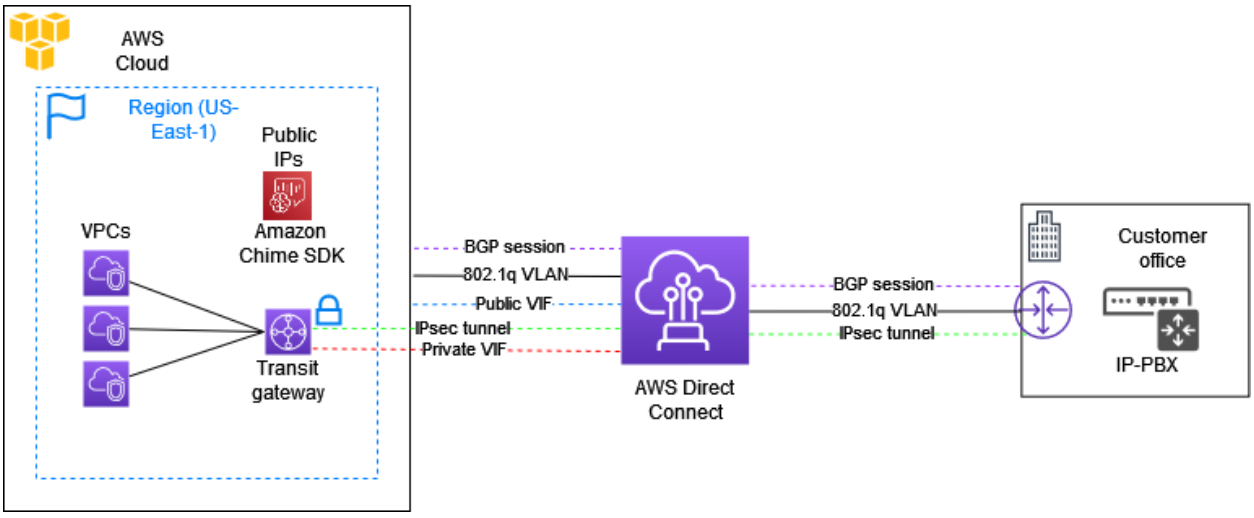
Virtual interfaces (VIF)

With these connections, you can create virtual interfaces directly to public AWS services (for example, to Amazon Simple Storage Service (Amazon S3) or Amazon Chime SDK Voice Connectors) or to Amazon virtual private cloud (VPC), bypassing internet service providers in your network path. An AWS Direct Connect point-of-presence (AWS DX POP), carrier interconnection, or data center interconnection provides access to AWS in the AWS Region with which it is associated. You can use a single connection in an AWS Region or AWS GovCloud (US) to access public AWS services in all other AWS Regions.

A public virtual interface (public VIF) enables access to public services such as Amazon S3 or Amazon Chime SDK Voice Connector. A private virtual interface (private VIF) enables access to your VPC and hosted workloads. A transit virtual interface (transit VIF) is used to access one or more Amazon Transit Gateways associated with Direct Connect gateways.

For information on the public IP address requirements of Direct Connect, refer to the AWS Direct Connect FAQ.

Voice Connector is a publicly addressed service. The inbound (from customer premise) allowed IP list can specify a single /32 host up to a /27 subnet with 30 hosts.



Network Requirements

To use AWS Direct Connect, your network must meet the following conditions:

- Your network is collocated with an existing AWS DX POP, or you are working with an AWS Direct Connect partner who is a member of the AWS Partner Network (APN), or you are working with an independent service provider to connect to AWS Direct Connect.
- The AWS Direct Connect network segment is configured to support:
    - 802.1Q VLAN encapsulation must be supported across the entire connection, including intermediate devices.
    - BGP and BGP MD5 authentication.

AWS Direct Connect supports both the IPv4 and IPv6 communication protocols. IPv6 addresses provided by public AWS services are accessible through AWS Direct Connect Public VIF.

To access public resources in a remote AWS Region, you must set up a public VIF and establish a BGP session. After you have created a public VIF and established a BGP session to it, your router learns the routes of the other public AWS Regions.

AWS Direct Connect applies inbound (from your on-premises data center) and outbound (from your AWS Region) routing policies for a public AWS Direct Connect connection. You can also use BGP community tags on routes advertised by Amazon and apply BGP community tags on the routes you advertise to Amazon.

AWS Direct Connect locations in AWS Regions or AWS GovCloud (US) can access public services in any other AWS Region excluding China (Beijing and Ningxia). In addition, AWS Direct Connect connections in AWS Regions or AWS GovCloud (US) can be configured to access a VPC in your account in any other AWS Region excluding China (Beijing and Ningxia). You can, therefore, use a single AWS Direct Connect connection to build multi-AWS Region services.

All networking traffic remains on the AWS global network backbone, regardless of whether you access public AWS services or a VPC in another AWS Region.

Scope BGP communities

You can apply BGP community tags on the public prefixes that you advertise to Amazon to indicate how far to propagate your prefixes in the Amazon network for:

- The local AWS Region only,
- All AWS Regions within a continent, or
- All AWS Regions.

You can use the following BGP communities for your prefixes:

- 7224:9100-Region (local AWS Region)
- 7224:9200-Continental (all AWS Regions for a continent)
    - North America
    - Asia Pacific
    - Europe, the Middle East, and Africa
- 7224:9300-Global (all public AWS Regions)

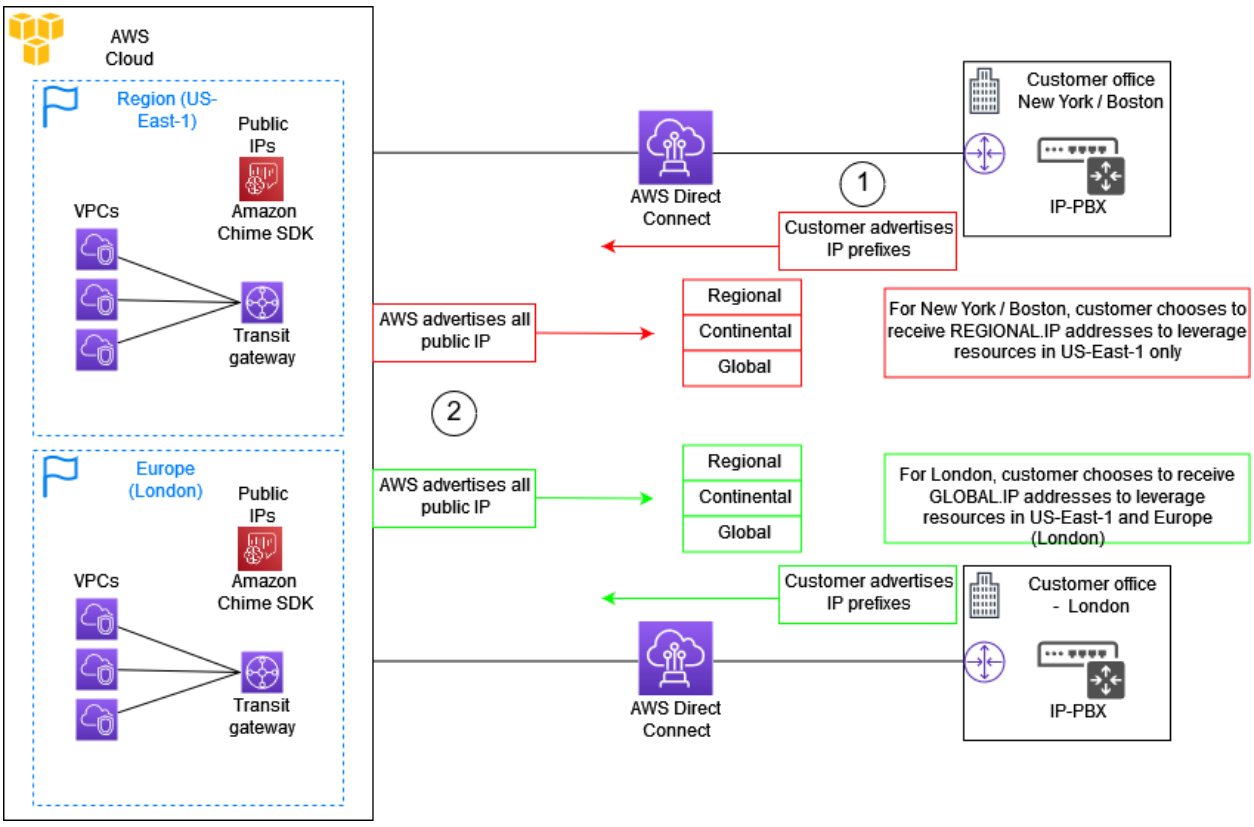
Note If you do not apply any community tags, prefixes are advertised to all public AWS Regions (globally) by default.

The communities 7224:1-7224:65535 are reserved by AWS Direct Connect.

AWS Direct Connect applies the following BGP communities to its advertised routes:

- 7224:8100 – Routes that originate from the same AWS Region in which the AWS Direct Connect point of presence is associated
- 7224:8200 – Routes that originate from the same continent with which the AWS Direct Connect point of presence is associated
- No tag – Global (all public AWS Regions) Communities that are not supported for an AWS Direct Connect public connection are removed.

Note If you do not apply any community tags, all AWS public IP addresses will be advertised into the customer network. Apply tags to limit the exposure into your network.



1. **Customer-advertised IP prefixes** – Public prefixes advertised to Amazon network
2. **AWS-advertised public addresses** – AWS public service IP addresses advertised over BGP

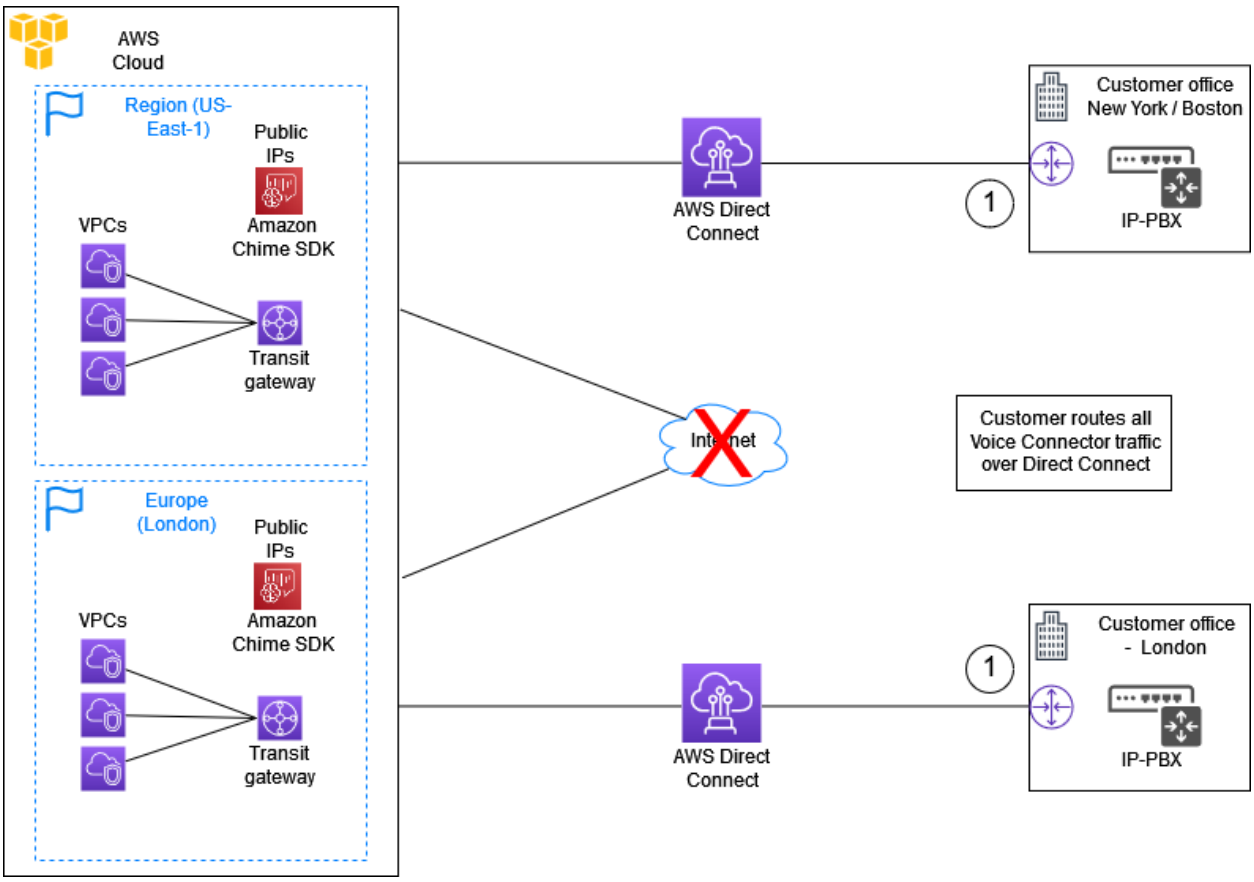
When you're using AWS Direct Connect to access public AWS services, you must specify the public IPv4 prefixes or IPv6 prefixes (where applicable) to advertise over BGP.

The following inbound routing policies apply:

- You must own the public prefixes, and they must be registered as such in the appropriate AWS Regional internet registry.
- Traffic must be destined to Amazon public prefixes. Transitive routing between connections is not supported.
- AWS Direct Connect performs inbound packet filtering to validate that the source of the traffic originated from your advertised prefix.

The following outbound routing policies apply:

- AS_PATH and longest prefix match is used to determine the routing path, and AWS Direct Connect is the preferred path for traffic sourced from Amazon.
- AWS Direct Connect advertises all local and remote AWS Region prefixes where available, and includes on-net prefixes from other AWS non-region points of presence (POP) where available: for example, Amazon CloudFront and Amazon Route 53.
- AWS Direct Connect advertises prefixes with a minimum path length of three.
- AWS Direct Connect advertises all public prefixes with the well-known NO_EXPORT BGP community.
- If you have multiple AWS Direct Connect connections, you can adjust the load sharing of inbound traffic by advertising prefixes with similar path attributes.
- The prefixes advertised by AWS Direct Connect must not be advertised beyond the network boundaries of your connection. For example, these prefixes must not be included in any public internet routing table.
- AWS Direct Connect keeps prefixes advertised by customers within the Amazon network. AWS does not re-advertise customer prefixes learned from a public virtual interface (VIF) to any of the following:
    - Other AWS Direct Connect customers
    - Networks that peer with the AWS Global Network
    - Amazon's transit providers



As indicated by the number on the diagram:

1. **Connections** – Direct Connect routing of Amazon Connect traffic.

Set up your network

Amazon Chime SDK requires the destination IPs and ports described in the Amazon Chime SDK Administrator Guide to have been allowed on customers' firewalls to enable access to the various services. If inbound or outbound traffic is blocked, this blockage might affect the ability to use various services, including audio, video, screen sharing, or chat.

Please refer to the Amazon Chime SDK Administrator Guide for the full port range and destination IP addresses.

Amazon Chime SDK Voice Connector AWS Region selection considerations

Your Amazon Chime SDK Voice Connector region selection may be contingent on a number of factors such as data governance requirements, use cases, service availability in each AWS Region, and latency in relation to your SIP gateway.

Voice Connector connectivity traverses the wide area network (WAN), so it is important that the SIP gateway has the lowest latency and fewest hops possible to the AWS Region where your Voice Connector is hosted.

When you set up your Voice Connector, consider creating your instance in the AWS Region that is geographically closest to your SIP gateway. If you need to set up an instance in a specific AWS Region to comply with company policies or other regulations, choose the configuration that results in the fewest network hops between your SIP gateway and your Voice Connector AWS Region.

Using Voice Connector Groups for resilience

The Amazon Chime SDK Voice Connector can help address several business concerns. Firstly, for customers utilizing PSTN inbound and outbound services, AWS provides carrier diversity. Secondly, the Voice Connector services are deployed across multiple Availability Zones within a AWS Region. Availability Zones are physically separated and isolated infrastructure, connected with low-latency, high-throughput, and highly redundant networking. Thirdly, Voice Connectors can be combined into a Voice Connector Group. Within this Group, each Voice Connector can be given a priority so that one may be prioritized over another, or they can be treated with the same priority, effectively load balancing traffic across them. Voice Connectors from different AWS Regions can be added to the same group to provide geographic redundancy, for example between US East (N. Virginia) and US West (Oregon).

Conclusion

Combining AWS Direct Connect with Amazon Chime SDK Voice Connector can resolve several business concerns that affect some customers, such as security availability and reliability. There are a number of considerations on architectural design and configuration to support this topology. Understanding the different design requirements and how to accomplish them is crucial to creating a functional implementation plan to support these needs.

Contributors

Contributors to this document include:

- Trevor Davis, Senior Technical Product Manager, Amazon Web Services
- Marc Wynter, Senior Solutions Architect, Amazon Web Services
- Greg Smith, Senior Solutions Architect, Amazon Web Services
- Greg Thomas, Scaling Solutions Architect, Amazon Web Services
- James Lamanna, Senior Principal SDE, Amazon Web Services

Further reading

For additional information, refer to:

- AWS Architecture Center
- AWS Whitepapers page
- What is AWS Direct Connect? (AWS documentation)
- Amazon Chime SDK Networking configuration and bandwidth requirements (AWS documentation)
- Routing policies and BGP communities (AWS documentation)

Document revisions

Date	Description
November 09, 2022	Initial draft created.
January 10, 2023	First publication