AWS Whitepaper

Amazon Virtual Private Cloud Connectivity Options

Amazon Virtual Private Cloud Connectivity Options: AWS Whitepaper

Table of Contents

Amazon Virtual Private Cloud Connectivity Options

Publication date: **April 5, 2023** (*Document revisions*)

Abstract

Amazon Virtual Private Cloud (Amazon VPC) lets customers provision a private, isolated section of the Amazon Web Services (AWS) Cloud where they can launch AWS resources in a virtual network using customer-defined IP address ranges. Amazon VPC provides customers with several options for connecting their AWS virtual networks with other remote networks. This document describes several common network connectivity options available to our customers. These include connectivity options for integrating remote customer networks with Amazon VPC and connecting multiple Amazon VPCs into a contiguous virtual network.

This whitepaper is intended for corporate network architects and engineers or Amazon VPC administrators who would like to review the available connectivity options. It provides an overview of the various options to facilitate network connectivity discussions as well as pointers to additional documentation and resources with more detailed information or examples.

Introduction

Amazon VPC provides multiple network connectivity options for you to use, depending on your current network designs and requirements. These connectivity options include using either the internet or an AWS Direct Connect connection as the network backbone and terminating the connection into AWS or user-managed network endpoints. Additionally, with AWS, you can choose how network routing is delivered between Amazon VPC and your networks, leveraging either AWS services or user-managed network equipment and routes. This whitepaper considers the following options with an overview and a high-level comparison of each:

- Network-to-Amazon VPC connectivity options
  - AWS Site-to-Site VPN – Describes establishing a managed IPsec VPN connection from your network equipment on a remote network to Amazon VPC.
  - AWS Transit Gateway + AWS Site-to-Site VPN – Describes establishing a managed IPsec VPN connection from your network equipment on a remote network to a regional network hub for Amazon VPCs, using AWS Transit Gateway.
  - AWS Direct Connect - Describes establishing a private, logical connection from your remote network to Amazon VPC, using AWS Direct Connect.
  - AWS Direct Connect + AWS Transit Gateway – Describes establishing a private, logical connection from your remote network to a regional network hub for Amazon VPCs, using AWS Direct Connect and AWS Transit Gateway.
  - AWS Direct Connect + AWS Site-to-Site VPN – Describes establishing a private, encrypted connection from your remote network to Amazon VPC, using AWS Direct Connect and AWS Site-to-Site VPN.
  - AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN – Describes establishing a private, encrypted connection from your remote network to a regional network hub for Amazon VPCs, using AWS Direct Connect and AWS Transit Gateway.
  - AWS VPN CloudHub – Describes establishing a hub-and-spoke model for connecting remote branch offices.
  - Software VPN – Describes establishing a VPN connection from your equipment on a remote network to a user-managed software VPN appliance running inside an Amazon VPC.
  - AWS Transit Gateway + SD-WAN solutions - Describes the integration of software-defined wide area network (SD-WAN) solutions to interconnect several remote locations to a regional network hub for Amazon VPCs, using the AWS backbone or the internet as a transit network.

- Amazon VPC-to-Amazon VPC connectivity options
  - VPC peering – Describes connecting Amazon VPCs within and across regions using the Amazon VPC peering feature.
  - AWS Transit Gateway – Describes connecting Amazon VPCs within and across regions using AWS Transit Gateway in a hub-and-spoke model.
  - AWS PrivateLink – Describes connecting Amazon VPCs with VPC interface endpoints and VPC endpoint services.
  - Software VPN – Describes connecting Amazon VPCs using VPN connections established between user-managed software VPN appliances running inside of each Amazon VPC.
  - Software VPN-to-AWS Site-to-Site VPN – Describes connecting Amazon VPCs with a VPN connection established between a user-managed software VPN appliance in one Amazon VPC and AWS Site-to-Site VPN attached to the other Amazon VPC.
- Software remote access-to-Amazon VPC connectivity options
  - AWS Client VPN – Describes connecting software remote access to Amazon VPC, leveraging AWS Client VPN.
  - Software client VPN – Describes connecting software remote access to Amazon VPC, leveraging user-managed software VPN appliances.
- Transit VPC - Describes establishing a global transit network on AWS using a software VPN in conjunction with an AWS-managed VPN.
- AWS Cloud WAN - Describes establishing a managed wide area network (WAN) to easily build, manage, and monitor global interconnections between resources in Amazon VPCs, datacenters, and remote branches.

Network-to-Amazon VPC connectivity options

This section provides design patterns for connecting remote networks with your Amazon VPC environment. These options are useful for integrating AWS resources with your existing on-site services (for example, monitoring, authentication, security, data or other systems) by extending your internal networks into the AWS Cloud. This network extension also allows your internal users to seamlessly connect to resources hosted on AWS just like any other internally facing resource.

VPC connectivity to remote customer networks is best achieved when using non-overlapping IP ranges for each network being connected. For example, if you'd like to connect one or more VPCs to your corporate network, make sure they are configured with unique Classless Inter-Domain Routing (CIDR) ranges. We recommend allocating a single, contiguous, non-overlapping CIDR block to be used by each VPC. For additional information about Amazon VPC routing and constraints, see the Amazon VPC Frequently Asked Questions.

Option	Use Case	Advantages	Limitations
AWS Site-to-Site VPN	AWS managed IPsec VPN connection over the internet to individual VPC	Reuse existing VPN equipment and processes Reuse existing internet connections AWS managed high availability VPN service Supports static routes or dynamic Border Gateway Protocol (BGP) peering and routing policies	Network latency, variability, and availability are dependent on internet conditions You are responsib le for implement ing redundancy and failover (if required) Remote device must support single-hop BGP (when leveragin g BGP for dynamic routing)
AWS Transit Gateway + AWS Site-to-Site VPN	AWS managed IPsec VPN connection over the internet to	Same as the previous option	Same as the previous option

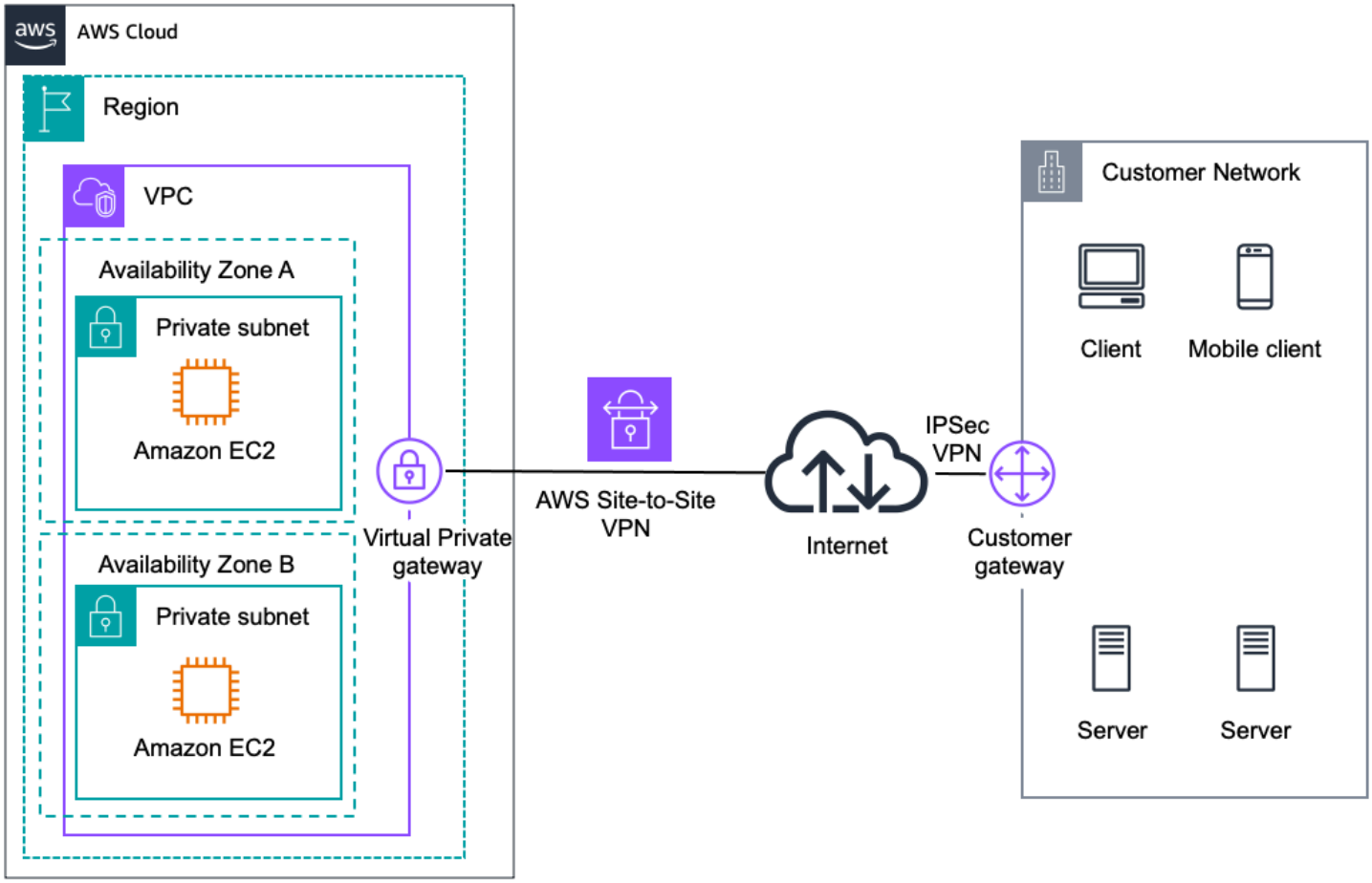
Option	Use Case	Advantages	Limitations
	regional router for multiple VPCs	AWS managed high availability and scalability regional network hub for up to 5,000 attachments	
AWS Direct Connect	Dedicated network connection over private lines	More predictable network performance Reduced bandwidth costs Supports BGP peering and routing policies	Might require additional telecom and hosting provider relationships or new network circuits to be provisioned
AWS Direct Connect + AWS Transit Gateway	Dedicated network connection over private lines to regional router for multiple VPCs	Same as the previous option AWS managed high availability and scalability regional network hub for up to 5,000 attachments	Same as previous option

Option	Use Case	Advantages	Limitations
AWS Direct Connect + AWS Site-to-Site VPN	IPsec VPN connection over private lines	More predictable network performance Reduced bandwidth costs Supports BGP peering and routing policies on AWS Direct Connect Reuse existing VPN equipment and processes AWS managed high availability VPN service Supports static routes or dynamic Border Gateway Protocol (BGP) peering and routing policies on VPN connection	May require additional telecom and hosting provider relationships or new network circuits to be provisioned You are responsible for implementing redundancy and failover (if required) Remote device must support single-hop BGP (when leveraging BGP for dynamic routing)
AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN	IPsec VPN connection over private lines to regional router for multiple VPCs	Same as previous option AWS managed high availability and scalability regional network hub for up to 5,000 attachments	Same as previous option

Option	Use Case	Advantages	Limitations
AWS VPN CloudHub	Connect remote branch offices in a hub-and-spoke model for primary or backup connectivity	Reuse existing internet connections and AWS VPN connections AWS managed high availability VPN service Supports BGP for exchanging routes and routing priorities	Network latency, variability, and availability are dependent on the internet User managed branch office endpoints are responsible for implementing redundancy and failover (if required)
AWS Transit Gateway + SD-WAN solutions	Connect remote branches and offices with a software-defined wide area network by using the AWS backbone or the internet as a transit network.	Supports a wider array of SD-WAN vendors, products, and protocols Some vendor solutions have integration with AWS native services.	You are responsible for implementing HA (high availability) of the SD-WAN appliances if they are placed in an Amazon VPC.
Software VPN	Software appliance-based VPN connection over the internet	Supports a wider array of VPN vendors, products, and protocols Fully customer-managed solution	You are responsible for implementing HA (high availability) solutions for all VPN endpoints (if required)

AWS Site-to-Site VPN

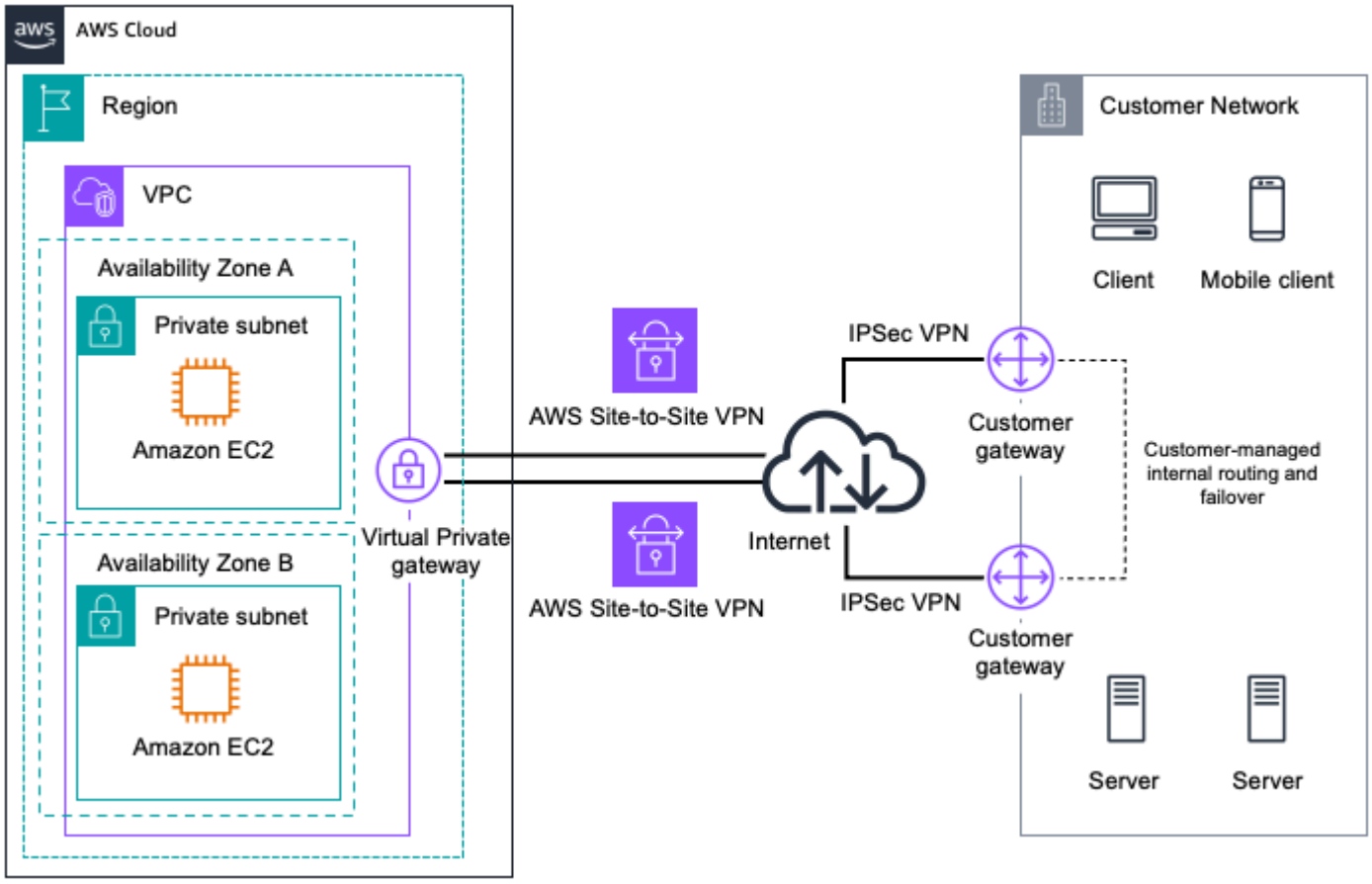
Amazon VPC provides the option of creating an IPsec VPN connection between your remote networks and Amazon VPC over the internet, as shown in the following figure.



AWS Managed VPN

Consider taking this approach when you want to take advantage of an AWS-managed VPN endpoint that includes automated redundancy and failover built into the AWS side of the VPN connection.

The virtual private gateway also supports and encourages multiple user gateway connections so that you can implement redundancy and failover on your side of the VPN connection, as shown in the following figure.



Redundant AWS Site-to-Site VPN Connections

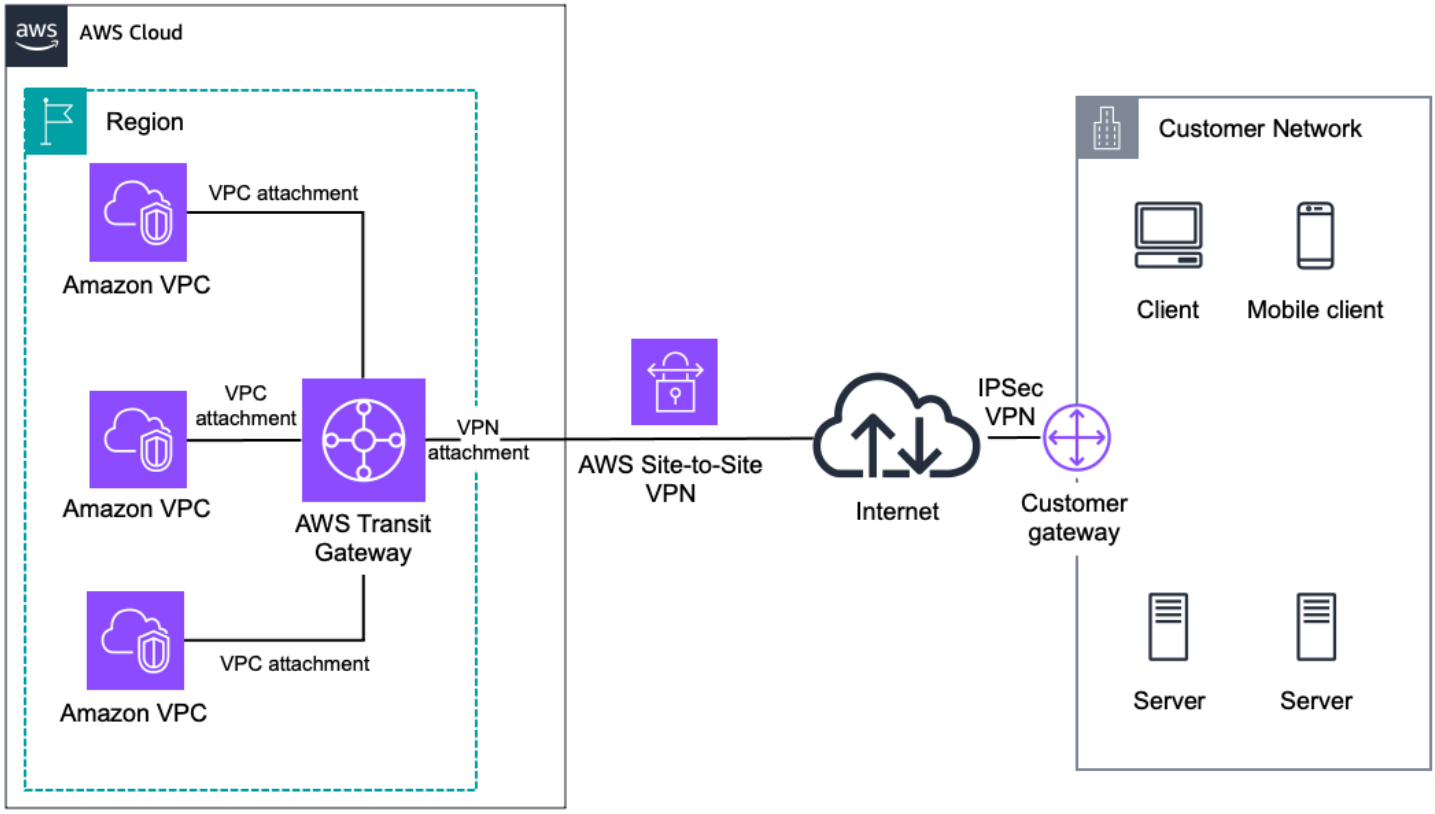
Both dynamic and static routing options are provided to give you flexibility in your routing configuration. Dynamic routing uses BGP peering to exchange routing information between AWS and these remote endpoints. With dynamic routing, you can also specify routing priorities, policies, and weights (metrics) in your BGP advertisements and influence the network path between your networks and AWS. It's important to note that when you use BGP, both the IPsec and the BGP sessions must be terminated on the same user gateway device, so it must be capable of terminating both IPsec and BGP sessions.

Additional resources

- AWS Site-to-Site VPN User Guide
- Requirements for customer gateway devices
- Customer gateway devices tested with Amazon VPC

AWS Transit Gateway + AWS Site-to-Site VPN

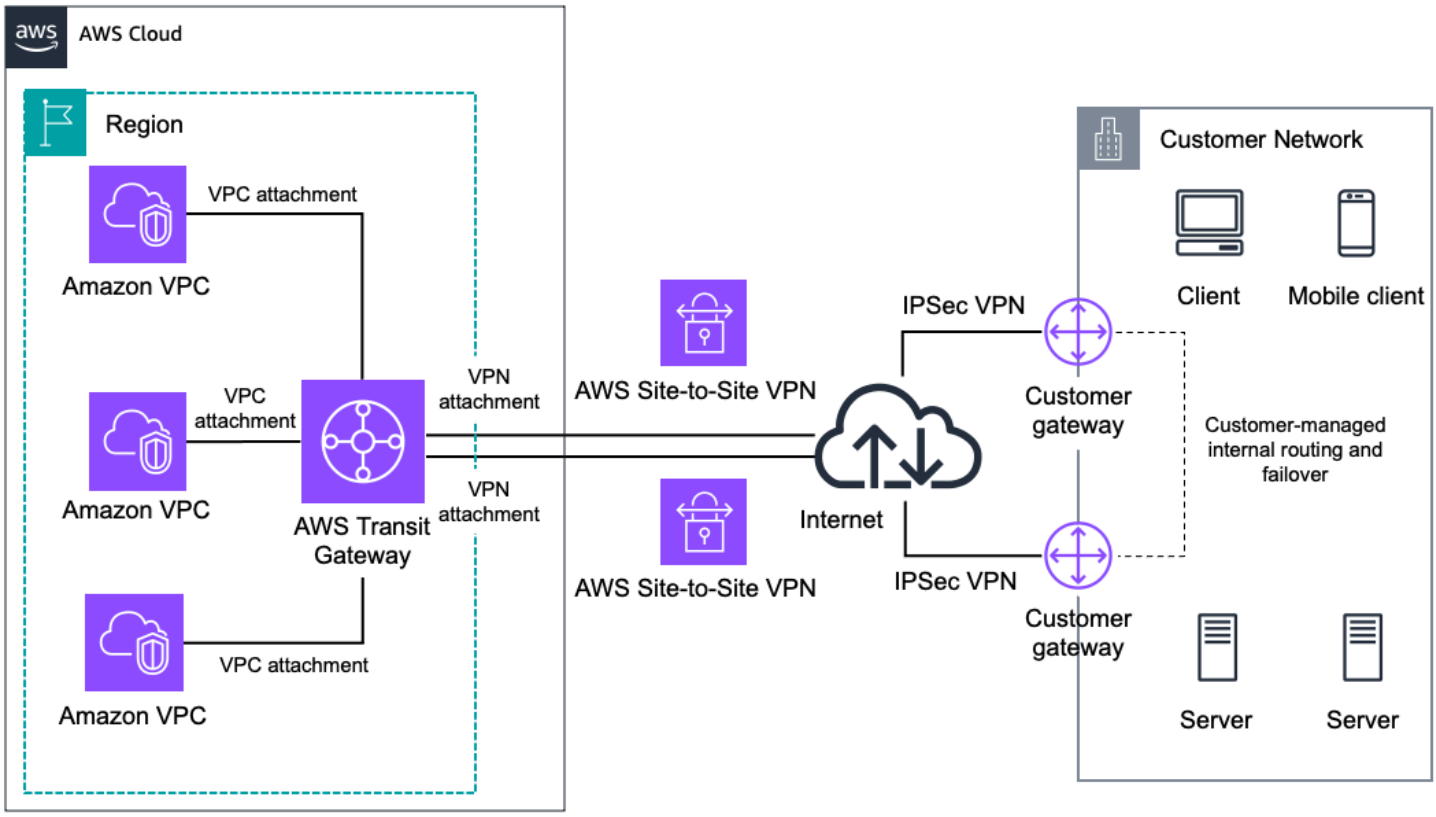
AWS Transit Gateway is an AWS managed high availability and scalability regional network transit hub used to interconnect VPCs and customer networks. AWS Transit Gateway + VPN, using the Transit Gateway VPN attachment, provides the option of creating an IPsec VPN connection between your remote network and the Transit Gateway over the internet, as shown in the following figure.



AWS Transit Gateway and AWS Site-to-Site VPN

Consider using this approach when you want to take advantage of an AWS-managed VPN endpoint for connecting to multiple VPCs in the same region without the additional cost and management of multiple IPsec VPN connections to multiple Amazon VPCs.

AWS Transit Gateway also supports and encourages multiple user gateway connections so that you can implement redundancy and failover on your side of the VPN connection as shown in the following figure.



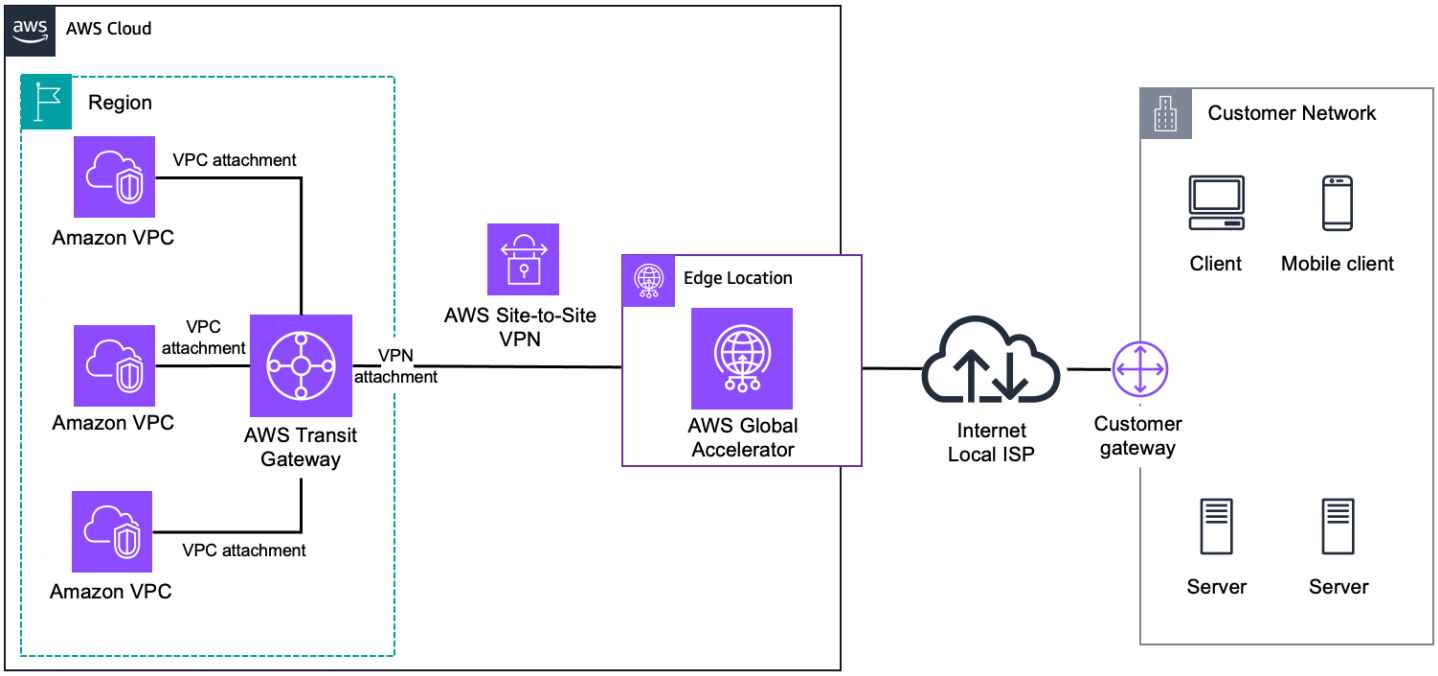
AWS Transit Gateway and Redundant VPN

Both dynamic and static routing options are provided to give you flexibility in your routing configuration on the Transit Gateway VPN IPsec attachment. Dynamic routing uses BGP peering to exchange routing information between AWS and these remote endpoints. With dynamic routing, you can also specify routing priorities, policies, and weights (metrics) in your BGP advertisements and influence the network path between your networks and AWS. It's important to note that when you use BGP, both the IPsec and the BGP sessions must be terminated on the same user gateway device, so it must be capable of terminating both IPsec and BGP sessions.

Per VPN connection, you can achieve 1.25 Gbps of throughput and 140,000 packets per second. When terminating the VPN connections in the Transit Gateway, you can use Equal Cost Multi-Path (ECMP) routing to get a higher VPN bandwidth by aggregating multiple VPN tunnels. To use ECMP, you need to configure dynamic routing in the VPN connections – ECMP is not supported using static routing.

In addition, you can enable acceleration in your AWS Site-to-Site VPN connections. An accelerated VPN connection uses AWS Global Accelerator to route traffic from your network to an AWS edge location that is closest to your customer gateway device. You can use this option to avoid network disruptions that might occur when the traffic is routed over the public internet. Acceleration is only

supported for VPN connections that are attached to a Transit Gateway, as shown in the following figure:



Accelerated AWS Site-to-Site VPN

Last, regarding IP addressing, Site-to-Site VPN connections on an AWS Transit Gateway support both IPv4 and IPv6 traffic. The following rules apply:

- IPv6 is only supported for the inside IP addresses of the VPN tunnel. The outside IP address for the AWS endpoints are public IPv4 addresses. The customer gateway IP address should be a public IPv4 address.
- A Site-to-Site VPN connection cannot support both IPv4 and IPv6 traffic. If your hybrid connectivity requires dual-stack communication, you should create different VPN tunnels for the IPv4 and IPv6 traffic.

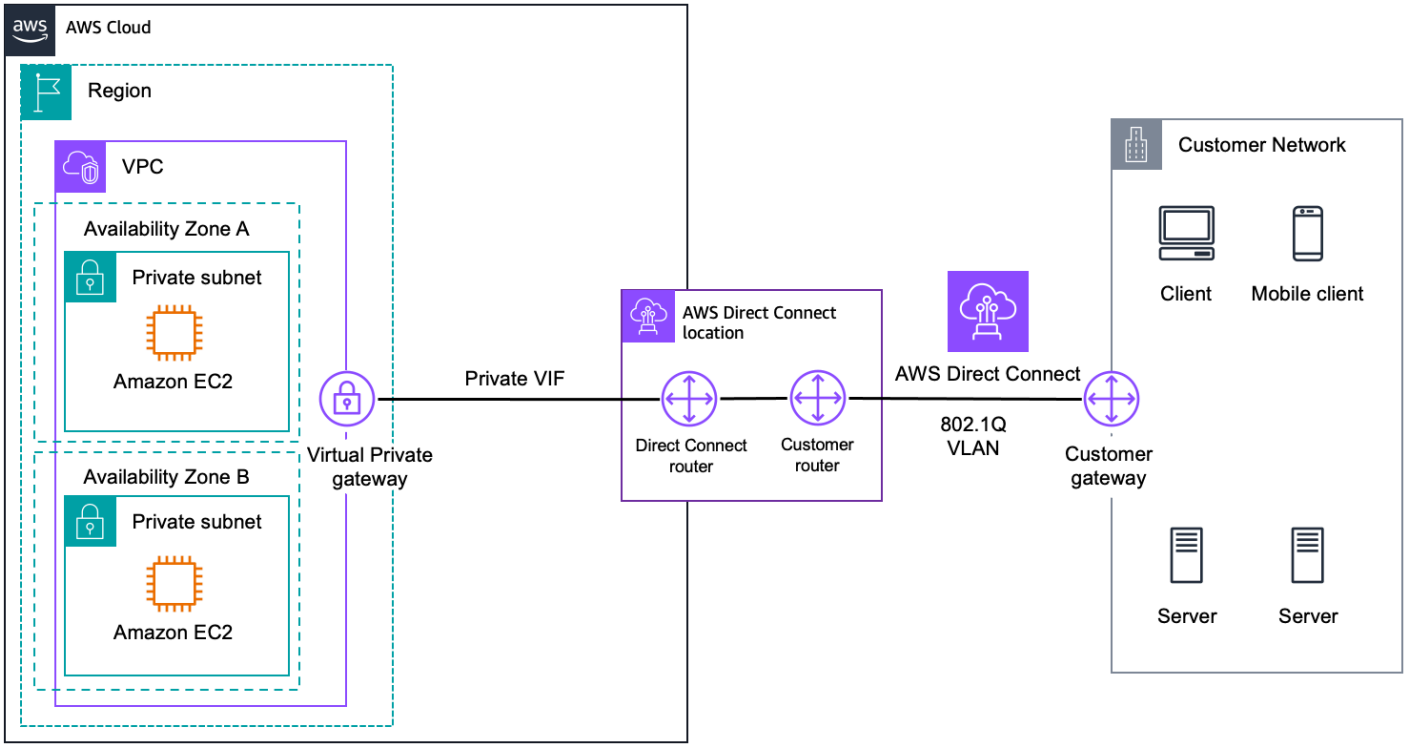
Additional resources

- Transit gateway VPN attachments
- Customer gateway
- Working with Site-to-Site VPN
- Accelerated Site-to-Site VPN connections

AWS Direct Connect

AWS Direct Connect makes it easy to establish a dedicated connection from an on-premises network to one or more VPCs. AWS Direct Connect can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than internet-based connections. It uses industry-standard 802.1Q VLANs to connect to Amazon VPC using private IP addresses. The VLANs are configured using virtual interfaces (VIFs), and you can configure three different types of VIFs:

- **Public virtual interface** - Establish connectivity between AWS public endpoints and your data center, office, or colocation environment.
- **Transit virtual interface** - Establish private connectivity between AWS Transit Gateway and your data center, office, or colocation environment. This connectivity option is covered in the section ???.
- **Private virtual interface** - Establish private connectivity between Amazon VPC resources and your data center, office, or colocation environment. The use of private VIFs is shown in the following figure.



AWS Direct Connect

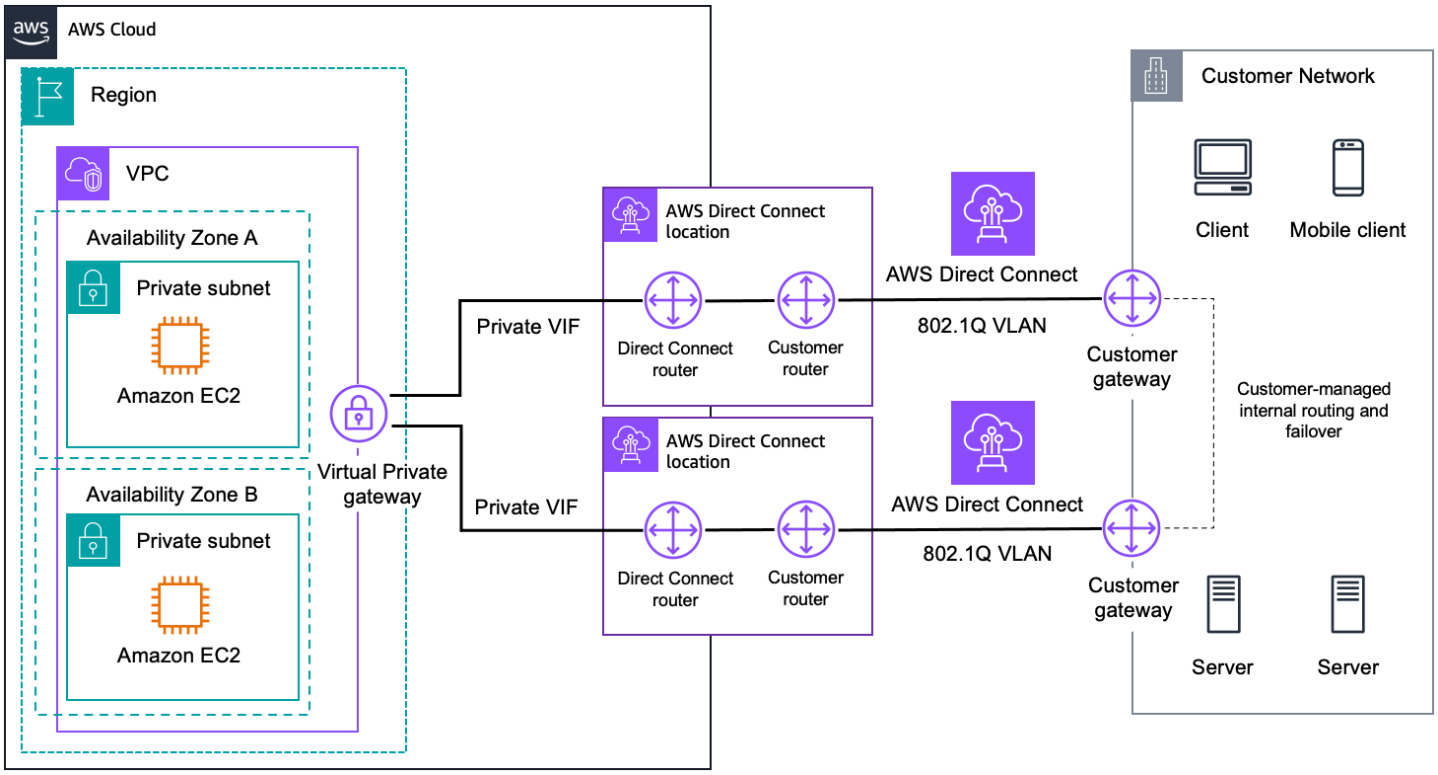
You can establish connectivity to the AWS backbone using AWS Direct Connect by establishing a cross-connect to AWS devices in a Direct Connect location. You can access any AWS Region from any of our Direct Connect locations (except China). If you don't have equipment at a location, you can choose from an ecosystem of WAN service providers for integrating your AWS Direct Connect endpoint in an AWS Direct Connect location with your remote networks.

With AWS Direct Connect, you have two types of connection:

- **Dedicated connections**, where a physical ethernet connection is associated with a single customer. You can order port speeds of 1, 10, or 100 Gbps. You might need to work with a partner in the AWS Direct Connect Partner Program to help you establish network circuits between an AWS Direct Connect connection and your data center, office, or colocation environment.
- **Hosted connections**, where a physical ethernet connection is provisioned by an AWS Direct Connect Partner and shared with you. You can order port speeds between 50 Mbps and 10 Gbps. Your work with the Partner in both the AWS Direct Connect connection they established and the network circuits between an AWS Direct Connect connection and your data center, office, or colocation environment.

For dedicated connections, you can also use a link aggregation group (LAG) to aggregate multiple connections at a single AWS Direct Connect endpoint. You treat them as a single, managed connection. You can aggregate up to four 1- or 10-Gbps connections, and up to two 100-Gbps connections.

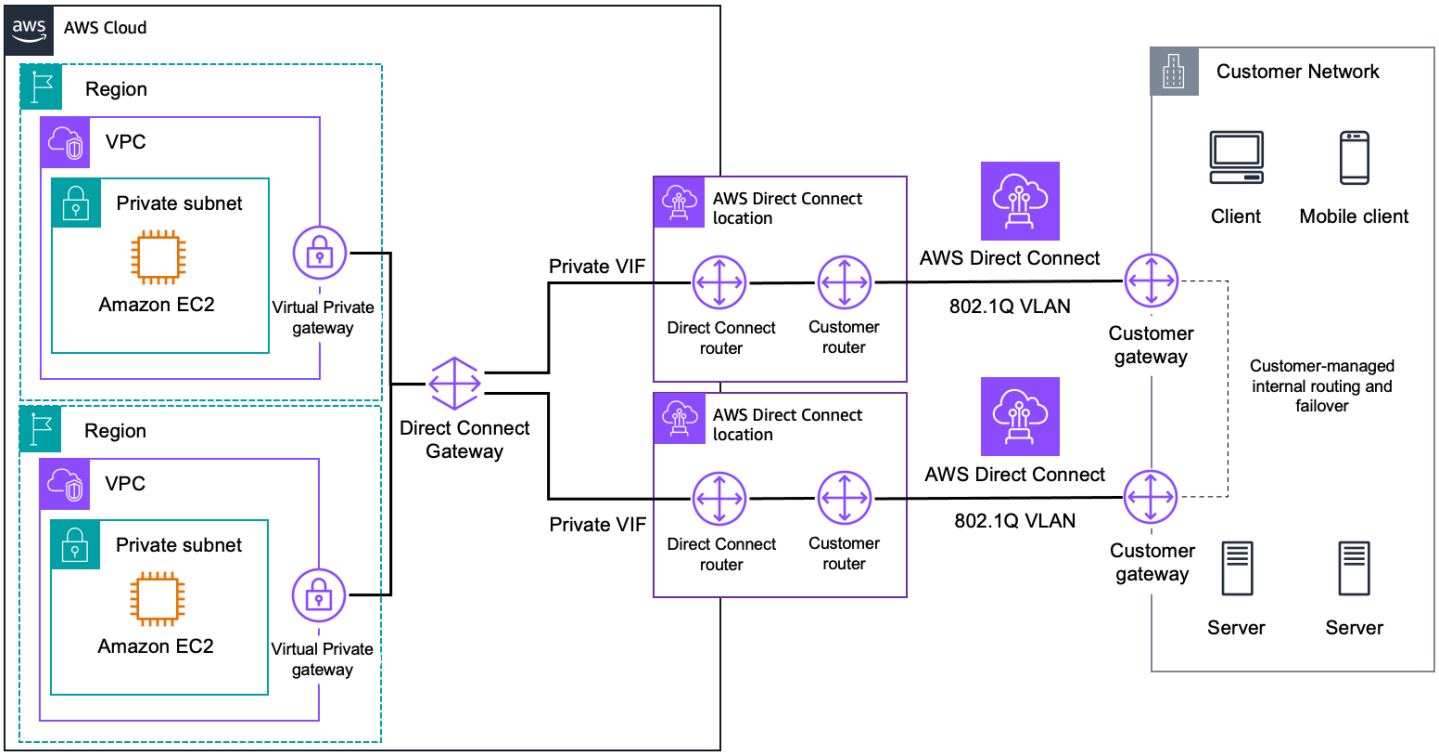
When discussing high availability in AWS Direct Connect, we recommend using additional AWS Direct Connect connections. The AWS Direct Connect Resiliency Toolkit offers guidance in building highly resilient network connections between AWS and your data center, office, or colocation environment. The following figure shows you an example of a high-resiliency connectivity option, with two AWS Direct Connect connections terminated in two different AWS Direct Connect locations.



Redundant AWS Direct Connect

AWS Direct Connect is not encrypted by default. For dedicated connections of 10 or 100 Gbps, you can use MAC security (MACsec) as an encryption option. For connections of 1 Gbps or less, you can create VPN tunnels on top of the connection – this option is covered in AWS Direct Connect + AWS Site-to-Site VPN and AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN sections.

One important resource in AWS Direct Connect is the Direct Connect gateway, which is a globally available resource to enable connections to multiple Amazon VPCs or Transit Gateways across different Regions or AWS accounts. This resource also allows you to connect to any participating VPC or Transit Gateway from one private VIF or transit VIF, reducing AWS Direct Connect management, as shown in the following figure.



AWS Direct Connect Gateway

Regarding IP addressing, AWS Direct Connect virtual interfaces support both IPv4 and IPv6 BGP sessions for dual-stack operation.

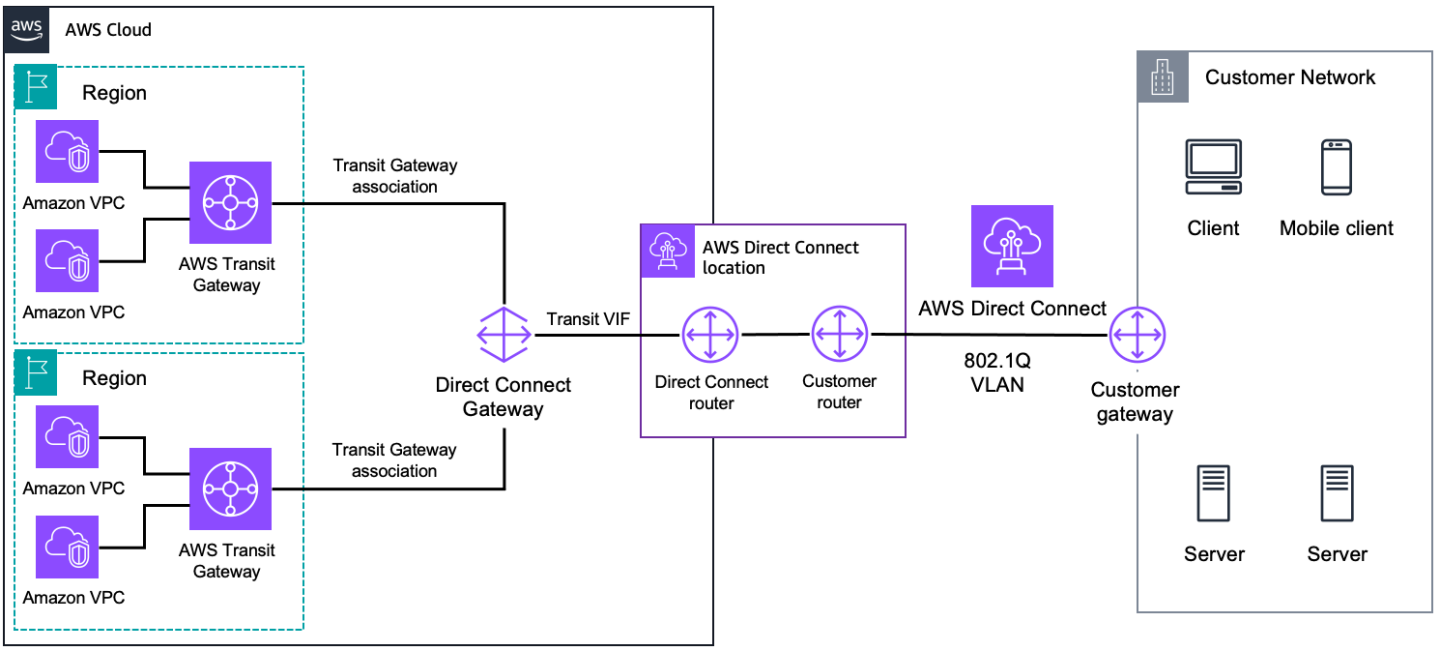
- Private and transit VIFs IPv4 configuration make use of either AWS-generated IPv4 addresses or addresses configured by you. For public VIFs IPv4 BGP peering, you must specify an unique public /31 IPv4 CIDR that you own (or submit a request to have a CIDR block assigned).
- For all types of VIFs IPv6 BGP peering, AWS assigns a /125 CIDR, which is not configurable.

Additional resources

- AWS Direct Connect User Guide
- AWS Direct Connect virtual interfaces
- AWS Direct Connect gateways
- AWS Direct Connect Resiliency Toolkit
- AWS Direct Connect MAC Security
- AWS Direct Connect locations
- AWS Direct Connect Delivery Partners

AWS Direct Connect + AWS Transit Gateway

AWS Direct Connect + AWS Transit Gateway, using transit VIF attachment to Direct Connect gateway, enables your network to connect several regional centralized routers over a private dedicated connection. The following diagram shows connecting to two routers.



AWS Direct Connect and AWS Transit Gateway

Each AWS Transit Gateway is a network transit hub to interconnect VPCs in the same region, consolidating Amazon VPC routing configuration in one place. This solution simplifies management of connections between an Amazon VPC and your networks over a private connection that can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than internet-based connections.

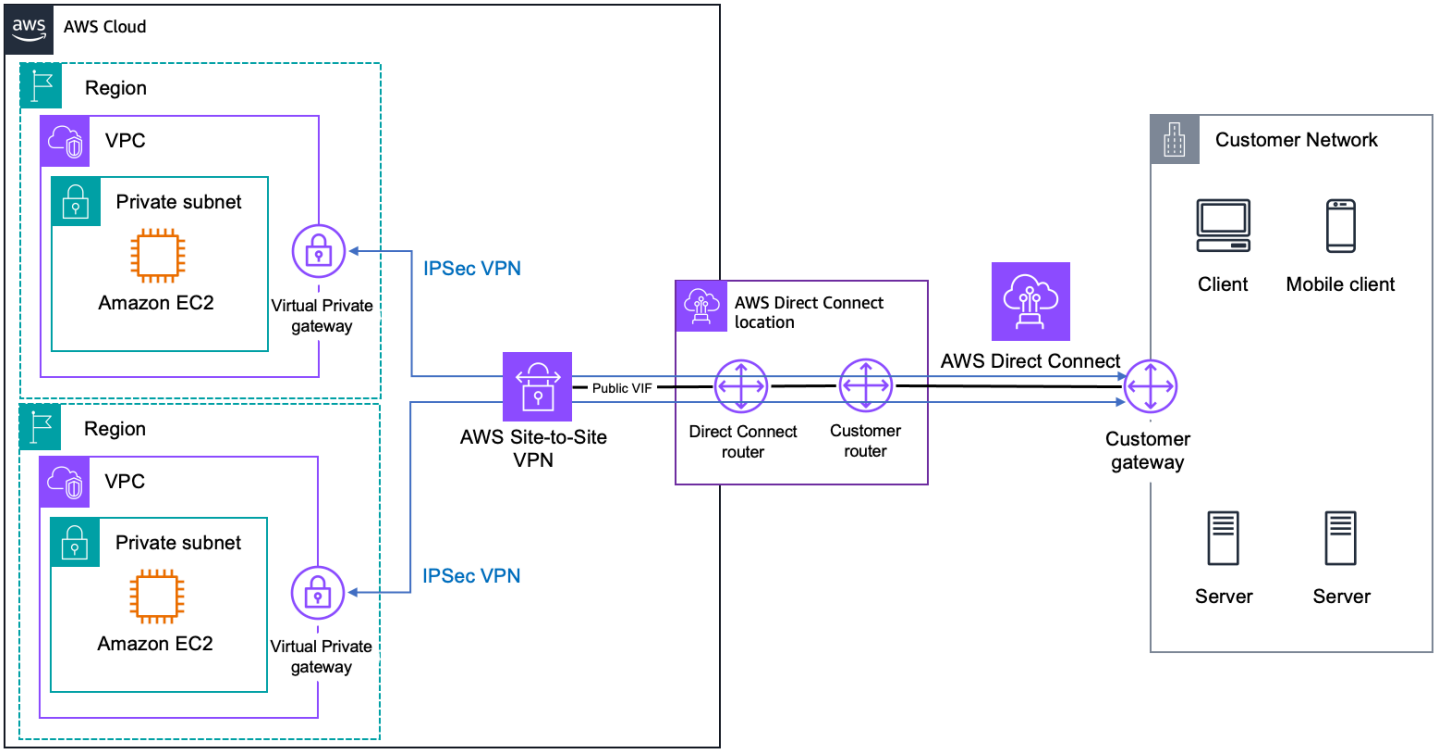
Additional resources

- AWS Direct Connect User Guide
- Link aggregation groups in AWS Direct Connect
- Blog post: Integrating sub-1 Gbps hosted connections with AWS Transit Gateway

AWS Direct Connect + AWS Site-to-Site VPN

With AWS Direct Connect + AWS Site-to-Site VPN, you can combine AWS Direct Connect connections with an AWS-managed VPN solution. AWS Direct Connect public VIFs establish a

dedicated network connection between your network and public AWS resources such as an AWS Site-to-Site VPN endpoint. Once you establish the connection to the service, you can create IPsec connections to the corresponding Amazon VPC virtual private gateways. The following figure illustrates this option.



AWS Direct Connect and AWS Site-to-Site VPN

This solution combines the benefits of the end-to-end secure IPsec connection with low latency and increased bandwidth of the AWS Direct Connect to provide a more consistent network experience than internet-based VPN connections. A BGP connection session is established between AWS Direct Connect and your router on the public VIF. Another BGP session or a static route will be established between the virtual private gateway and your router on the IPsec VPN tunnels.

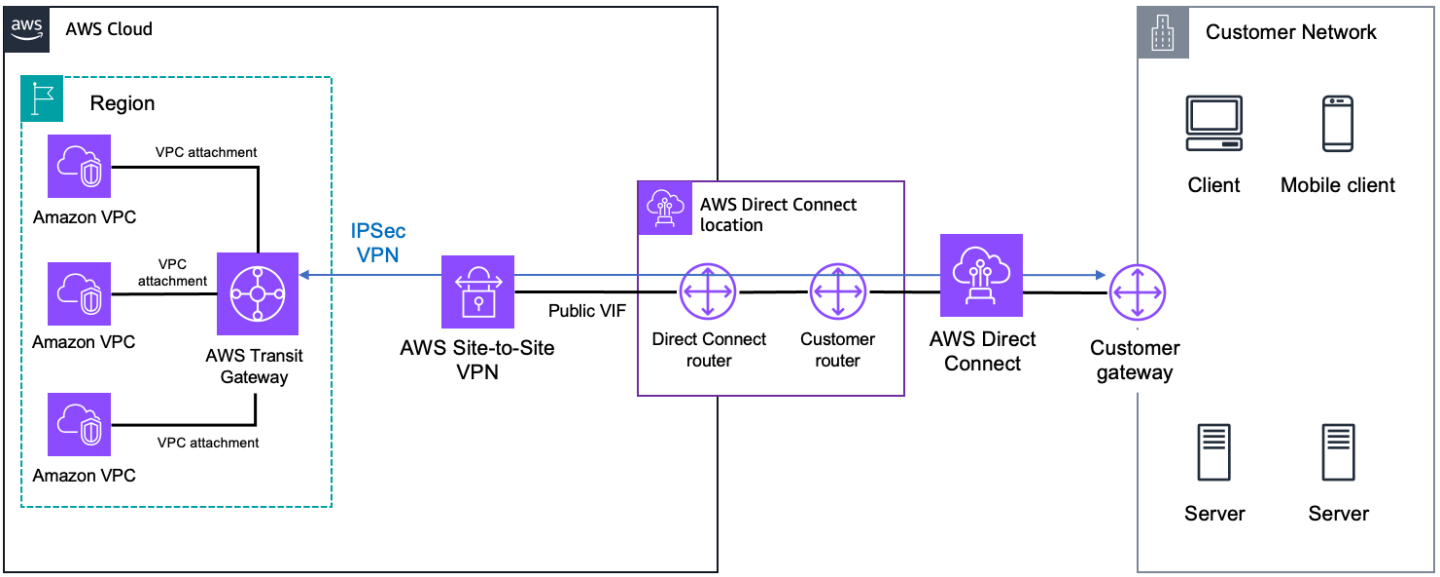
Additional resources

- AWS Direct Connect
- AWS Direct Connect virtual interfaces
- AWS Site-to-Site VPN User Guide

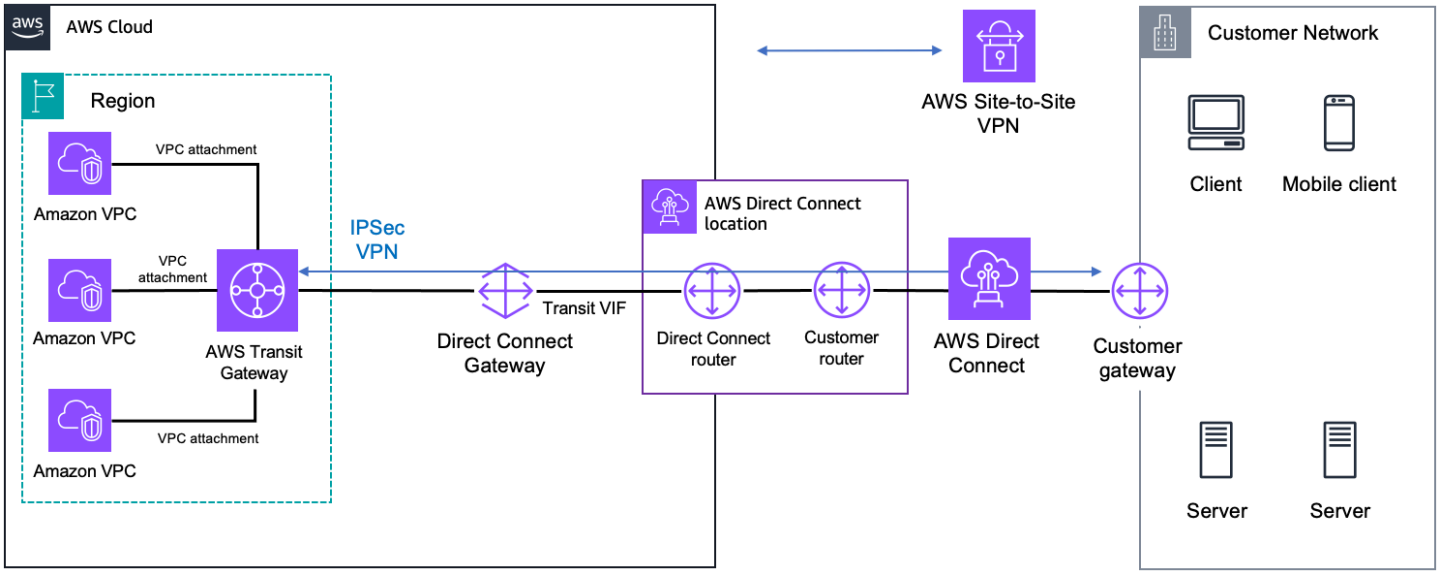
AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN

With AWS Direct Connect + AWS Transit Gateway + AWS Site-to-Site VPN, you can enable end-to-end IPsec-encrypted connections between your networks and a regional centralized router for Amazon VPCs over a private dedicated connection.

You can use AWS Direct Connect public VIFs to first establish a dedicated network connection between your network to public AWS resources, such as AWS Site-to-Site VPN endpoints. Once this connection is established, you can create an IPsec connection to AWS Transit Gateway. The following figure illustrates this option.



AWS Direct Connect, AWS Transit Gateway, and AWS Site-to-Site VPN (public VIF)



AWS Direct Connect, AWS Transit Gateway, and AWS Site-to-Site VPN (transit VIF)

Consider taking this approach when you want to simplify management and minimize the cost of IPsec VPN connections to multiple Amazon VPCs in the same region, with the low latency and consistent network experience benefits of a private dedicated connection over an internet-based VPN. A BGP session is established between AWS Direct Connect and your router using either the public or the transit VIF. Another BGP session or a static route will be established between AWS Transit Gateway and your router on the IPsec VPN tunnel.

Additional resources

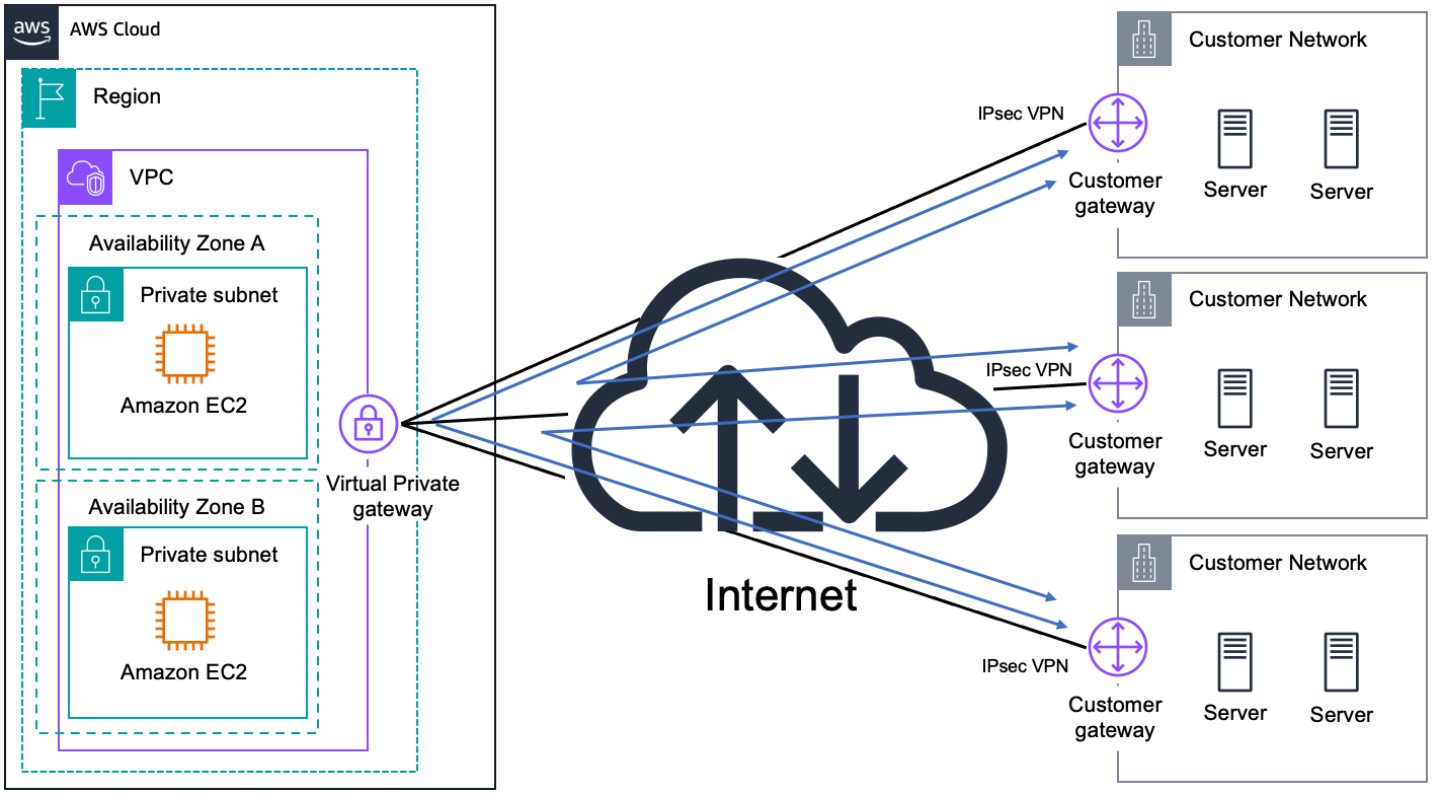
- AWS Direct Connect virtual interfaces
- Transit gateway VPN attachments
- Requirements for customer gateway devices
- Customer gateway devices tested with Amazon VPC
- AWS Site-to-Site VPN – Private IP VPN with AWS Direct Connect

AWS VPN CloudHub

Building on the AWS managed VPN options described previously, you can securely communicate from one site to another using the AWS VPN CloudHub. The AWS VPN CloudHub operates on a simple hub-and-spoke model that you can use with or without a VPC. Use this approach if you have multiple branch offices and existing internet connections and would like to implement a

convenient, potentially low-cost hub-and-spoke model for primary or backup connectivity between these remote offices.

The following figure shows the AWS VPN CloudHub architecture, with lines indicating network traffic between remote sites being routed over their AWS VPN connections.



AWS VPN CloudHub

AWS VPN CloudHub uses an Amazon VPC virtual private gateway with multiple customer gateways, each using unique BGP autonomous system numbers (ASNs). The remote sites must not have overlapping IP ranges. Your gateways advertise the appropriate routes (BGP prefixes) over their VPN connections. These routing advertisements are received and re-advertised to each BGP peer so that each site can send data to and receive data from the other sites.

Additional resources

- Providing secure communication between sites using VPN CloudHub
- AWS Site-to-Site VPN User Guide
- Requirements for customer gateway devices
- Customer gateway devices tested with Amazon VPC

AWS Transit Gateway + SD-WAN solutions

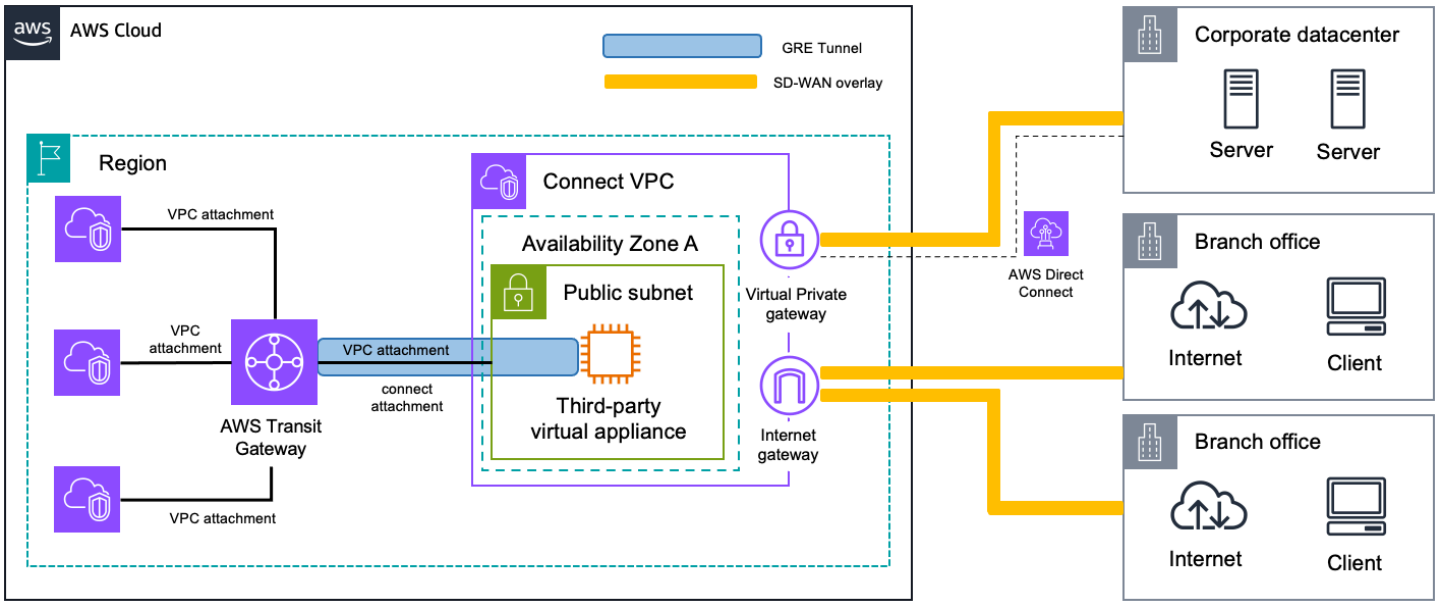
Software Defined Wide Area Networks (SD-WANs) are used to connect your data centers, offices, or colocation environments over different transit networks (such as the public internet, MPLS networks, or the AWS backbone using AWS Direct Connect), managing the traffic automatically and dynamically across the most appropriate and efficient path based on network conditions, application type or quality of service (QoS) requirements.

Use this approach if you have a complex network topology, with several data centers, offices, or colocation environments that need to communicate between themselves and with AWS. SD-WAN solutions can help you to efficiently manage this type of network.

When talking about the connection of an SD-WAN network to AWS, AWS Transit Gateway provides a managed highly-available and scalable regional network transit hub to interconnect VPCs and your SD-WAN network. Transit Gateway connect attachments provide a native way to connect your SD-WAN infrastructure and appliances with AWS. This makes it easy to extend your SD-WAN into AWS without having to set up IPsec VPNs.

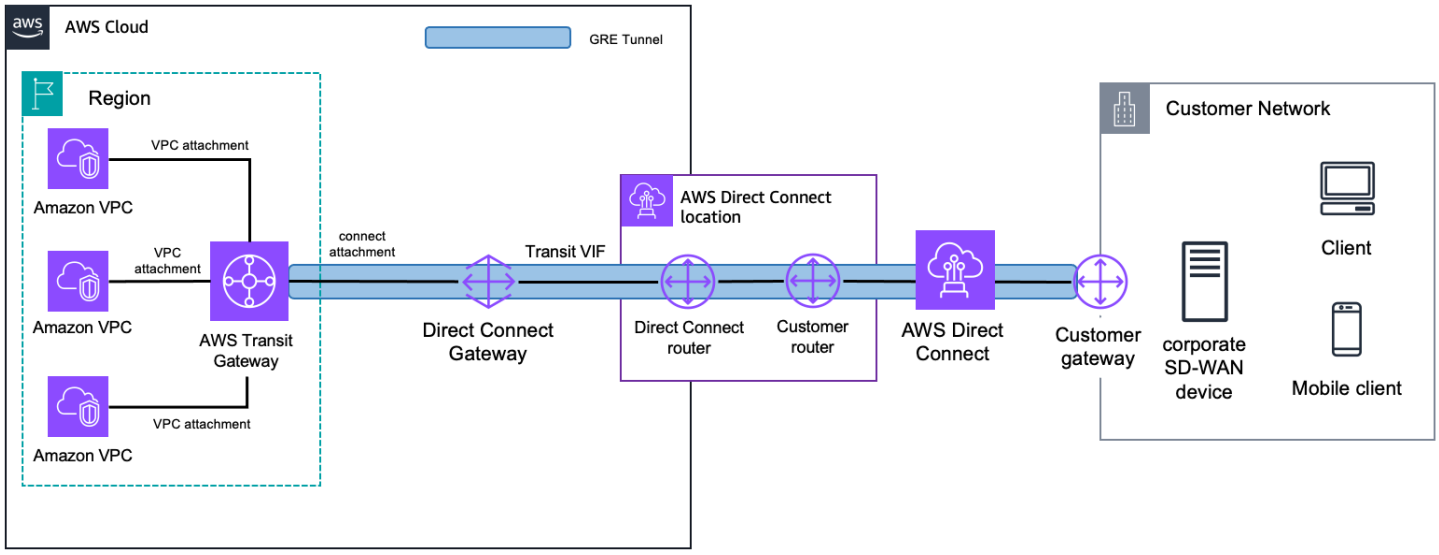
Transit Gateway connect attachments support Generic Routing Encapsulation (GRE) for higher bandwidth performance compared to a VPN connection. It supports Border Gateway Protocol (BGP) for dynamic routing, and removes the need to configure static routes. This simplifies network design and reduces the associated operational costs. In addition, its integration with Transit Gateway Network Manager provides advanced visibility through global network topology, attachment level performance metrics, and telemetry data.

When integrating your SD-WAN network to Transit Gateway using connect attachments, you have two common patterns. The first one is placing virtual appliances of the SD-WAN network in a VPC within AWS. Then, you use a VPC attachment as underlying transport for the Transit Gateway connect attachment between the virtual appliances and the Transit Gateway, as can be shown in the following figure.



SD-WAN connectivity with AWS Transit Gateway (virtual appliance in AWS)

Alternatively, you can extend and segment your SD-WAN traffic to AWS without adding extra infrastructure. You can create Transit Gateway connect attachments using an AWS Direct Connect connection as underlying transport, as can be shown in the following figure.



SD-WAN connectivity with AWS Transit Gateway (Direct Connect as transport)

There are some considerations to be aware when using Transit Gateway connect attachments:

- You can create a connect attachments on existing Transit Gateways.

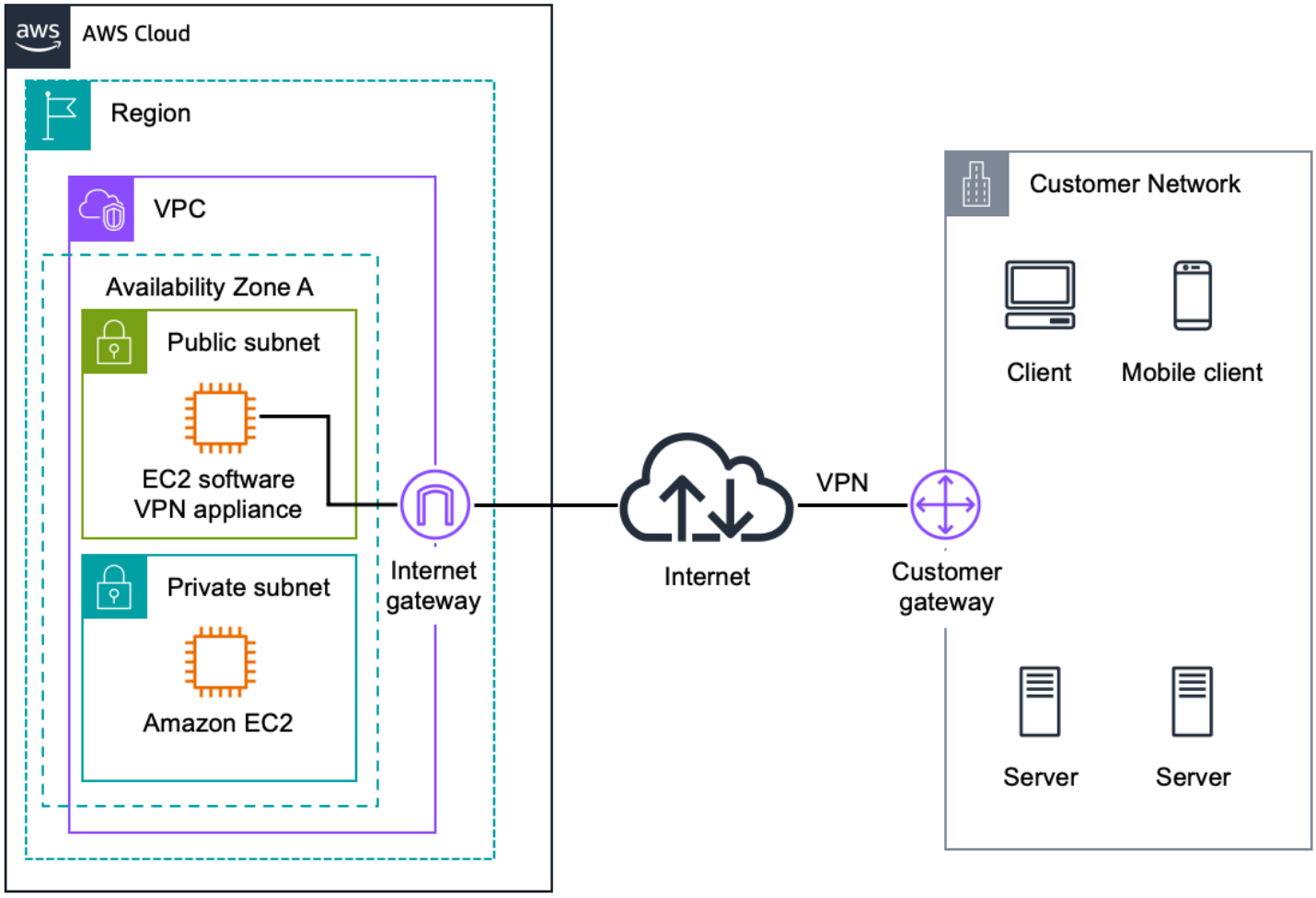
- Third-party appliances must be configured with a GRE tunnel in order to send and receive traffic from Transit Gateway using connect attachments. The appliance must be configured with BGP for dynamic route updates and health checks.
- Connect attachments do not support static routes.
- Transit Gateway connect attachments support a maximum bandwidth of five Gbps per GRE tunnel. Bandwidth above five Gbps can achieved by advertising the same prefixes across multiple Connect peer (GRE tunnels) for the same Connect attachment.
- A maximum of four Connect peers are supported for each connect attachment.
- Transit Gateway connect attachments support IPv6 and dynamic route advertisements through Multiprotocol Extensions for BGP (MBGP or MP-BGP).

Additional resources

- Transit gateway peering attachments
- Requirements and considerations
- Blog post: Simplify SD-WAN connectivity with AWS Transit Gateway Connect

Software VPN

Amazon VPC offers you the flexibility to fully manage both sides of your Amazon VPC connectivity by creating a VPN connection between your remote network and a software VPN appliance running in your Amazon VPC network. This option is recommended if you must manage both ends of the VPN connection, either for compliance purposes or for leveraging gateway devices that are not currently supported by Amazon VPC's VPN solution. The following figure shows this option.



Software Site-to-Site VPN

You can choose from an ecosystem of multiple partners and open-source communities that have produced software VPN appliances that run on Amazon EC2. Along with this choice comes the responsibility that you must manage the software appliance, including configuration, patches, and upgrades.

Note that this design introduces a potential single point of failure into the network design because the software VPN appliance runs on a single Amazon EC2 instance. For additional information, see Appendix A: High-Level HA architecture for software VPN instances Architecture for Software VPN Instances.

Additional resources

- VPN appliances available in the AWS Marketplace
- Tech Brief - Connecting Cisco ASA to VPC EC2 Instance (IPsec)

- Tech Brief - Connecting Multiple VPCs with EC2 Instances (IPsec)
- Tech Brief - Connecting Multiple VPCs with EC2 Instances (SSL)

Amazon VPC-to-Amazon VPC connectivity options

Use these design patterns when you want to integrate multiple Amazon VPCs into a larger virtual network. This is useful if you require multiple VPCs due to security, billing, presence in multiple regions, or internal charge-back requirements, to more easily integrate AWS resources between Amazon VPCs. You can also combine these patterns with the Network–to–Amazon VPC connectivity options for creating a corporate network that spans remote networks and multiple VPCs.

VPC connectivity between VPCs is best achieved when using non-overlapping IP ranges for each VPC being connected. For example, if you'd like to connect multiple VPCs, make sure each VPC is configured with unique Classless Inter-Domain Routing (CIDR) ranges. Therefore, we advise you to allocate a single, contiguous, non-overlapping CIDR block to be used by each VPC. For additional information about Amazon VPC routing and constraints, see the Amazon VPC Frequently Asked Questions.

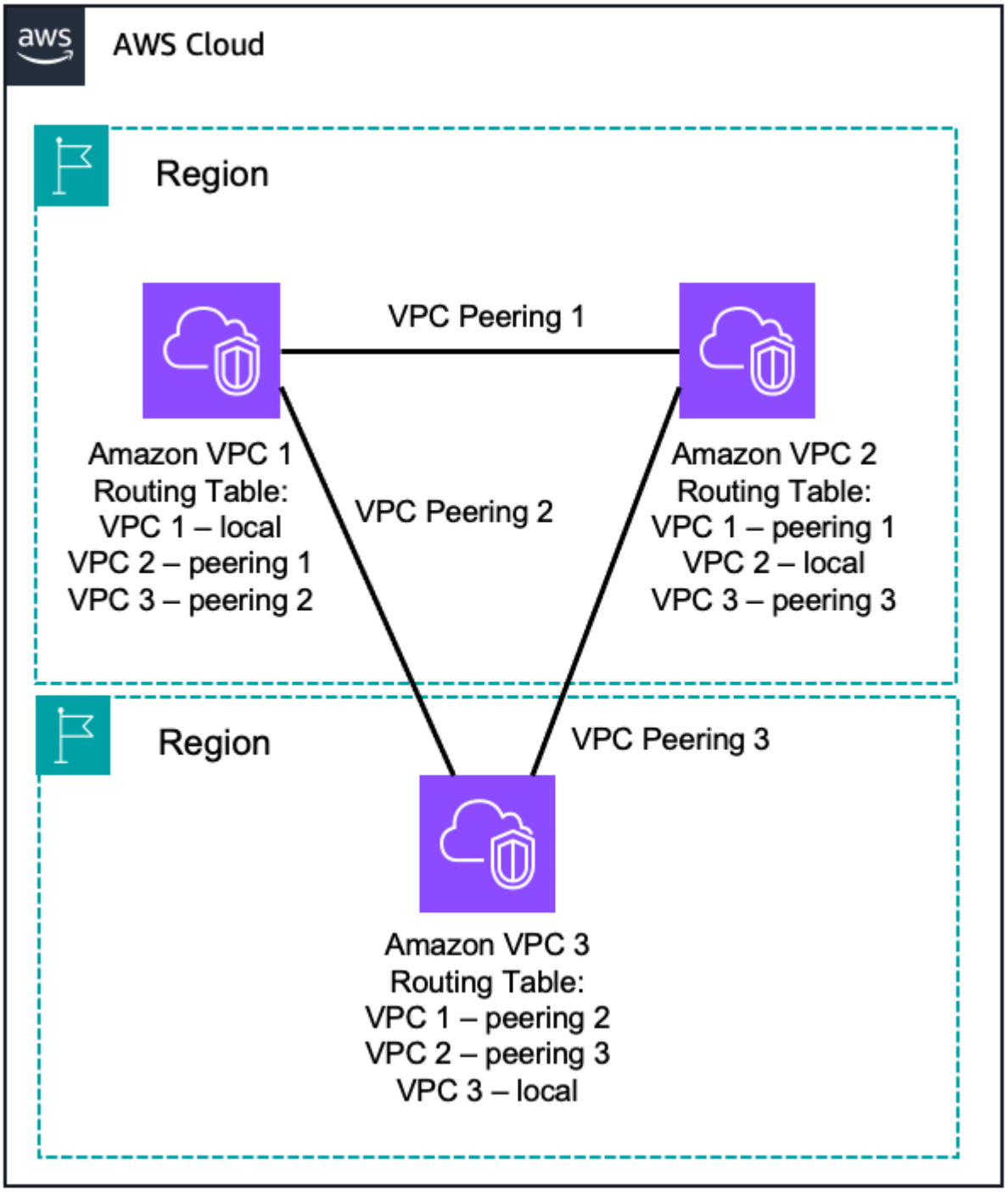
Option	Use Case	Advantages	Limitations
VPC peering	AWS-provided network connectivity between two VPCs.	Leverages AWS managed scalable networking infrastructure	VPC peering does not support transitive peering relationships Difficult to manage at scale
AWS Transit Gateway	AWS-provided regional router connectivity for VPCs	AWS managed high availability and scalability service Regional network hub for up to 5,000 attachments	Transit Gateway peering only supports static routes
AWS PrivateLink	AWS-provided network connectivity between two VPCs using interface endpoints	Leverages AWS managed scalable networking infrastructure	VPC Endpoint services only available in the AWS region in which they are created

Option	Use Case	Advantages	Limitations
Software VPN	Software appliance-based VPN connections between VPCs	Supports a wide array of VPN vendors, products, and protocols Managed entirely by you	You are responsible for implementing HA solutions for all VPN endpoints (if required) VPN instances could become a network bottleneck
Software VPN-to-AWS Site-to-Site VPN	Software appliance to VPN connection between VPCs	AWS managed high availability VPC VPN connection Supports a wide array of VPN vendors and products managed by you Supports static routes and dynamic BGP peering and routing policies	You are responsible for implementing HA solutions for the software appliance VPN endpoints (if required) VPN instances could become a network bottleneck IPsec VPN protocol only to AWS Managed VPN

VPC peering

A VPC peering connection is a networking connection between two VPCs that enables routing using each VPC's private IP addresses as if they were in the same network. VPC peering connections can be created between your own VPCs or with a VPC in another AWS account. VPC peering also supports inter-region peering.

Traffic using inter-region VPC Peering always stays on the global AWS backbone and never traverses the public internet, thereby reducing threat vectors, such as common exploits and DDoS attacks.



VPC-to-VPC Peering

AWS uses the existing infrastructure of a VPC to create VPC peering connections and does not rely on a separate piece of physical hardware. Therefore, they do not introduce a potential single point of failure or network bandwidth bottleneck between VPCs. Additionally, VPC routing tables, security groups, and network access control lists can be leveraged to control which subnets or instances are able to utilize the VPC peering connection.

Amazon VPCs do not support transitive peering, meaning that you can't communicate two VPCs that are not directly peered using a third VPC as transit. If you want all of your VPCs to communicate with each other using VPC peering, you will need to create 1:1 VPC peering connections between each of them. Alternatively, you can use AWS Transit Gateway or AWS Cloud WAN to act as a network transit hub.

Both IPv4 and IPv6 traffic is supported in VPC peering connections. However, two VPCs cannot be peered if their primary IPv4 CIDR block overlaps, regardless of the secondary IPv4 or IPv6 CIDR blocks used. Take this into account when assigning the primary CIDR block to your VPCs if you plan to use VPC peering between them.

Additional resources

- Amazon VPC peering
- What is VPC peering?

AWS Transit Gateway

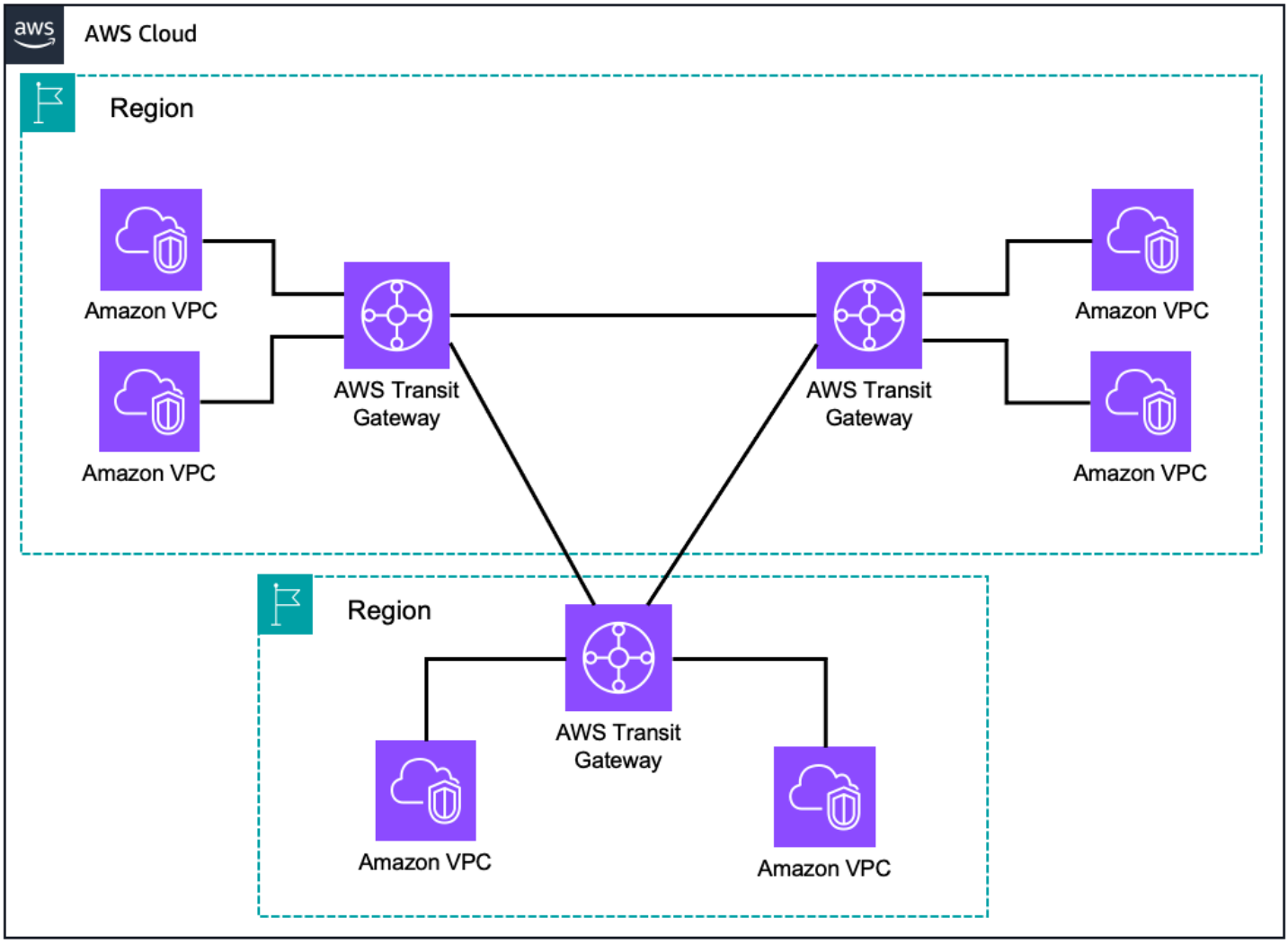
AWS Transit Gateway is a highly available and scalable service to consolidate the AWS VPC routing configuration for a region with a hub-and-spoke architecture. Each spoke VPC only needs to connect to the Transit Gateway to gain access to other connected VPCs. Both IPv4 and IPv6 traffic is supported in AWS Transit Gateway.

You can take advantage of several Transit Gateway route tables, associations, and propagations to segment your traffic within the same Transit Gateway. You will be able to manage different routing domains (for example, production and non-production traffic) from a single point of management, ensuring that these routing domains won't be able to communicate between each other.

You can also take advantage of the hub-and-spoke architecture created by Transit Gateway to centralize access to shared services such as traffic inspection, interface VPC endpoint access, or egress traffic through a NAT gateway or NAT instances. This centralization simplifies the complexity of managing these resources in several VPCs, and allow for a better control as you extend your footprint in AWS.

Transit Gateways can be peered with each other within the same AWS Region or between different AWS Regions. AWS Transit Gateway traffic always stays on the global AWS backbone and never traverses the public internet, thereby reducing threat vectors such as common exploits and DDoS attacks.

With a large number of VPCs, Transit Gateway provides simpler VPC-to-VPC communication management over VPC Peering, as shown in the following figure.



AWS Transit Gateway

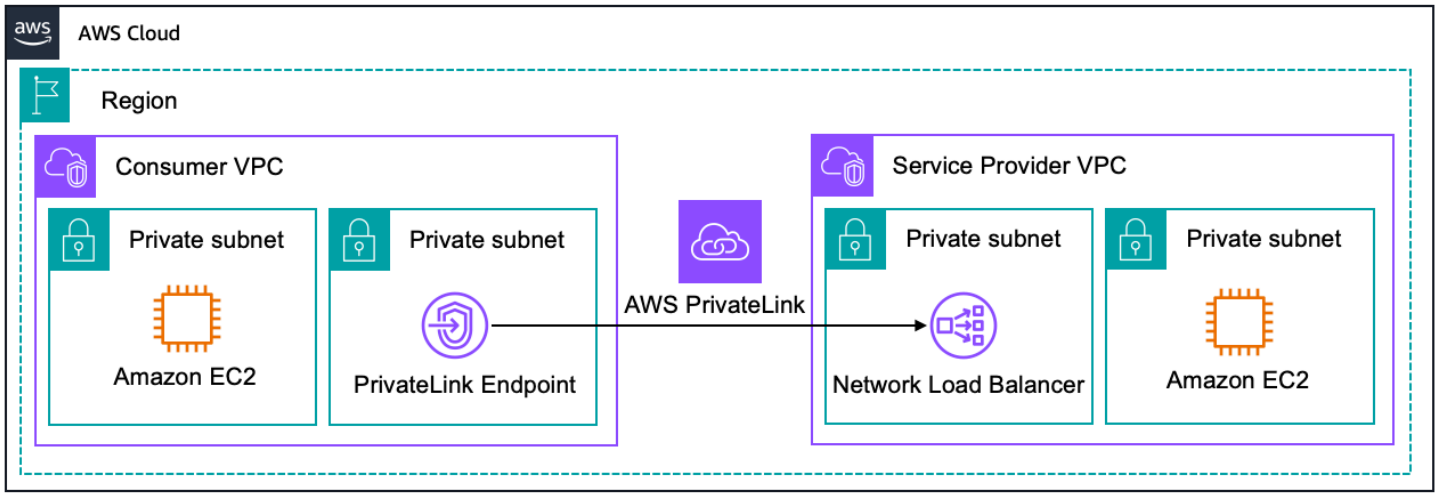
For a central visibility of IP traffic going to and from your Transit Gateways, you can publish Transit Gateway Flow Logs to Amazon CloudWatch Logs and Amazon S3. Flow log data is collected outside of the path of your network traffic, and therefore does not affect network throughput or latency.

Additional resources

- Amazon VPC transit gateway
- Transit gateway peering attachments
- Work with Transit Gateways
- Logging network traffic using Transit Gateway Flow Logs

AWS PrivateLink

AWS PrivateLink enables you to connect to some AWS services, services hosted by other AWS accounts (referred to as *endpoint services*), and supported AWS Marketplace partner services, via private IP addresses in your VPC. The interface endpoints are created directly inside of your VPC, using elastic network interfaces and IP addresses in your VPC's subnets. That means that VPC Security Groups can be used to manage access to the endpoints.



AWS PrivateLink

We recommend this approach if you want to use services offered by another VPC securely within an AWS network, using private IP addresses. Alternatively, AWS PrivateLink is a good solution when the VPCs have overlapped IP addresses.

AWS PrivateLink fully supports IPv6, but both of the destination VPCs, VPC Subnets, the Network Load Balancer, and the DNS names have to be enabled or modified to use dual-stack. After these pre-requisites are met, IPv6 can be enabled at the service configuration for the endpoint.

Access controls to AWS PrivateLink

The interface endpoints are created directly inside of your VPC by using elastic network interfaces and IP addresses in your VPC's subnets. That means that VPC Security Groups can be used to manage network access to the endpoints.

When you create an interface endpoint or a gateway endpoint, you can also attach an endpoint policy. The endpoint policy controls which AWS principals (AWS accounts, IAM users, and roles) can use the VPC endpoint to access the endpoint service.

You cannot attach more than one policy to an endpoint. However, you can modify an endpoint policy at any time.

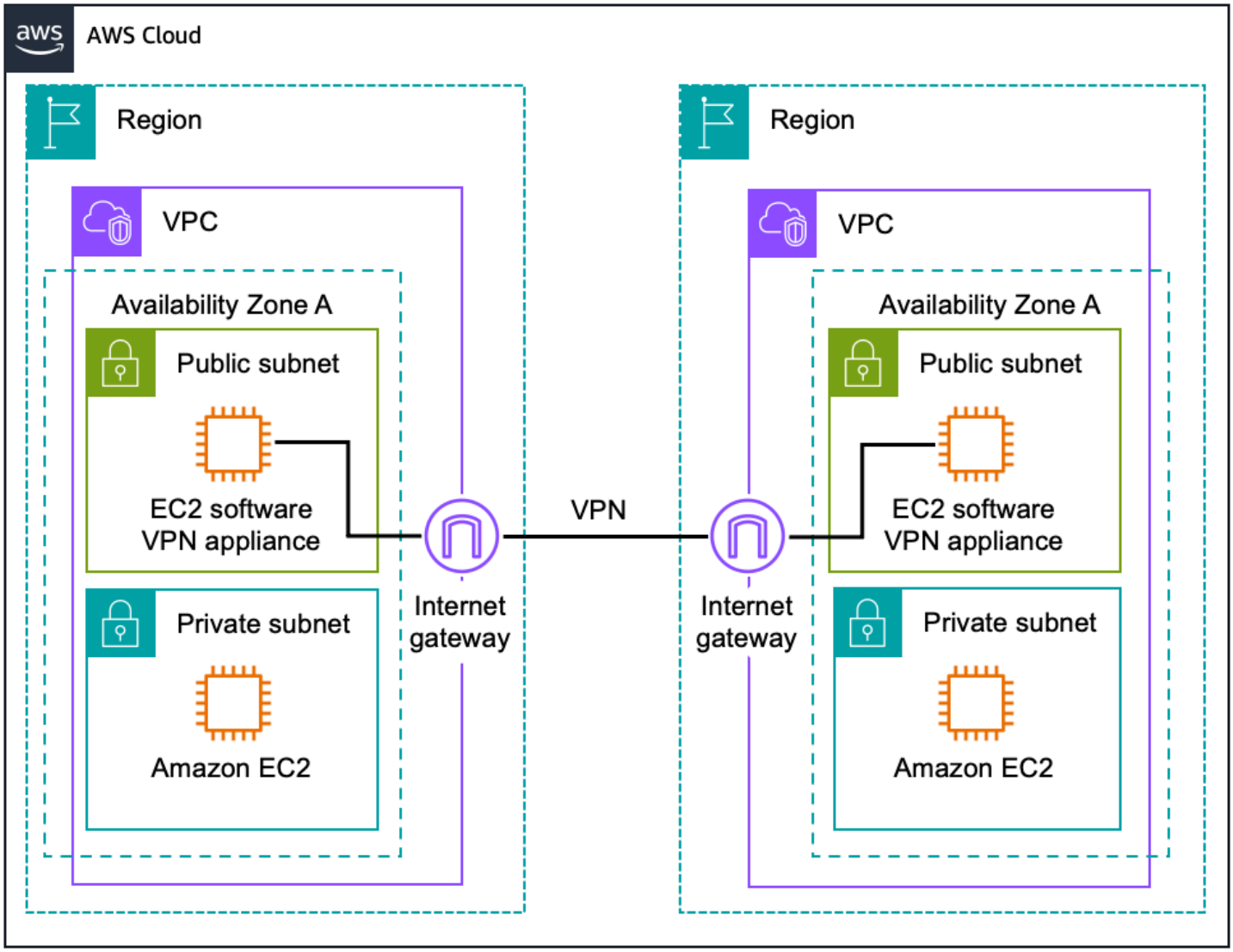
An endpoint policy does not override or replace IAM user policies or service-specific policies (such as Amazon S3 bucket policies). If you're using an interface endpoint to connect to Amazon S3, you can also use Amazon S3 bucket policies to control access to buckets from specific endpoints or specific VPCs.

Additional resources

- Interface VPC endpoints (AWS PrivateLink)
- VPC endpoint services (AWS PrivateLink)
- Blog post: Expedite your IPv6 adoption with PrivateLink services and endpoints
- Blog post: Connecting Networks with Overlapping IP Ranges
- AWS PrivateLink Partners

Software VPN

Amazon VPC provides network routing flexibility. This includes the ability to create secure VPN tunnels between two or more software VPN appliances to connect multiple VPCs into a larger virtual private network so that instances in each VPC can seamlessly connect to each other using private IP addresses. This option is recommended when you want to manage both ends of the VPN connection using your preferred VPN software provider. This option uses an internet gateway attached to each VPC to facilitate communication between the software VPN appliances.



Software Site-to-Site VPN VPC-to-VPC Routing

You can choose from an ecosystem of multiple partners and open source communities that have produced software VPN appliances that run on Amazon EC2. Along with this choice comes the responsibility for you to manage the software appliance including configuration, patches, and upgrades.

Note that this design introduces a potential single point of failure into the network design as the software VPN appliance runs on a single Amazon EC2 instance. For additional information, see Appendix A: High-Level HA architecture for software VPN instances.

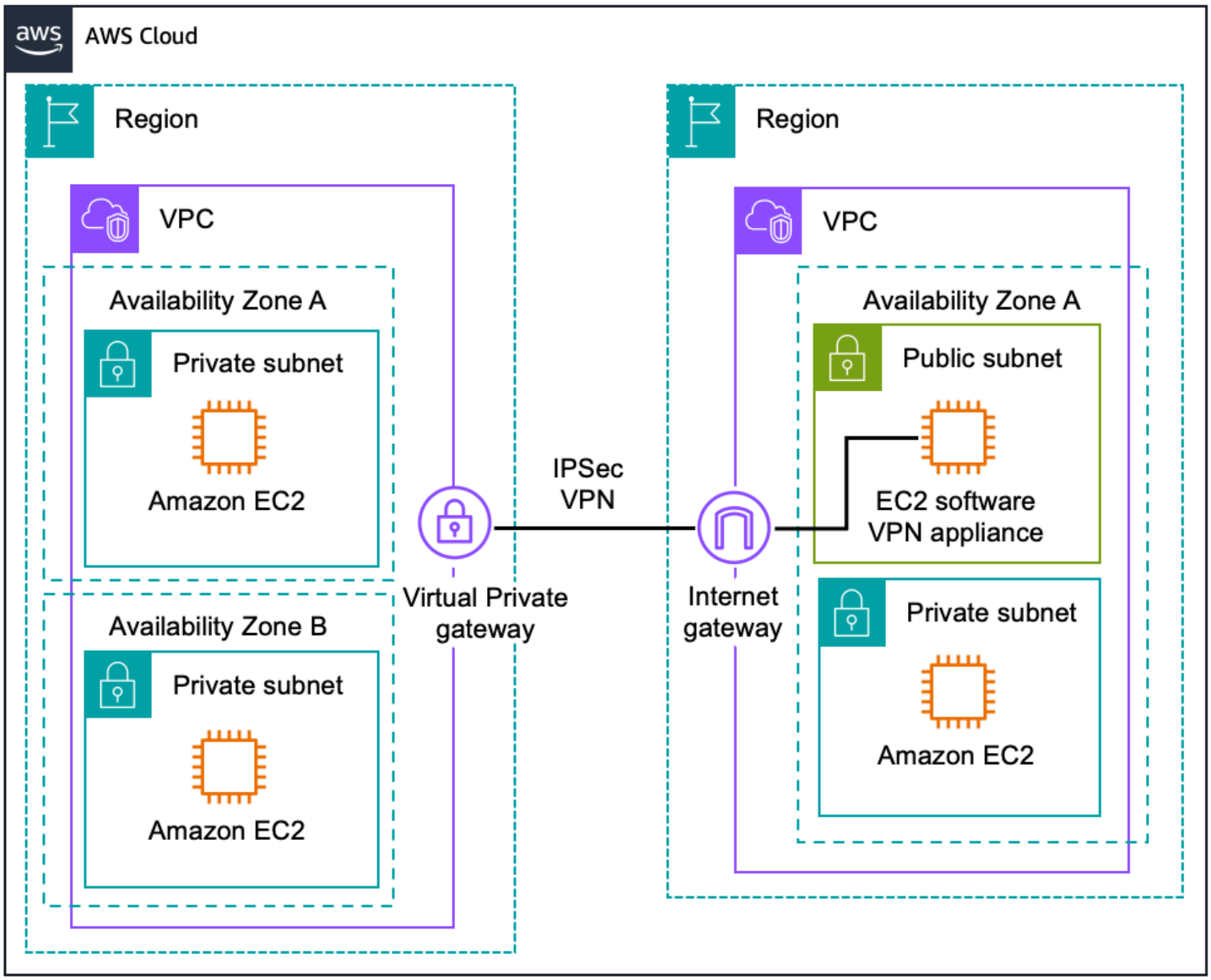
Additional resources

- VPN appliances available from the AWS Marketplace

- Tech Brief - Connecting Multiple VPCs with EC2 Instances (IPsec)
- Tech Brief - Connecting Multiple VPCs with EC2 Instances (SSL)

Software VPN-to-AWS Site-to-Site VPN

Amazon VPC provides the flexibility to combine the AWS managed VPN and software VPN options to connect multiple VPCs. With this design, you can create secure VPN tunnels between a software VPN appliance and a virtual private gateway, allowing instances in each VPC to seamlessly connect to each other using private IP addresses. This option uses a virtual private gateway in one Amazon VPC and a combination of an internet gateway and software VPN appliance in another Amazon VPC, as shown in the following figure.



Software VPN to AWS Site-to-Site VPN VPC-to-VPC Routing

Note that this design introduces a potential single point of failure into the network design. For additional information, see Appendix A: High-Level HA architecture for software VPN instances.

Additional resources

- VPN appliances available from the AWS Marketplace
- AWS Site-to-Site VPN User Guide
- Requirements for customer gateway devices

Software remote access-to-Amazon VPC connectivity options

With software remote access VPN, you can leverage low cost, elastic, and secure services to implement remote-access solutions while also providing a seamless experience connecting to AWS hosted resources. This option is typically preferred by smaller companies with less extensive remote networks or who have not already built and deployed remote access solutions for their employees.

You can combine these patterns with the Network-to-Amazon VPC connectivity options connectivity options and Amazon VPC-to-Amazon VPC connectivity options to create a network that spans remote networks and multiple VPCs.

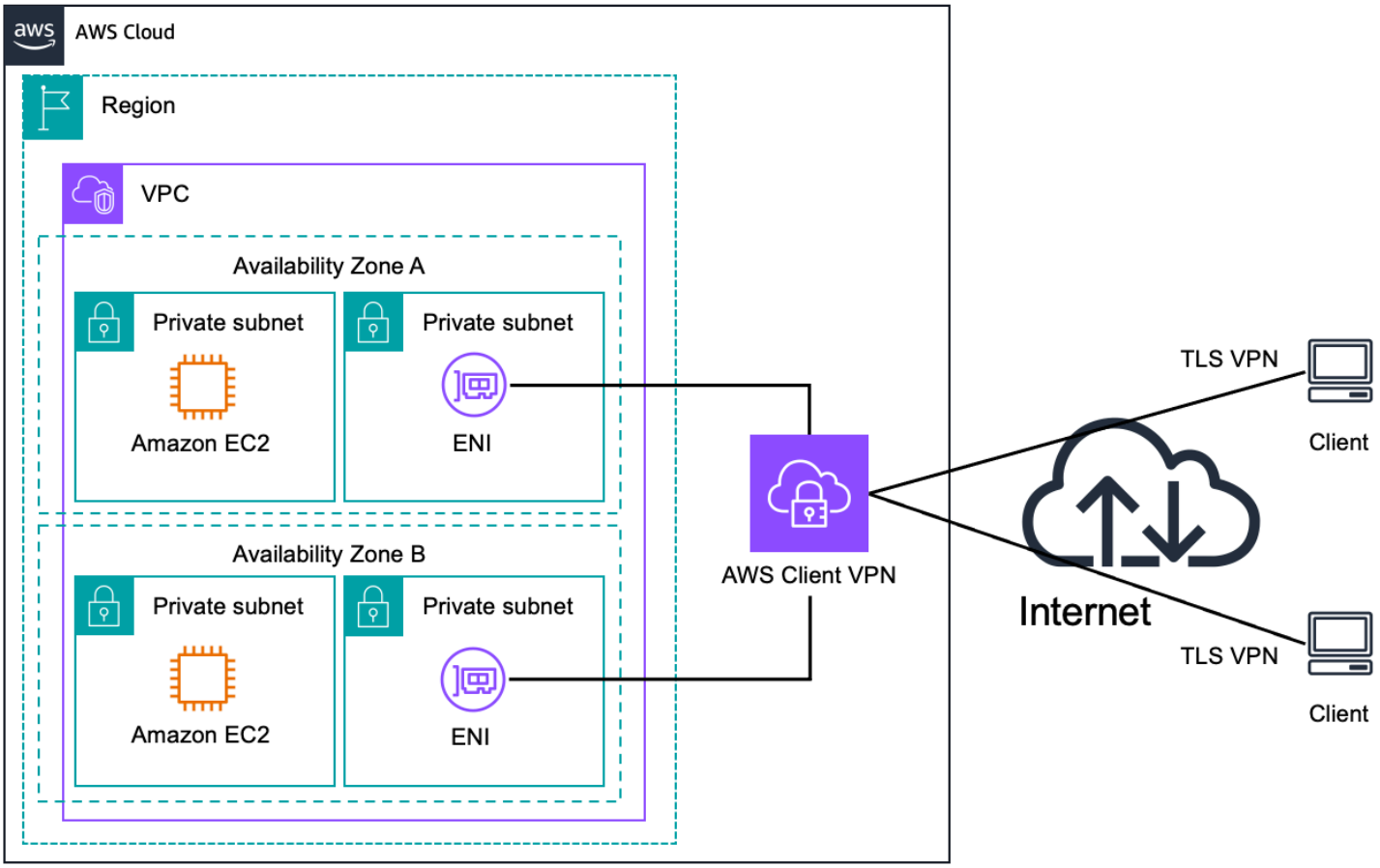
The following table outlines the advantages and limitations of these options.

Option	Use Case	Advantages	Limitations
AWS Client VPN	AWS managed remote access solution to Amazon VPC and/or internal networks	AWS managed high availability and scalability service	OpenVPN clients only
Software client VPN	Software VPN appliance remote access solution to Amazon VPC and/or internal networks	Supports a wider array of VPN vendors, products, and protocols Fully customer-managed solution	You are responsible for implementing HA solutions

AWS Client VPN

AWS Client VPN is an AWS managed high availability and scalability service enabling secure software remote access. It provides the option of creating a secure TLS connection between remote

clients and your Amazon VPCs, to securely access AWS resources and on-premises over the internet, as shown in the following figure.



AWS Client VPN Remote Access

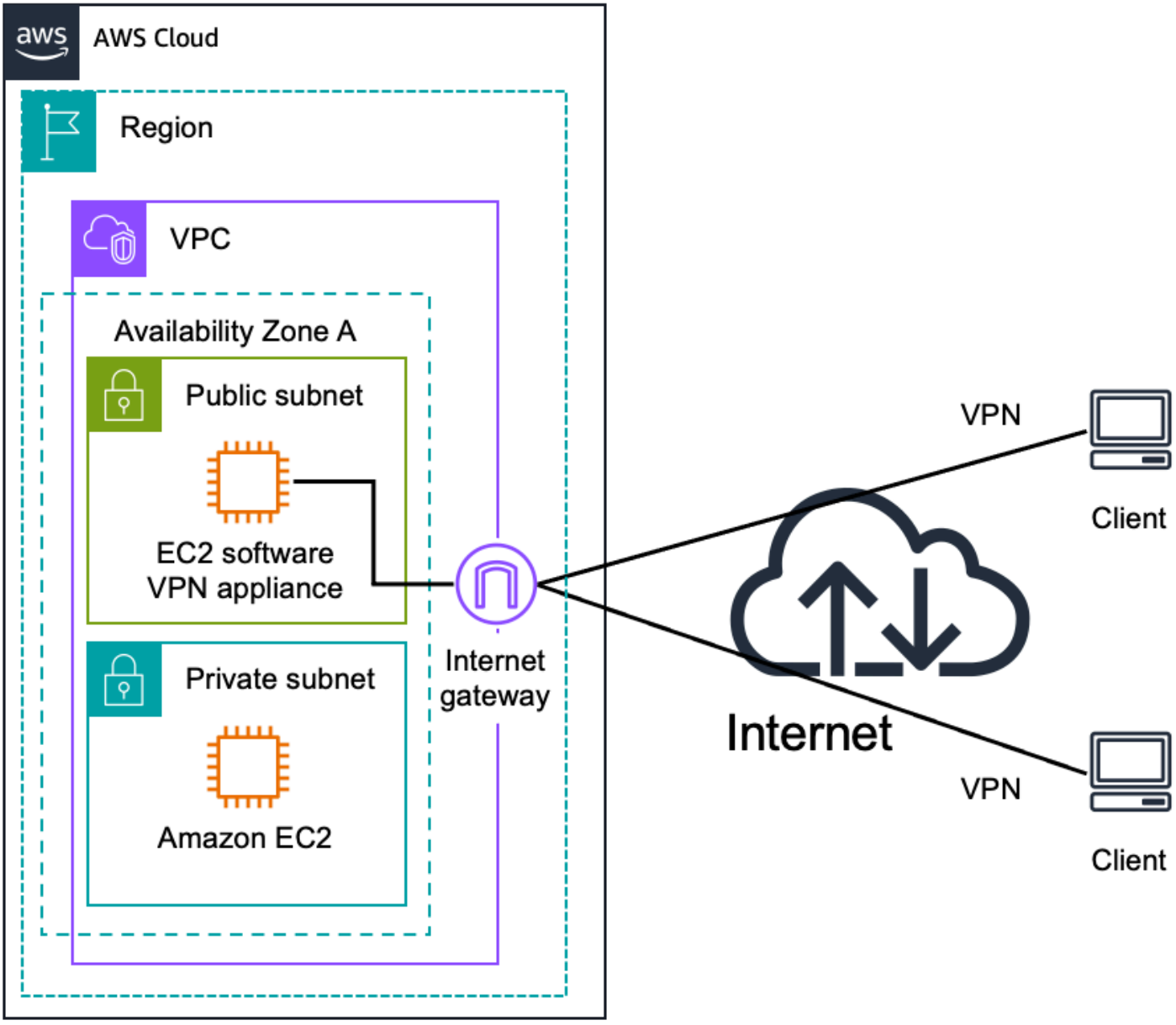
The remote clients can be the AWS Client VPN for Desktop, or third-party OpenVPN VPN clients, with authentication by either Active Directory or mutual certificate authentication.

Additional resources

- AWS Client VPN Administrator Guide

Software client VPN

You can choose from an ecosystem of multiple partners and open source communities that have produced remote-access solutions that run on Amazon EC2. These solutions provide great flexibility on the security protocol use for remote-access into your Amazon VPCs, to securely access AWS resources and on-premises over the internet, as shown in the following figure.



Software Client VPN Remote Access

Remote-access solutions range in complexity, support multiple client authentication options (including multifactor authentication) and can be integrated with either Amazon VPC or remotely hosted identity and access management solutions (leveraging one of the network-to-Amazon VPC options) like Microsoft Active Directory or other LDAP/multifactor authentication solutions.

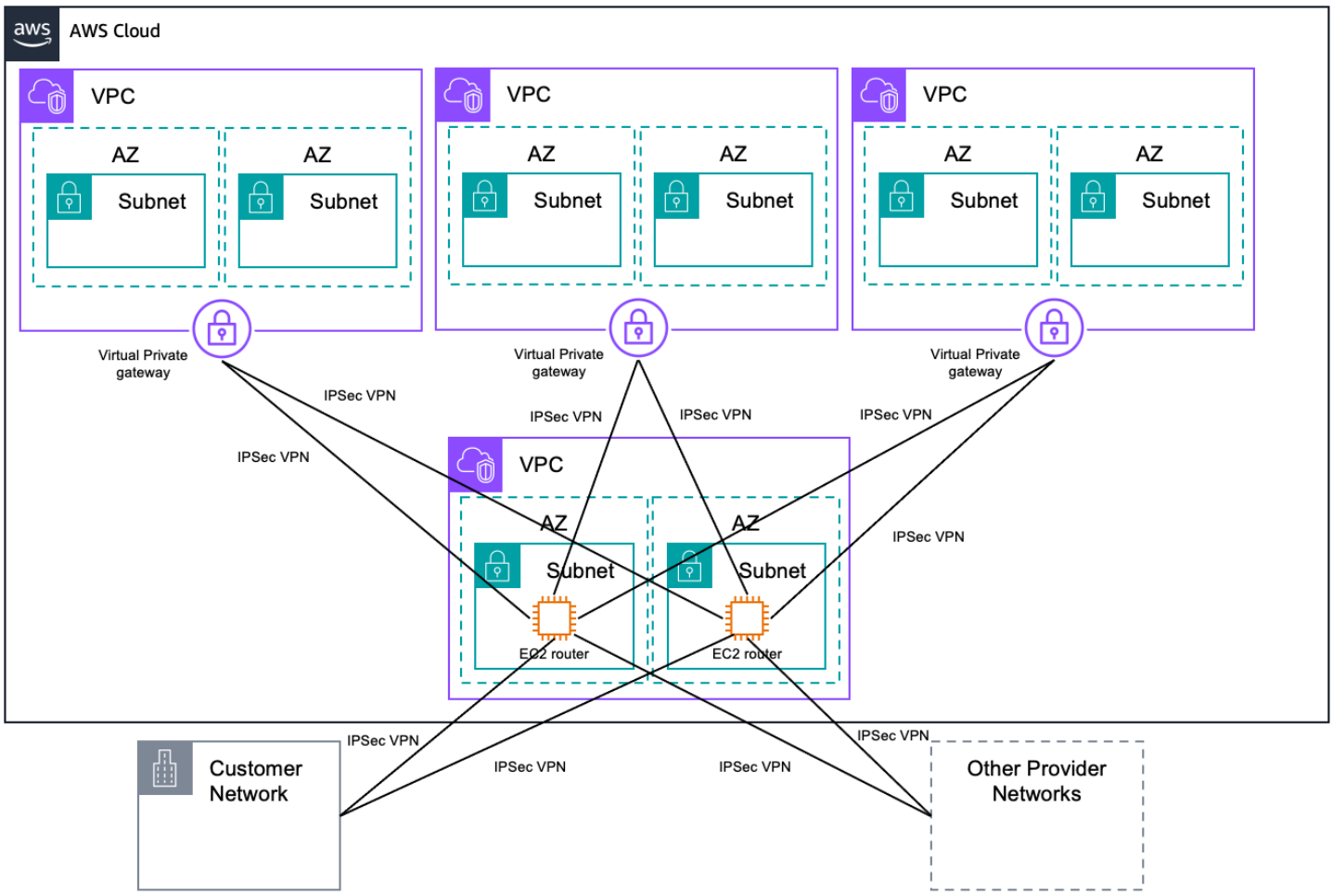
You are responsible for managing the remote access software including user management, configuration, patches and upgrades. This design introduces a potential single point of failure into the network design as the remote access server runs on a single Amazon EC2 instance. For additional information, see Appendix A: High-Level HA architecture for software VPN instances.

Additional resources

- VPN appliances available from the AWS Marketplace
- OpenVPN Access Server Quick Start Guide

Transit VPC

Building on the Software VPN designs mentioned above, you can create a global transit network on AWS. A transit VPC is a common strategy for connecting multiple, geographically disperse VPCs and remote networks in order to create a global network transit center. A transit VPC simplifies network management and minimizes the number of connections required to connect multiple VPCs and remote networks. The following figure illustrates this design.



Transit VPC

Along with providing direct network routing between VPCs and on-premises networks, this design also enables the transit VPC to implement more complex routing rules, such as network address translation between overlapping network ranges, or to add additional network-level packet filtering or inspection. The transit VPC design can be used to support important use cases like, private networking, shared connectivity and cross account AWS usage.

Additional resources

- AWS Transit Gateway
- Cisco Catalyst 8000V for SD-WAN & Routing in AWS Marketplace

AWS Cloud WAN

AWS Cloud WAN is an intent-driven managed wide area network (WAN), described by a policy you define that unifies your data center, branch, and AWS networks. While you can create your own global network by interconnecting multiple Transit Gateways across Regions, Cloud WAN provides built-in automation, segmentation, and configuration management features designed specifically for building and operating global networks, based on your core network policy. Cloud WAN has added features such as automated VPC attachments, integrated performance monitoring, and centralized configuration.

The core network policy is written in a declarative language that defines segments, AWS Region routing, and how the attachments should map to segments. With a core network policy, you can describe your intent for access control and traffic routing, while AWS Cloud WAN handles the network configuration details.

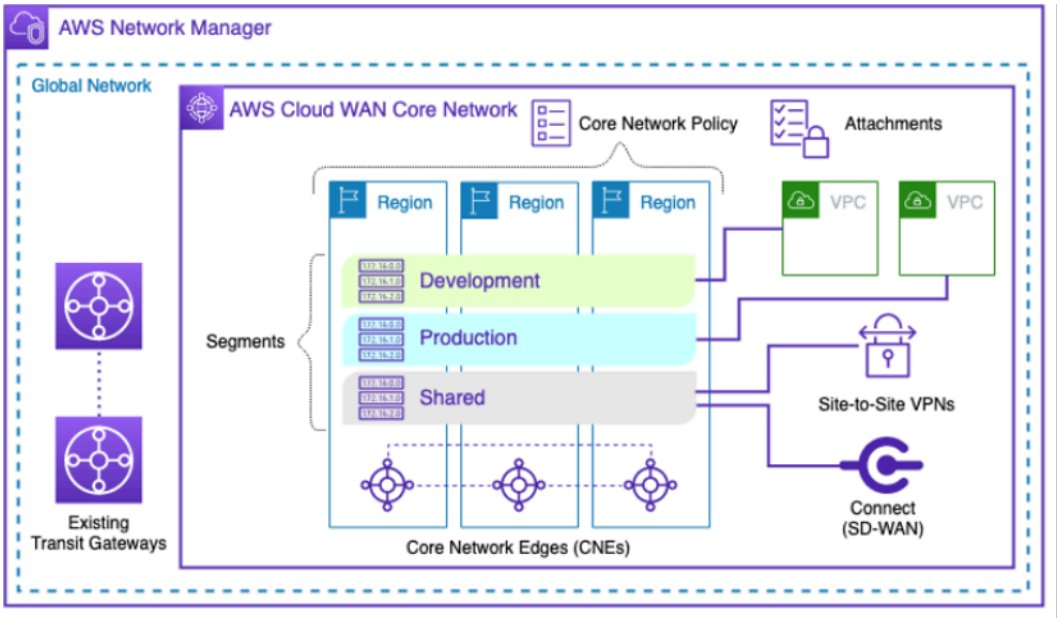
Cloud WAN is managed within AWS Network Manager, which enables you to centrally manage and visualize your Cloud WAN core network and Transit Gateway networks across AWS accounts, Regions, and on-premises locations. Network Manager provides you several dashboard visualizations to help you view and monitor all aspects of your global network. Some of the dashboards include:

- World maps that pinpoint where your network resources, such as edge locations, devices, and attachments, are located.
- Monitoring that uses CloudWatch Events to track 15 months' worth of statistics, giving you a better perspective on how your networks are performing.
- Event tracking that streams real-time events to an events dashboard.
- Topological and logical diagrams of your transit gateway networks and transit gateways.

Both Transit Gateway and Cloud WAN allow centralized connectivity between VPCs and on-premises locations. Transit Gateway is a regional network connectivity hub and is optimal for customers that operate in a few AWS Regions, want to manage their own peering and routing configuration, or prefer to use their own automation. Cloud WAN is optimal for customers who want to define their global network through policy and have the service implement the underlying components automatically.

Things to know

- CNE (Core network edge) inherits many Transit Gateway characteristics, such as throughput per VPC attachment.
- Cloud WAN supports both IPv4 and IPv6.
- Currently, Cloud WAN does not natively support AWS Direct Connect attachments. In order to use AWS Direct Connect with Cloud WAN, you need a Transit Gateway attached to an AWS Direct Connect gateway, and then the Transit Gateway peered to Cloud WAN.
- For large networks with many changes, consider creating a separate development and testing global network where you can validate changes.



AWS Cloud WAN

Additional resources

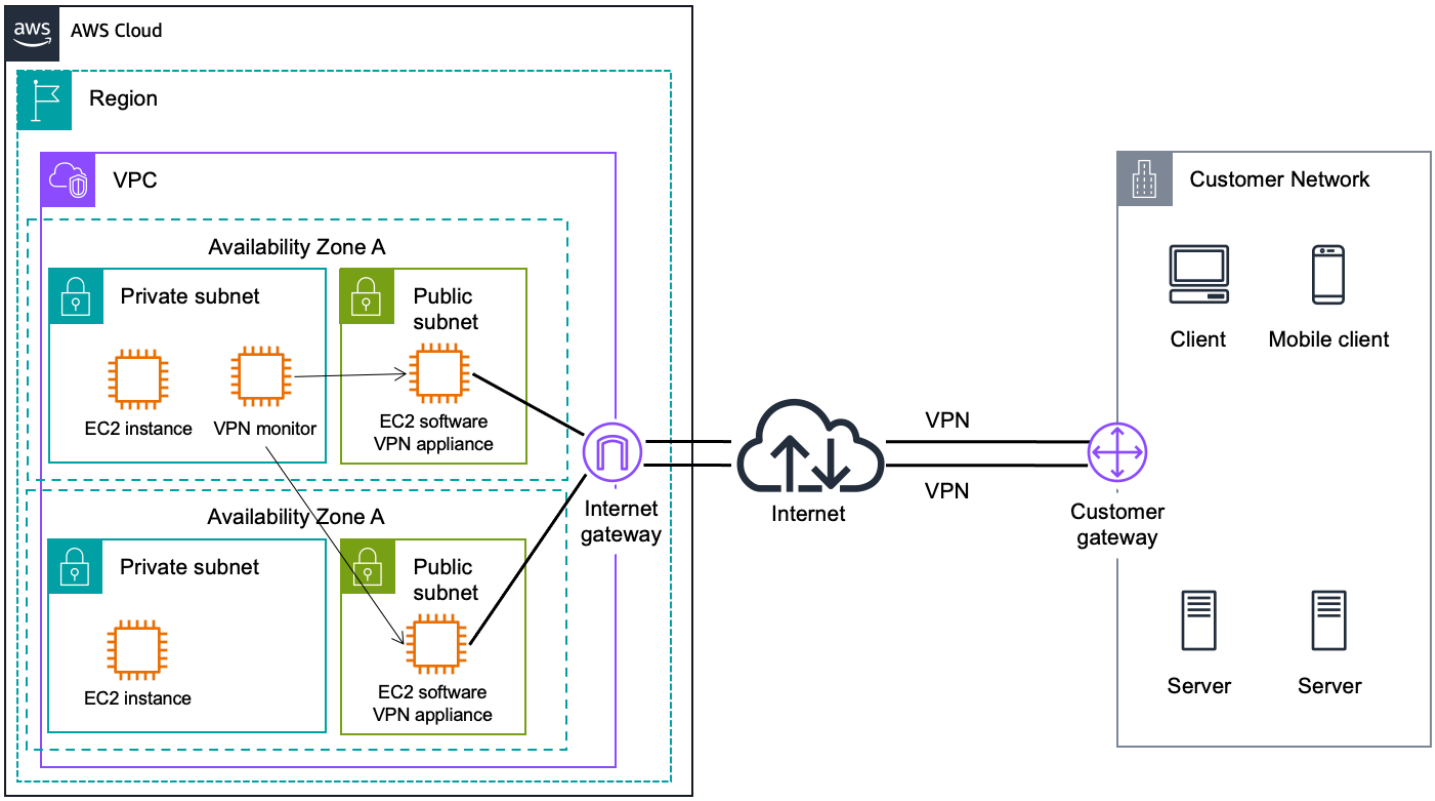
- AWS Cloud WAN Documentation
- Blog post: AWS Cloud WAN and AWS Transit Gateway migration and interoperability patterns

Conclusion

AWS provides a number of efficient, secure connectivity options to help you get the most out of AWS when integrating your remote networks with Amazon VPC. The options provided in this whitepaper highlight several of the connectivity options and patterns that customers have used to successfully integrate their remote networks or multiple Amazon VPC networks. You can use the information provided here to determine the most appropriate mechanism for connecting the infrastructure required to run your business regardless of where it is physically located or hosted.

Appendix A: High-Level HA architecture for software VPN instances

Creating a fully resilient VPC connection for software VPN instances requires the setup and configuration of multiple VPN instances and a monitoring instance to monitor the health of the VPN connections.



High-Level Software VPN HA

We recommend configuring your VPC route tables to leverage all VPN instances simultaneously by directing traffic from all of the subnets in one Availability Zone through its respective VPN instances in the same Availability Zone. Each VPN instance then provides VPN connectivity for instances that share the same Availability Zone.

VPN monitoring

To monitor Software based VPN appliance you can create a VPN Monitor. The VPN monitor is a custom instance that you will need to run the VPN monitoring scripts. This instance is intended to run and monitor the state of VPN connection and VPN instances. If a VPN instance or connection

goes down, the monitor needs to stop, terminate, or restart the VPN instance while also rerouting traffic from the affected subnets to the working VPN instance until both connections are functional again. Since customer requirements vary, AWS does not currently provide prescriptive guidance for setting up this monitoring instance. However, an example script for enabling HA between NAT instances could be used as a starting point for creating an HA solution for Software VPN instances. We recommend that you think through the necessary business logic to provide notification or attempt to automatically repair network connectivity in the event of a VPN connection failure.

Additionally, you can monitor the AWS Managed VPN tunnels using Amazon CloudWatch metrics, which collects data points from the VPN service into readable, near real-time metrics. Each VPN connection collects and publishes a variety of tunnel metrics to Amazon CloudWatch. These metrics allow you to monitor tunnel health, activity, and create automated actions.

Contributors

Contributors to this document include:

- Daniel Yu, Senior Technical Account Manager, AWS Enterprise Support
- Garvit Singh, Solutions Builder, AWS Solution Architecture
- Steve Morad, Senior Manager, Solution Builders, AWS Solution Architecture
- Sohaib Tahir, Solutions Architect, AWS Solution Architecture
- Fiona Armada, Principal Solutions Architect, AWS Solution Architecture
- Pablo Sánchez Carmona, Networking Specialist Solutions Architect, AWS Solution Architecture
- Tony Hawke, Senior Networking Specialist Technical Account Manager, AWS Enterprise Support

Document revisions

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

Change	Description	Date
Whitepaper updated	Added AWS Cloud WAN and Transit Gateway connect attachment options, updated diagrams and information throughout.	April 5, 2023
Whitepaper updated	Added AWS Transit Gateway and AWS Client VPN options, updated diagrams and information throughout.	June 6, 2020
Minor update	Minor change to fix reference to software VPN appliance.	May 20, 2020
Whitepaper updated	Updated information throughout. Focus on the following designs/features: transit VPC, Direct Connect gateway, and AWS PrivateLink.	January 1, 2018
Initial publication	Amazon Virtual Private Cloud Connectivity Options published.	July 1, 2014

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.