AWS Whitepaper

AWS Direct Connect for Amazon Connect

AWS Direct Connect for Amazon Connect: AWS Whitepaper

Table of Contents

AWS Direct Connect for Amazon Connect

Publication date: **November 2, 2022** (*Document revisions*)

Abstract

Many contact centers and security architects want to use Amazon Connect in conjunction with AWS Direct Connect. This whitepaper outlines best practices, architecture 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 at no charge 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 Connect is an easy-to-use omnichannel cloud contact center service that can operate over any public internet connection. For most customers, this means you can build an enterprise-grade contact center that can easily scale from a handful of agents to tens of thousands of agents—and your agents can log in with nothing but a web browser and headset.

However, there are edge cases that might dictate private connectivity between the contact center and your AWS Cloud. Common scenarios that elicit this requirement 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

Amazon Connect uses Transport Layer Security (TLS) to encrypt signaling and messaging traffic and Secure Real-time Transport Protocol (SRTP) to encrypt voice traffic, to ensure that traffic is protected from interception and snooping. There are times when organizations require additional hardening to prevent the possibility of man-in-the-middle attacks. You can use AWS Direct Connect to minimize exposure. AWS Direct Connect supports MACsec encryption to further encrypt traffic between the customer's contact center 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 contact centers may require the service level guarantees 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.

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 public internet. These customers can use dedicated links to avoid routing 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 at the customer's router, which prioritizes this private routing of data over the Direct Connect service. Once the traffic reaches the AWS edge routers in the Region, a network address translation takes place to reach the internal service.

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 ride the same fiber links as the incumbent ISP. With AWS Direct Connect, customers can use a Site-to-Site VPN over private connections as well as public connections independently, to allow for maximum resilience to ISP or private networks. For more information about Transit Gateway peering and multicast, refer to AWS Transit Gateway features.

Technical overview

This whitepaper outlines the ease with which Amazon Connect users of the agent Contact Control Panel (CCP or Agent UI) can ensure that data flows across new or existing Direct Connect services, and that customers realize the benefits of doing so. It also provides the context of using the Amazon Connect CCP, and ensures that the signaling, messaging, and voice payload flows over the AWS Direct Connect service to the Amazon Connect public IP addresses.

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

1. Connect—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—Regional, continental, or global.
4. Set up and advertise an 802.1q virtual local area network (VLAN).
5. Route CCP traffic to advertised Amazon Connect addresses.

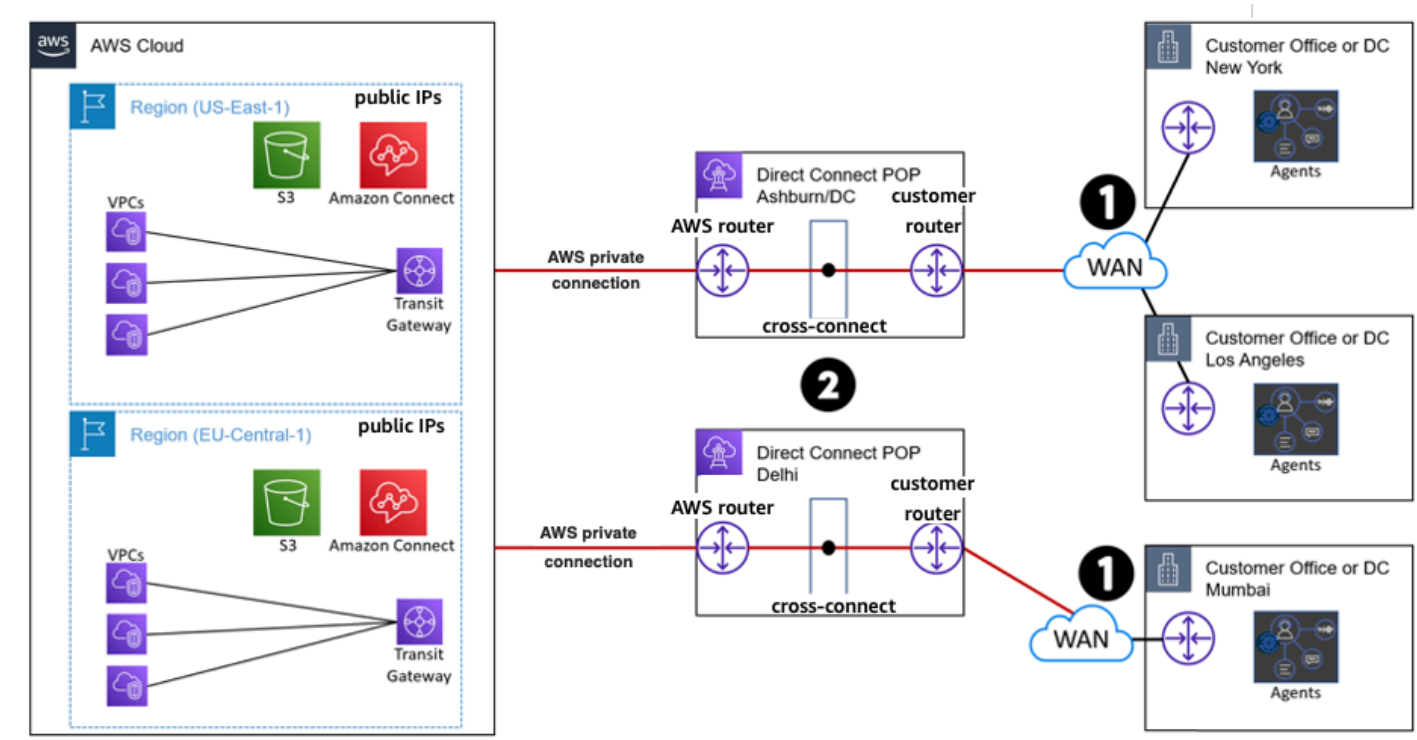
Connect

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.



Reference architecture for a physical cross-connect to Direct Connect

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.

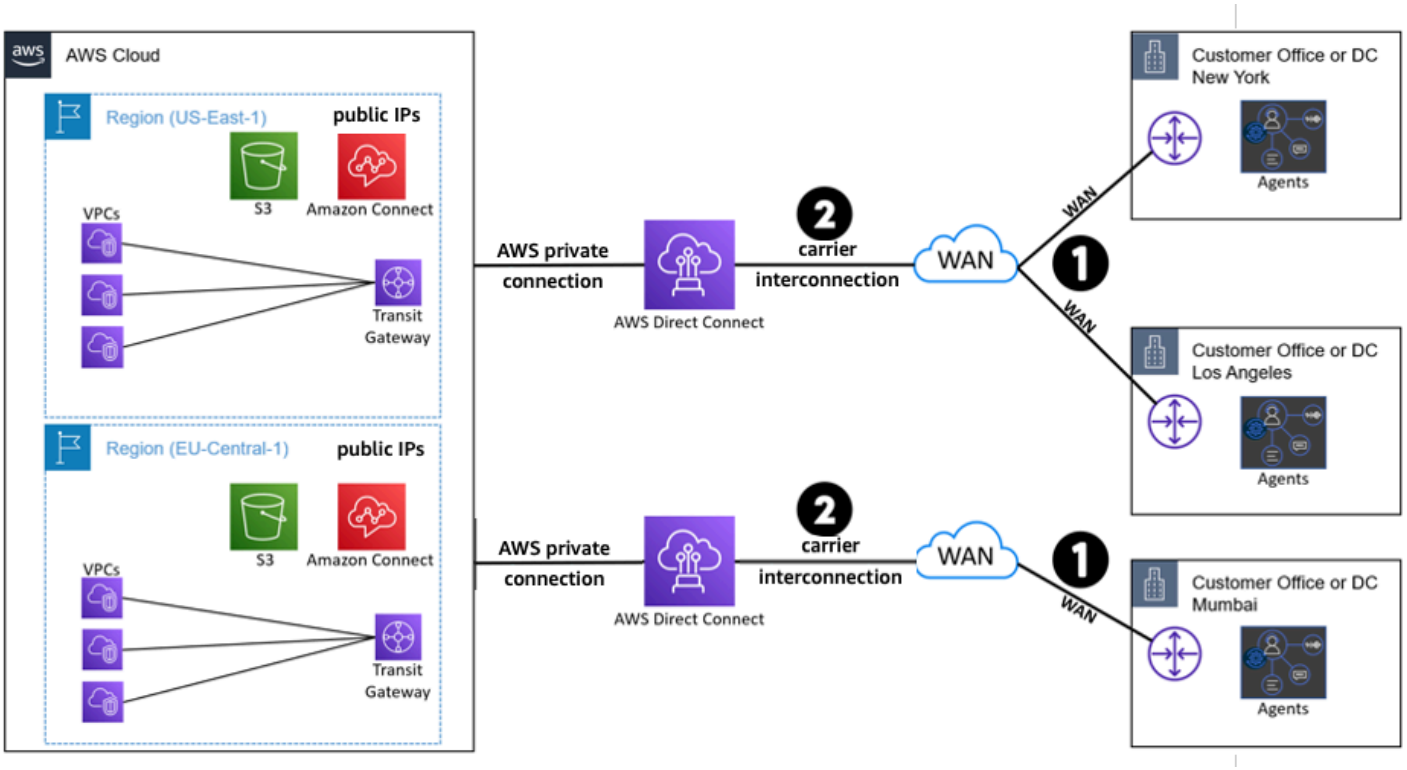
- **Port speed** — The possible values are one Gbps, 10 Gbps, and 100 Gbps. You cannot change the port speed after you create the connection request. To change the port speed, you must create and configure a new connection.

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.



Reference architecture for carrier interconnection to Direct Connect

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.

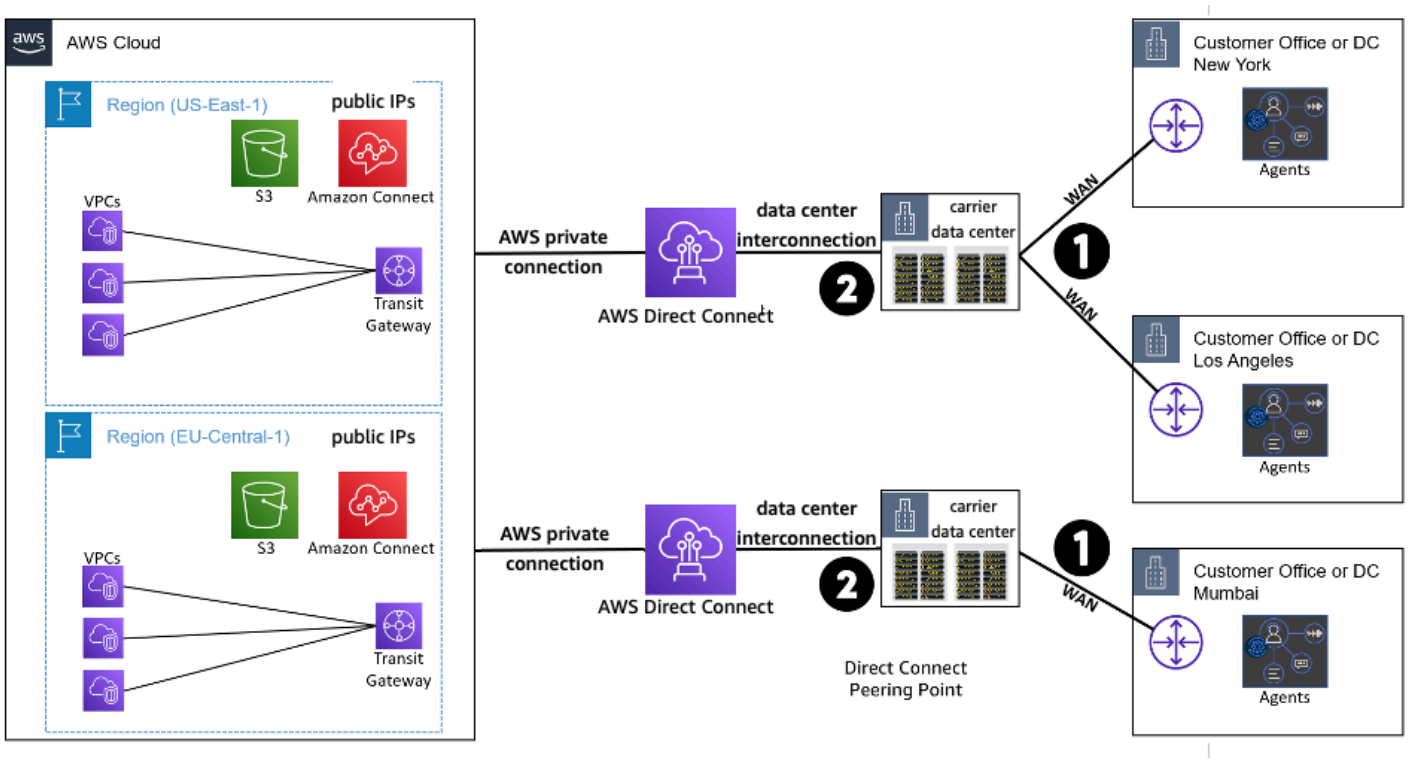
   Examples of carriers that can provide this service are:

   - 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.



Reference architecture for data center interconnection to Direct Connect

As indicated by the numbers on the diagram:

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:

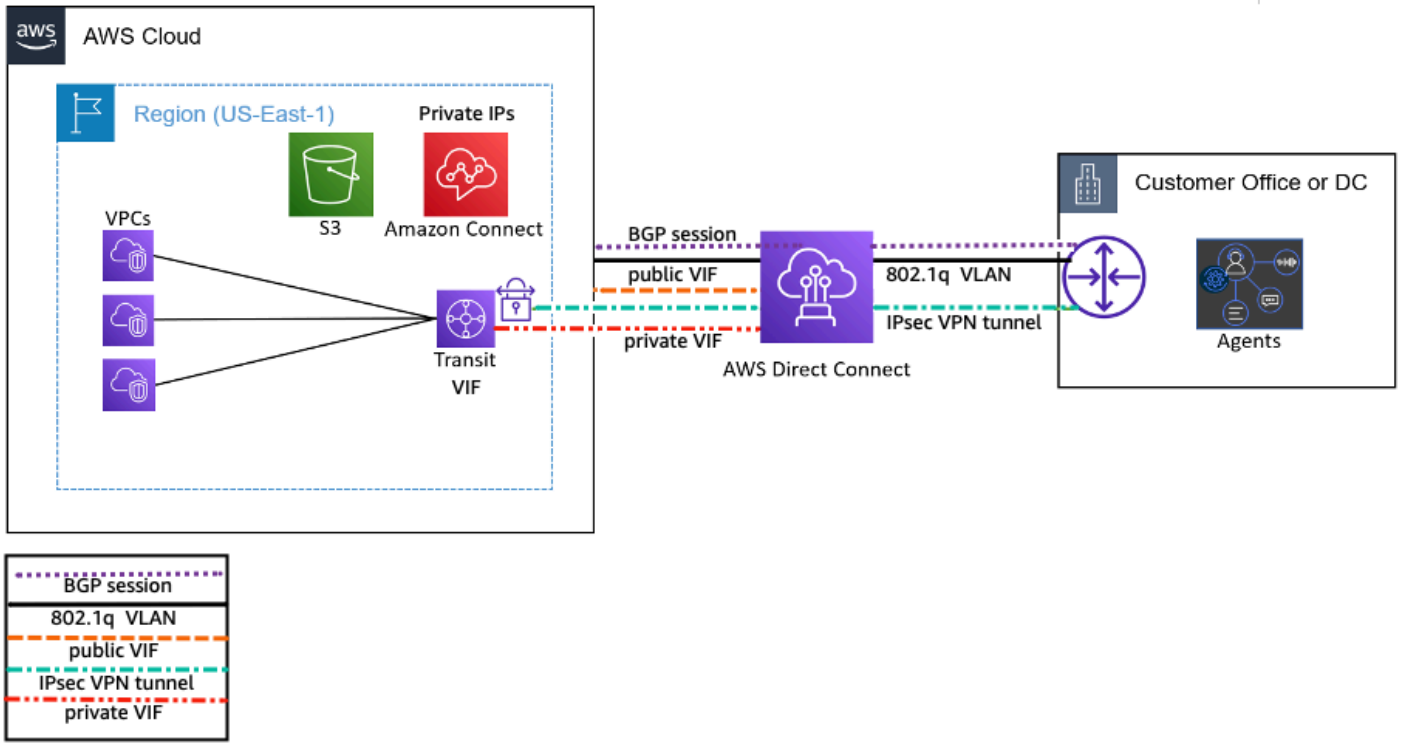
   - Equinix with Equinix Cloud Exchange
   - Switch with Switch Cloud Platform

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 Connect) or to Amazon VPC, bypassing internet service providers in your network path. An AWS Direct Connect point-of-presence (AWS DX POP), carrier interconnection, and data center interconnection provides access to AWS in the 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 Regions.

Create a virtual interface to enable access to AWS services. A public virtual interface (public VIF) enables access to public services such as Amazon S3 or Amazon Connect. 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.



Reference diagram of VIF propagation over BGP

Network requirements

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

- Your network is collocated with an existing AWS DX POP.
- You are working with an AWS Direct Connect partner who is a member of the AWS Partner Network (APN).
- 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 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 Regions or AWS GovCloud (US) can access public services in any other Region excluding China (Beijing and Ningxia). In addition, AWS Direct Connect connections in Regions or AWS GovCloud (US) can be configured to access a VPC in your account in any other Region excluding China (Beijing and Ningxia). You can, therefore, use a single AWS Direct Connect connection to build multi-Region services.

There are SLA implications of this design. All networking traffic remains on the AWS global network backbone, regardless of whether you access public AWS services or a VPC in another 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 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.

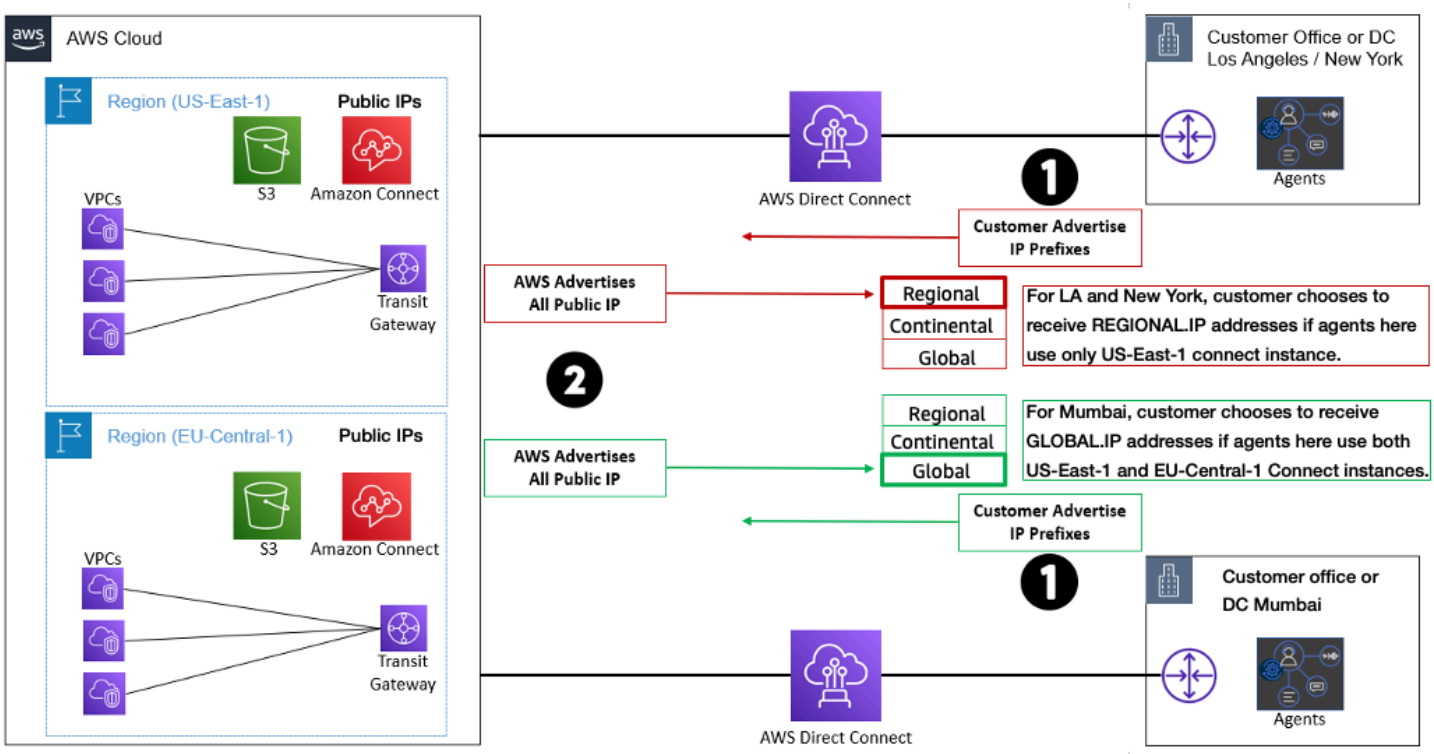
The communities 7224:1—7224:65535 are reserved by AWS Direct Connect.

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.



Reference diagram of advertising BGP Community Tags using Direct Connect

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.

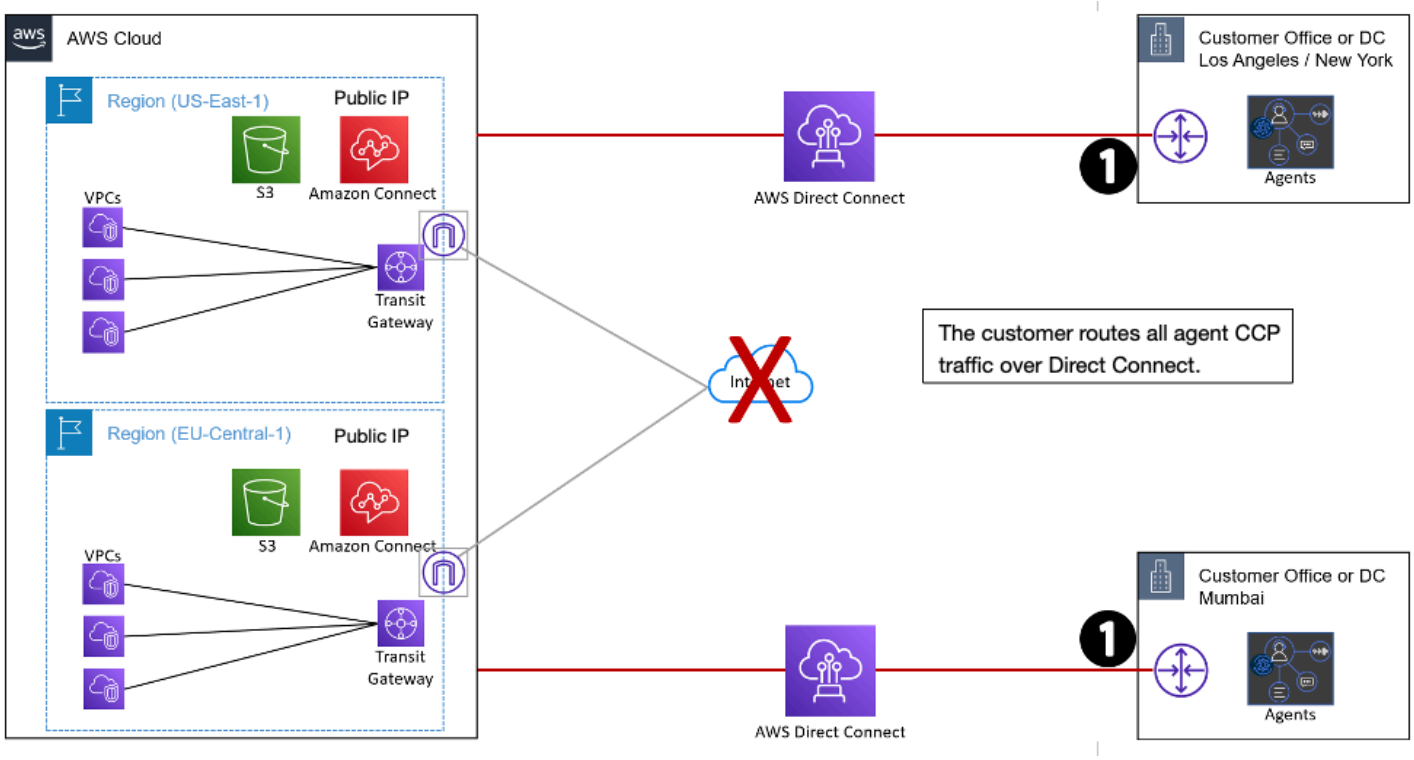
The following inbound routing policies apply:

- You must own the public prefixes, and they must be registered as such in the appropriate 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



Reference diagram of public VIF routing of Amazon Connect traffic using Direct Connect

As indicated by the number on the diagram:

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

Set up your network

Traditional Voice over IP (VoIP) solutions require you to allow both inbound and outbound traffic for specific User Datagram Protocol (UDP) port ranges and IPs, such as 80 and 443. These solutions also apply to Transmission Control Protocol (TCP). In comparison, the network requirements for using the Contact Control Panel (CCP) with a softphone are less intrusive. You can establish persistent outbound send/receive connections through your web browser. As a result, you don't need to open a client-side port to listen for inbound traffic.

The following diagram shows you what each port is used for:

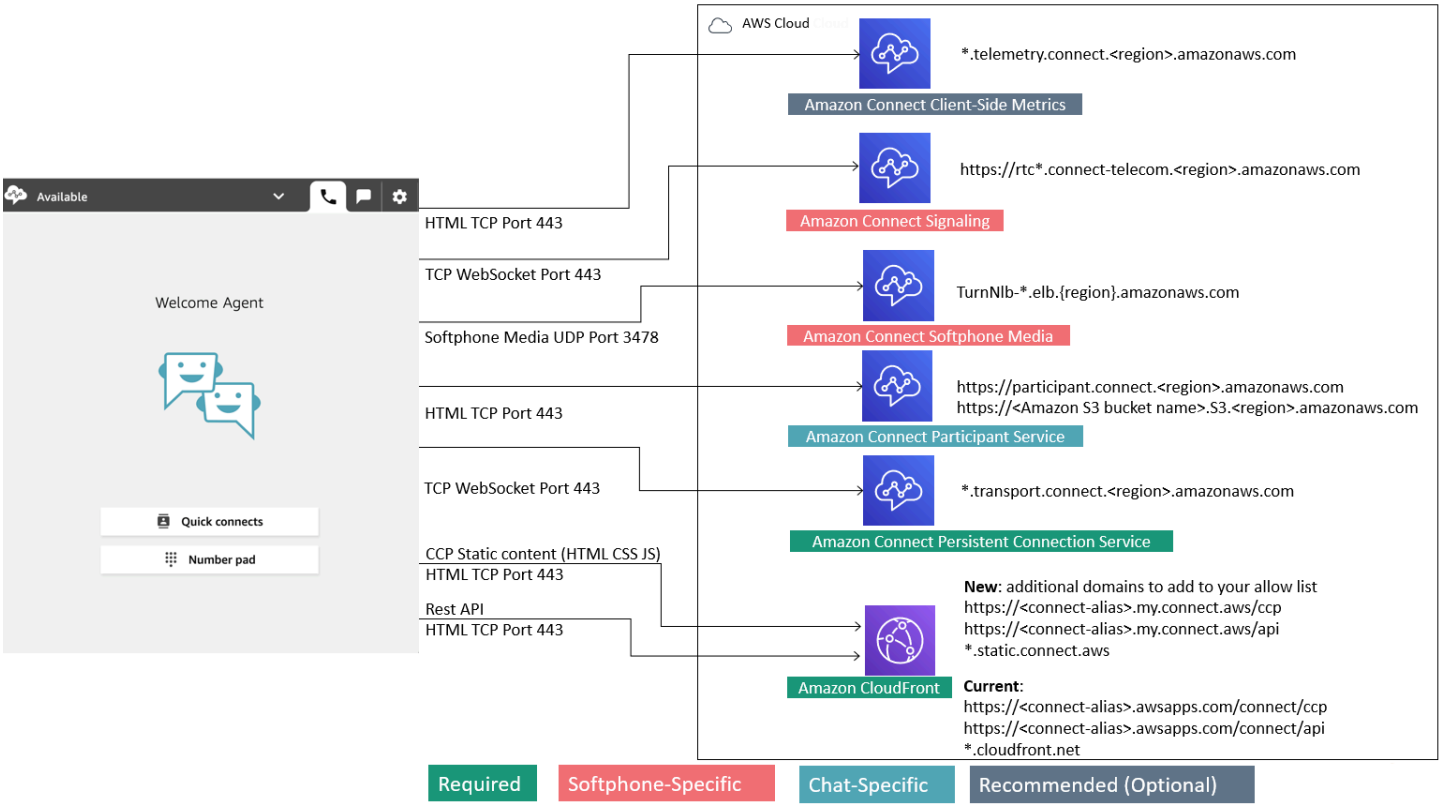


Diagram of Amazon Connect port and fully qualified domain name (FQDN) usage

Allow IP address ranges

In the AWS ip-ranges.json file, the whole /19 IP address range is owned by Amazon Connect. All traffic to and from the /19 range comes to and from Amazon Connect. The /19 IP address range isn't shared with other services. It's for the exclusive use of Amazon Connect globally. In the AWS `ip-ranges.json` file, you can see the same range listed twice. For example:

```
{ "ip_prefix": "15.193.0.0/19",
"region": "GLOBAL",
"service": "AMAZON"
},
{
"ip_prefix": "15.193.0.0/19",
"region": "GLOBAL",
"service": "AMAZON_CONNECT"
},
```

AWS always publishes any IP range twice: once for the specific service, and once for “AMAZON” service. There could even be a third listing for a more specific use case within a service.

When there are new IP address ranges supported for Amazon Connect, they are added to the publicly available `ip-ranges.json` file. They are kept for a minimum of 30 days before they are used by the service. After 30 days, softphone traffic through the new IP address ranges increases over the subsequent two weeks. After two weeks, traffic is routed through the new ranges equivalent to all available ranges.

Stateless firewalls

If you're using a stateless firewall for both options, use the requirements described in the previous sections. Then you must add to your allow list the ephemeral port range used by your browser, as shown in the following table.

Table 1 — Ephemeral IP port range

IP-Range entry	Port	Direction	Traffic
AMAZON_CONNECT	49152-65535 (UDP)	INBOUND	SEND/RECEIVE

Port and protocol considerations

Consider the following when implementing your network configuration changes for Amazon Connect:

- Allow traffic for all addresses and ranges for the Region in which you created your Amazon Connect instance.

- If you are using a proxy or firewall between the Contact Control Panel (CCP) and Amazon Connect, increase the Secure Sockets Layer (SSL) certificate cache timeout to cover the duration of an entire shift for your agents; do this to avoid connectivity issues with certificate renewals during their scheduled working time. For example, if your agents are scheduled to work eight-hour shifts that include breaks, increase the interval to eight hours plus time for breaks and lunch.
- When opening ports, Amazon Connect requires only the ports for endpoints in the same Region as your instance. CloudFront, however, serves static content from an edge location that has the lowest latency in relation to where your agents are located. IP range allow lists for CloudFront are global, and require all IP ranges associated with "service" and "CLOUDFRONT" in `ip-ranges.json`.
- Once the `ip-ranges.json` is updated, the associated AWS service will begin using the updated IP ranges after 30 days. To avoid intermittent connectivity issues when the service begins routing traffic to the new IP ranges, be sure to add the new IP ranges to your allow list, within 30 days from the time they were added to `ip-ranges.json`.
- If you are using a custom CCP with the Amazon Connect Streams API, you can create a media-less CCP that does not require opening ports for communication with Amazon Connect, but still requires ports opened for communication with CloudFront.

Amazon Connect Region selection considerations

Amazon Connect Region selection is contingent upon data governance requirements, use case, services available in each Region, and latency in relation to your agents, contacts, and external transfer endpoint geography.

- **Agent location and network** — CCP connectivity traverses the wide area network (WAN), so it is important that the workstation has the lowest latency and fewest hops possible, specifically to the AWS Region where your resources and Amazon Connect instance are hosted. For example, hub-and-spoke networks that need to make several hops to reach an edge router can add latency and reduce the quality of experience.

  When you set up your instance and agents, make sure to create your instance in the Region that is geographically closest to the agents. If you need to set up an instance in a specific Region to comply with company policies or other regulations, choose the configuration that results in the fewest network hops between your agents' computers and your Amazon Connect instance.
- **Location of your callers** — Because calls are anchored to your Amazon Connect Region endpoint, they are subject to public switched telephone network (PSTN) latency. Ideally your callers and transfer endpoints are geographically located as closely as possible to the AWS Region where your Amazon Connect instance is hosted for lowest latency.

  For optimal performance, and to limit the latency for your customers when they call in to your contact center, create your Amazon Connect instance in the Region that is geographically closest to where your customers call from. You might consider creating multiple Amazon Connect instances and provide contact information to customers for the number that is closest to where they call from.

  External transfers from Amazon Connect remain anchored to your Amazon Connect Region endpoint for the duration of the call. Per-minute usage continues to accrue until the call is disconnected by the recipient of the transferred call. The call is not recorded after the agent drops or the transfer completes. The contact record data and associated call recording of a transferred call are generated after the call is ended. Whenever possible, don't transfer calls that could be transferred back into Amazon Connect, known as circular transfers, to avoid compounding PSTN latency.

Conclusion

Combining AWS Direct Connect with Amazon Connect can solve for several business concerns that affect some customers. There are a multitude of considerations on architecture design and configuration requirements 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:

- Greg Smith, Senior Solutions Architect, Amazon Web Services
- Greg Thomas, Scaling Solutions Architect, Amazon Web Services

Further reading

For additional information, refer to:

- AWS Architecture Center

- AWS Whitepapers page
- What is AWS Direct Connect? (AWS documentation)
- Amazon Connect networking: Set up your network (AWS documentation)
- Routing policies and BGP communities (AWS documentation)

Document revisions

To be notified about updates to this whitepaper, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Whitepaper published.	November 2, 2022

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.

AWS Glossary

For the latest AWS terminology, see the AWS glossary in the *AWS Glossary Reference*.